ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Análisis, Diseño e Implementación de un Sistema de Administración de Información basado en una Intranet"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN COMPUTACIÓN

Presentada por:

Marfiu Wladimir Rodríguez Jara

Freddy Wladimir Vergara Uquillas

GUAYAQUIL – ECUADOR

2004

AGRADECIMIENTO

A todas las personas que de uno u otro modo colaboraron en la realización de este trabajo y especialmente en el Dr. Enrique Peláez Director de Tesis, por su invaluable ayuda.

DEDICATORIA

NUESTROS PADRES

NUESTRAS ESPOSAS

NUESTROS HIJOS

DIOS

TRIBUNAL DE GRADUACIÓN

ING. MIGUEL YAPUR
SUBDECANO DE LA FIEC
PRESIDENTE DEL TRIBUNAL

DR. ENRIQUE PELAEZ
DIRECTOR DE TESIS

ING. GUIDO CALCEDO
VOCAL PRINCIPAL

ING. SIXTO GARCÍA
VOCAL PRINCIPAL

Escaneado con CamScanner

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de ésta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”

(Reglamento de Graduación de la ESPOL).

_____

Marfiu Wladimir Rodríguez Jara

_____

Freddy Vladimir Vergara Uquillas

RESUMEN

El propósito de ésta tesis de grado es diseñar la infraestructura técnica, administrativa y organizacional que soporte un sistema de administración de información de la Armada basado en una Intranet.

En el capítulo 1, se resalta la importancia de la información y su rol en la evolución de la organización. Se describe el impacto de la tecnología al fomentar las superautopistas de información, detallando el potencial del web como el medio de comunicación que revolucionará la forma en que las organizaciones deberán funcionar. Para alcanzar esta meta se detallan aspectos fundamentales a ser considerados, a manera de metas, que permitan adoptar una actitud organizacional acorde a la presente era de la información.

En el capítulo 2 se describe formalmente la tecnología de Intranet buscando un enfoque estratégico para su uso. Se determina que paralelamente a la adopción de la tecnología se demanda una reforma organizacional para afrontar los nuevos paradigmas. Se justificará la necesidad de una descentralización de la toma de decisiones, permitiendo que sea la Intranet la que centralice la comunicación y la coordinación. Se define también el significado de las actividades conducidas por propósito, la importancia de habilitar a la organización con una herramienta que permita compartir

información, en base a lo cual se pueda innovar para tener una institución que aprende, orientada permanentemente al mejoramiento continuo. Trata también el problema de la sobrecarga de información y, analizando la tecnología de push y pull se consideran alternativas para enfocar la información en demanda. Finalmente se definen los roles, organismos y el marco de trabajo de una organización bajo una Intranet.

En el capítulo 3 se define el esquema de la organización de la información que se manejará electrónicamente; se describe una metodología para la definición de una arquitectura lógica de la información en la Intranet. Se hace un análisis funcional de la Armada, con el objetivo de determinar las interacciones entre los sectores y repartos que permitirá entender el flujo de la información en la Institución y proponer un portafolio de desarrollo de sistemas de información.

El capítulo 4 define los diferentes tipos de aplicaciones que podría tener el Intranet con el propósito de sugerir a la Armada en que escenarios sería aplicable su uso. Definir esquemas de grandes repositorios de datos consolidados en un solo sistema de administración de base de datos relacional, que a futuro se tengan para realizar un diseño macro del Intranet definiendo la infraestructura tecnológica requerida y las necesidades de enlaces de comunicaciones.

El capítulo 5 es práctico, se implementa una Intranet piloto en el INOCAR, definiendo roles, procedimientos y estándares para su manejo, así como un sistema de información basado en la plataforma Java 2 Enterprise Edition sobre el web; el sistema se diseñó basado en el paradigma orientado a objetos siguiendo el enfoque de UML e implementado con el lenguaje orientado a objetos JAVA.

ÍNDICE GENERAL

Pág.

RESUMEN …… VI

ÍNDICE GENERAL…….. IX

ÍNDICE DE FIGURAS…….. XIV

ÍNDICE DE TABLAS…… XXI

INTRODUCCIÓN…….. 1

I. CONSIDERACIONES BÁSICAS SOBRE EL MANEJO ADECUADO DE LA INFORMACIÓN…… 5

1.1 Importancia de la Información en el Ámbito Militar……. 6

1.2 Definición de un Sistema de Mando y Control……. 8

1.3 Proceso de Obtención de Información…….. 10

1.4 La Era de la Información…… 11

1.5 La Información Influye en la Evolución de la Organización….. 17

1.6 Beneficios de la Tecnología Web…….. 28

II. IMPACTO DE UNA INTRANET EN LA ORGANIZACIÓN……... 31

2.1 Qué es una Intranet?…… 31

2.2 La Toma de las Decisiones Descentralizadas…… 33

2.3 Control y Comunicación: La Clave para las Actividades Conducidas por Propósitos…… 37

2.3.1 Innovación Adaptiva…… 43

2.4 Ciclo de Vida de la Administración de la Información…… 45

2.4.1 Acceso, Poder e Innovación …….. 46

2.5 Reducción de la Sobrecarga de Información …….. 52

2.5.1 Potenciando al Individuo ……. 58

2.5.2 Transferencia Eficiente de la Información …….. 59

2.6 Diferencias Medulares en las Herramientas Disponibles …….. 60
2.7 Marco de Trabajo para la Información en una Intranet ……. 64
2.7.1 Usuarios/Autores/Agentes/Publicadores ……..... 64
2.7.2 Revisión del Marco de Trabajo ……..... 69
2.8 Quienes son los Actores? …….. 70
2.8.1 Roles para la Administración de una Intranet …… 70
2.8.2 Roles Organizacionales ……..... 81

III. PLANIFICACIÓN DE LA INTRANET……..... 88
3.1 Clasificación de las Fuentes de Información …….. 88
3.2 Calificación de la Información ……. 90
3.3 Roles para la Implementación y Administración de la Intranet 93
3.3.1 Algunas Palabras Previas …….. 93
3.3.2 Guía de Implementación de la Intranet ……. 96
3.3.3 Normas para Establecer los Sitios Web …….. 102
3.3.4 Acerca de los Servicios de una Intranet …….. 105
3.3.5 Criterios de Selección de Servicios de una Intranet ….. 108
3.3.6 Tipos de Servicios para una Intranet ……. 111
3.4 Requerimientos Básicos de Seguridad y Disponibilidad de la Información……. 116
3.4.1 Aspectos Generales de la Seguridad de la Información 118
3.4.2 Políticas de Seguridad Informática……... 126
3.4.3 Modelo de Seguridad …….. 132
3.4.4 Servicios de Seguridad……. 133
3.4.5 Herramientas de Seguridad Disponibles…….. 136
3.5 Análisis Funcional de la Armada como Organización……. 143
3.6 Definición de Interacciones entre los Sectores de la Armada y sus Repartos Subordinados …….. 156
3.7 Escenarios Aplicables para: Repositorios de Información, 166

Mensajería, Publicación, Grupos de Discusión y Herramientas Colaborativas ……..
3.7.1 Sistemas de Información Propuestos…… 166
3.7.2 Repositorios de Información …….. 202
3.7.3 Publicación ……... 205

IV. DISEÑO DE LA INTRANET DE LA FUERZA NAVAL..... 220
4.1 Reglas para Guiar el Pensamiento del Diseñador de una Aplicación de Intranet ……. 213
4.1.1 Normas de Diseño de Aplicaciones…… 217
4.2 Diseño de la Arquitectura Lógica ……. 226
4.2.1 Conceptos Preliminares……. 227
4.2.2 El Mapa del Sitio …….. 233
4.2.3 El Mapa de Sombra ……. 237
4.2.4 Búsqueda General…….. 240
4.2.5 El Directorio de Búsqueda……. 241
4.2.6 El Índice de la Organización…….. 241
4.3 Desarrollo de Aplicaciones Centradas en el Web…….. 243
4.3.1 Evolución hacia la Arquitectura Centrada en el Web … 246
4.3.2 Java y el Ambiente de Aplicaciones Distribuidas…….. 260
4.3.3 Arquitecturas Distribuidas (Corba – RMI)…… 265
4.3.4 MVC (Patrón de Diseño)……. 272
4.3.5 Plataforma JAVA 2 Enterprise Edition…… 283
4.4 Diseño Macro de la Intranet, Distribución Física de los Servidores en los Data Center…….. 324
4.4.1 Diseño de la Intranet de la Armada…….. 326
4.4.2 Infraestructura Tecnológica de Procesamiento……..... 340
4.5 Diseño de la Red de Datos……. 347
4.5.1 Requerimientos Institucionales…..…… 351

4.5.2 Definición de las Zonas de Seguridad…… 355
4.5.3 Definición de las Capas de Servicios…….. 367
4.5.4 Desempeño y Disponibilidad Requerida…… 371
4.5.5 Restricciones de Comunicaciones Impuestas…… 373
4.5.6 Red de Campus de la Base Naval Sur (Guayaquil)…… 387
4.5.7 Redes de Campus Menores …….. 395
4.5.8 Redes de Área Local …….. 400
4.5.9 Red de Área Extendida …….. 401
4.5.10 Acceso a Internet…… 410
4.5.11 Centro de Operación de la Red (NOC)…… 420
4.5.12 Seguridad de la Infraestructura Tecnológica…… 424
4.5.13 Aplicaciones futuras de la red…… 435

V. IMPLEMENTACIÓN DE LA INTRANET PILOTO DEL INSTITUTO OCEANOGRÁFICO DE LA ARMADA..... 456
5.1 Definición y aplicación del marco de trabajo en la Intranet…… 457
5.2 Definición de roles, organismos, procedimientos y estándares para el manejo de la Intranet …… 460
5.2.1 Roles para Administración de la Intranet …… 461
5.2.2 Roles Organizacionales …….. 467
5.2.3 Servicios de la Intranet ……... 469
5.3 Implementación del Sistema de Información de Avisos a los Navegantes utilizando el Paradigma Orientado a Objetos en un Ambiente Intranet ……... 473
5.3.1 Finalidad del Proyecto …… 474
5.3.2 Propósito del Proyecto …… 474
5.3.3 Definición del SISNAV …… 474
5.3.4 Alcance del SISNAV …… 475
5.3.5 Solución Tecnológica del SISNAV …… 476

5.3.6 Entregables del SISNAV ……. 477
5.4 Infraestructura Tecnológica……. 477

VI. CONCLUSIONES Y RECOMENDACIONES..... 491

APÉNDICES

A Descripción de los Roles para el Desarrollo y Mantenimiento de la Intranet
B Elementos y Procesos de la Metodología de Desarrollo de Sitios Web
C Arquitectura Java 2 Enterprise Edition
D Plataforma Tecnológica de Procesamiento
E Plataforma Tecnológica de Conectividad
F Seguridad de Redes
G Procedimientos para Administración de la Intranet en INOCAR
H Documentación Técnica del Análisis y Diseño Aplicando el Paradigma Orientado a Objetos al Sistema Avisos a los Navegantes
I Manual de Usuario de SISNAV

BIBLIOGRAFÍA

INDICE DE FIGURAS

		Pág.
Figura 1.1	Proceso de Producción de Inteligencia Básica…….	10
Figura 1.2	Latencia Organizacional……	19
Figura 1.3	Inercia Organizacional……..	20
Figura 2.1	Modelo de Toma de Decisiones Distribuidas…….	39
Figura 2.2	Modelos de Control y Comunicación Centralizados y Distribuidos…….	41
Figura 2.3	Información del Tipo "Por Si Acaso" en el Modelo de Empuje…….	54
Figura 2.4	Los Primeros Modelos de Información en Demanda…	55
Figura 2.5	Información en Demanda Basada en el Modelo Clásico Cliente/Servidor…….	56
Figura 2.6	Información en Demanda Basada en el Cliente Universal……..	57
Figura 2.7	Marco de Trabajo de una Organización bajo una Intranet…….	69
Figura 2.8	Administración de la Información en una Intranet…….	81
Figura 2.9	Organismos para la Administración de una Intranet….	82
Figura 2.10	El Consejo Organizacional del Web…….	84
Figura 2.11	Comité Técnico del Web…….	86
Figura 2.12	Elementos Esenciales de una Intranet Organizacional	86
Figura 3.1	Elementos y Procesos de la Metodología de Desarrollo de Sitios Web……..	104
Figura 3.2	Aspectos Fundamentales de un Sistema de Información Seguro…….	119
Figura 3.3	Visión Global de la Seguridad de la Información en un Ambiente Informático…….	120

Figura 3.4	Diagrama para Análisis de un Sistema de Seguridad..	131
Figura 3.5	Encriptación con Claves Asimétricas……..	137
Figura 3.6	Representación de un Firewall…….	143
Figura 3.7	Organización de la Armada por Sectores……...	148
Figura 3.8	Propuesta de la Organización Informática en la Armada…….	155
Figura 3.9	Acciones Generales de la Comandancia General de Marina……..	156
Figura 3.10	Tareas Principales del Comandante General de Marina……...	157
Figura 3.11	Acciones Generales de la Dirección de Inteligencia Naval…….	158
Figura 3.12	Acciones Generales de los Órganos de Asesoramiento y Consejo…….	159
Figura 3.13	Tareas Principales del Estado Mayor de la Armada….	159
Figura 3.14	Tareas Principales de la Inspectoría General de la Armada…….	160
Figura 3.15	Tareas Principales del Comando de Operaciones Navales…….	161
Figura 3.16	Tareas Principales de la Secretaría del Comando General…….	162
Figura 3.17	Tareas Principales de la Dirección General del Personal……...	162
Figura 3.18	Tareas Principales de la Dirección de Educación…….	163
Figura 3.19	Tareas Principales de la Dirección General de Finanzas……...	164
Figura 3.20	Tareas Principales de la Dirección General del Material…….	164
Figura 3.21	Tareas Principales de la Dirección General de	165

	Intereses Marítimos……	
Figura 3.22	Tareas Principales de la Dirección General de Marina Mercante y del Litoral……	166
Figura 3.23	El Cuadro de Mando Integral como Estructura para Transformar una Estrategia en Términos Operativos..	168
Figura 3.24	El Cuadro de Mando Integral como un Marco Estratégico para la Acción……	168
Figura 3.25	Modelo Funcional de Oracle Collaboration Suite……..	171
Figura 3.26	Modelo Esquemático del Portal de la Armada……..	174
Figura 3.27	Ciclo de Gestión del Conocimiento…….	176
Figura 3.28	Mantenimiento Asistido por Computador…….	179
Figura 3.29	Modelo Conceptual del Subsistema de Abastecimiento del Sistema Logístico Naval…….	182
Figura 3.30	Diagrama Esquemático del Paradigma Portal……..	192
Figura 3.31	Sitio Web del Sistema de Educación a Distancia de la Academia de Guerra Naval……..	194
Figura 3.32	Sitio Web de la Dirección General de Intereses Marítimos……	199
Figura 3.33	Sitio Web del Instituto Oceanográfico de la Armada…	199
Figura 4.1	Cuadros funcionales de la infraestructura de una aplicación para una Intranet……..	218
Figura 4.2	Arquitectura Lógica de la Información…….	232
Figura 4.3	El Mapa del Sitio……..	234
Figura 4.4	Estructura Final de la Arquitectura Lógica de la Información……..	243
Figura 4.5	Aplicaciones Monolíticas de los años 80…….	246
Figura 4.6	Aplicaciones Cliente – Servidor Clásico de inicios de los años 90……..	248
Figura 4.7	Aplicaciones de tres capas de finales de los años 90..	254

Figura 4.8	Aplicaciones de “N” Capas…….	256
Figura 4.9	Arquitectura centrada en red de una aplicación típica de una Intranet…….	257
Figura 4.10	Oracle Network Computing Architecture…….	259
Figura 4.11	Esquemático de una Arquitectura Distribuida…….	262
Figura 4.12	Estructura del Ambiente de Desarrollo y Ejecución en Java……...	264
Figura 4.13	Componentes de la Arquitectura CORBA……..	268
Figura 4.14	Principio de diseño Model-View-Controller…….	274
Figura 4.15	Diálogo en Patrón Diseño Model–View–Controller…..	275
Figura 4.16	Diálogo en Patrón Diseño Model–View–Controller…..	276
Figura 4.17	Ejemplo del Patrón Diseño Model–View–Controller….	277
Figura 4.18	Aplicación del Patrón Diseño MVC a un Aplicación Web……...	278
Figura 4.19	El Efecto Iceberg en los Costos Ocultos del Mantenimiento del Software…….	280
Figura 4.20	Diagrama de Bloque de una Aplicación J2EE……...	284
Figura 4.21	Modelo de Aplicación J2EE……..	285
Figura 4.22	Componentes Web de una Aplicación J2EE…….	290
Figura 4.23	Componentes de Negocio EJB de Aplicación J2EE….	291
Figura 4.24	Tipos de Contenedores en Especificación J2EE……..	295
Figura 4.25	Roles en la Especificación J2EE…….	301
Figura 4.26	Elementos de la Plataforma J2EE……...	306
Figura 4.27	Implementación del Patrón de Diseño MVC en la Plataforma J2EE…….	307
Figura 4.28	Modelo de Operación de la Tecnología EJB……..	309
Figura 4.29	Representación de un Componente EJB del Tipo Entity Bean……..	312
Figura 4.30	Modelo de Operación de SOAP/UDDI/WSDL…….	319

Figura 4.31	Modelo de Operación de ebXML…….	321
Figura 4.32	Modelo de Operación de servicios web sobre J2EE…	323
Figura 4.33	Cluster con Balanceo de Carga en Capas Intermedias con Switches de Capa 4 – 7……..	336
Figura 4.34	Cluster de Recuperación de Fallos con Cold Failover.	339
Figura 4.35	Cluster de Recuperación de Fallos con Hot Failover…	339
Figura 4.36	Infraestructura Tecnológica de Procesamiento de la Zona Desmilitarizada Pública – Internet Servers……..	342
Figura 4.37	Infraestructura Tecnológica de Procesamiento de la Zona Desmilitarizada Privada – Intranet Servers……..	344
Figura 4.38	Infraestructura Tecnológica de Procesamiento y Almacenamiento de la Zona Militarizada – Data Center Servers…….	345
Figura 4.39	Definición de las Zonas de Seguridad…….	366
Figura 4.40	Definición de las Capas de Servicios en las Zonas de Seguridad…….	369
Figura 4.41	Diagrama Lógico, Capas de Servicios y Zonas de Seguridad…….	375
Figura 4.42	Diagrama Lógico, Capas de Servicios, Zonas de Seguridad y Roles de Red…….	382
Figura 4.43	Equipos de Red para el Data Center……..	387
Figura 4.44	Capa de Distribución de la Red de Campus de la Base Naval Sur……...	390
Figura 4.45	Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur…….	391
Figura 4.46	Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa……..	392
Figura 4.47	Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector Noroccidental y Edificio de	393

	la Dirección General del Personal…….	
Figura 4.48	Red Inalámbrica Tipo NLOS para las Unidades de Superficie y Submarinas…….	395
Figura 4.49	Red de Campus de la Comandancia General de Marina y Acceso a la Red Naval de Datos…….	396
Figura 4.50	Red de Campus de la Base Naval Norte y Acceso a Internet y a la Red Naval de Datos……..	398
Figura 4.51	Red de Campus de la Base Naval de Salinas y Acceso a Internet y a la Red Naval de Datos…….	399
Figura 4.52	Topología Física de la Red de Área Extendida con Dependencia del Nodo Guayaquil (CETEIG) – Región Suroccidental……..	404
Figura 4.53	Topología Física de la Red de Área Extendida con Dependencia del Nodo Quito (CETEIQ) – Región Nororiental…….	405
Figura 4.54	Esquema de Acceso de los Repartos con Enlaces ISDN a la Red Naval de Datos…….	406
Figura 4.55	Esquema de Acceso de los Repartos con Enlaces Seriales por el Sistema Multiacceso a la Red Naval de Datos……..	407
Figura 4.56	Esquema de Interconexión de Quito – Guayaquil a través del Enlace E1……..	408
Figura 4.57	Esquema de Acceso en Demanda a través de Servidores de Acceso…….	409
Figura 4.58	Modelo Funcional de los Mecanismos de Seguridad de la Red Naval de Datos y Acceso al Internet…….	417
Figura 4.59	Modelo Esquemático del Centro de Operación de la Red Naval de Datos……..	423
Figura 4.60	Visión Global de la Seguridad Informática…….	427

Figura 4.61	Comparación de Capacidades entre Internet 2 y Diferentes Tecnologías del Internet Actual……	439
Figura 5.1	Mapa de Procesos Intranet INOCAR……..	460
Figura 5.2	Asignación de Roles a Procesos Intranet……...	466
Figura 5.3	Infraestructura Tecnológica de Procesamiento de la DMZ Pública del INOCAR……	480
Figura 5.4	Infraestructura Tecnológica de Procesamiento de la DMZ Privada del INOCAR……	481
Figura 5.5	Infraestructura Tecnológica de Procesamiento de la Zona Militarizada del INOCAR……	481
Figura 5.6	Distribución Organizacional y de Edificio del INOCAR.	482
Figura 5.7	Diagrama Esquemático de la Red de Datos Implementada en el INOCAR……..	484
Figura B.1	Puntos de Verificación para el Proceso de Análisis…..	B-10
Figura B.2	Verificación de la Integridad del Propósito, Objetivos y Especificaciones para un Sitio Web…….	B-13
Figura B.3	Técnicas de Promocionamiento de un Sitio Web……..	B-26
Figura C.1	Modelo de Operación de JDBC…….	C-2
Figura C.2	Modelo de Operación de JNDI…….	C-3
Figura C.3	Modelo de Operación de la Tecnología EJB……..	C-9
Figura C.4	Modelo de Operación de un Entity Bean…….	C-15
Figura C.5	Modelo de Operación de los Servlets…….	C-21
Figura D.1	Ciclo de Seguridad de Redes……..	D-14

INDICE DE TABLAS

		Pág.
Tabla I	Patrones de Evolución de la Información……..	15
Tabla II	Comparación de la Actitud de los Productores de Información en los Modelos de Empujar y Halar ……..	49
Tabla III	Comparación de la Actitud de los Usuarios de Información en los Modelos de Empujar y Halar ……..	51
Tabla IV	Sistema de Planificación Institucional de la Armada…	145
Tabla V	Comparación de Estructuras y Entornos ……..	251
Tabla VI	Cambios en un Mundo Distribuido……..	251
Tabla VII	Nuevos Retos para Tecnología de Información…….	252
Tabla VIII	Categorías de los Servicios de CORBA…….	269
Tabla IX	Tareas a Cargo de Contenedores y Componentes…..	297
Tabla X	Tecnologías e Interfaces de Programación de Aplicaciones (APIs) que Conforman la Plataforma J2EE…….	301
Tabla XI	Capas de Servicios…….	367
Tabla XII	Requerimientos de Disponibilidad de Servicios…….	371
Tabla XIII	Niveles de Desempeño de las Zonas de Servicios…..	372
Tabla XIV	Roles de Red por Segmento…….	374
Tabla XV	Segmentación Propuesta……..	377
Tabla XVI	Equipos de la Infraestructura Informática de Procesamiento del INOCAR…….	485
Tabla D-I	Equipos para Servicios Públicos de Internet (Zona Desmilitarizada Pública)…….	D-1
Tabla D-II	Equipos para Servicios Privados de Intranet (Zona Desmilitarizada Privada) ……..	D-4

Tabla D-III	Equipos para Servicios de Almacenamiento de Información (Zona Militarizada)…….	D-9
Tabla E-I	Equipos de Red Previstos para el Data Center…….	E-1
Tabla E-II	Equipos de Red de la Capa de Distribución de la Red de Campus de la Base Naval Sur…….	E-3
Tabla E-III	Equipos de Red de la Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur….	E-5
Tabla E-IV	Equipos de Red de la Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa…….	E-7
Tabla E-V	Equipos de Red de la Capa de Acceso a la Red de Campus de la Base Naval Sur desde el Sector Noroccidental y del Edificio de la Dirección General del Personal…….	E-9
Tabla E-VI	Equipos para la Red de Campus de la Comandancia General de Marina y Acceso a la Red Naval de Datos	E-11
Tabla E-VII	Equipos para la Red de Campus de la Base Naval Norte y Acceso a Internet y a la Red Naval de Datos..	E-13
Tabla E-VIII	Equipos para la Red de Campus de la Base Naval de Salinas y Acceso a Internet y a la Red Naval de Datos…….	E-14
Tabla E-IX	Equipos para la Red de Área Extendida para Repartos con Enlaces Dedicados ISDN para Acceso a la Red Naval de Datos…….	E-15
Tabla E-X	Equipos para la Red de Área Extendida para Repartos con Enlaces Seriales por el Sistema Multiacceso a la Red Naval de Datos…….	E-16
Tabla E-XI	Equipos para la Interconexión de Quito – Guayaquil a través del Enlace E1 en la Red Naval de Datos…….	E-18

INTRODUCCIÓN

Con el crecimiento acelerado y el vertiginoso ritmo con el que los avances tecnológicos evolucionan especialmente en las áreas relacionadas directa e indirectamente con la tecnología de información, cada vez un número mayor de organizaciones se ven en la necesidad de utilizar las tecnologías de Internet y del web para soportar los procesos principales que les permite cumplir de una manera más efectiva su misión.

La base de la competitividad, creación de riqueza y uso óptimo de los recursos en la nueva economía digital es el potenciamiento de estrategias modernas de dirección y administración como la calidad total, la reingeniería de procesos, la toma efectiva de decisiones y la planificación situacional a niveles antes imposibles de alcanzar, gracias al buen uso de la información, lo que permite a las organizaciones innovar creando modelos de operación y procesos mucho más eficientes que sus antecesores.

En la medida que el mundo se ha movido del paradigma tipo broadcast al paradigma interactivo, los cambios de todas nuestras estrategias, técnicas y metodologías han sido más drásticos y profundos. En la economía emergente, hay una nueva infraestructura basada en el Internet, que es la causa principal de dejar a un lado muchas de las suposiciones típicas del

mundo en que se desenvuelven las organizaciones tradicionales y caducas. En la medida en que las redes se vuelvan ubicuas, robustas y posean el ancho de banda suficiente cubriendo al planeta, en las organizaciones tendrán que emerger rápidamente nuevos modelos de cómo operar y desenvolverse en los nuevos escenarios nacidos en esta nueva economía.

El Internet ha cambiado la forma de competir, la velocidad de las acciones y la naturaleza del liderazgo. El Internet está aquí y para un buen tiempo, muy pocas sociedades y organizaciones serán inmunes a este nuevo fenómeno tecnológico. Muchos se han inquietado ante esta nueva realidad, surgiendo términos adaptados como el e-business, e-commerce, e-markets, e-procurement, e-goverment; todos quieren estar ahí, pero la pregunta es: ¿Qué camino nos llevará al éxito en la nueva economía digital? ¿Cuáles son los pasos que debo dar para tener una navegación segura que me lleve al destino triunfal? ¿Cuáles son las características de las aplicaciones empresariales de la próxima generación? ¿Cómo las puedo hacer útiles para mí?

El propósito de éste trabajo es diseñar la infraestructura técnica, administrativa y organizacional que soporte un sistema de administración de información de la Armada basado en una Intranet, una red privada basada en la tecnología del Internet.

Para alcanzar la meta propuesta nos trazamos los siguientes objetivos específicos que a lo largo de la tesis los vamos desarrollando en cinco capítulos teóricos, conceptuales, de investigación y de implantación práctica que demuestran como la tecnología bien aplicada puede apoyar la gestión efectiva y eficiente de una organización como la Armada:

- Definir las necesidades para la organización y administración de la información formal de la Armada justificando el uso de la tecnología de Intranet.

- Definir las políticas, estándares y arquitectura para la elaboración de sistemas de información basados en Web a nivel de la Armada en un plan estratégico que contemple el marco de futuros desarrollos informáticos.

- Definir los requerimientos básicos de infraestructura tecnológica, seguridad y disponibilidad que permitan un control centralizado sobre los sistemas de información.

- Analizar, diseñar e implementar un Sistema de Información Oceanográfico basado en tecnología de Intranet.

En el capítulo I, se resalta la importancia de la información y su rol en la evolución de la organización. Se describe el impacto de la tecnología al fomentar las superautopistas de información, detallando el potencial del Web

como el medio de comunicación que revolucionará la forma que las organizaciones deberán funcionar. Para esto se detallan aspectos fundamentales a ser considerados, a manera de metas, que permitan adoptar una actitud organizacional acorde a la presente era digital.

En el capítulo 2, se describe formalmente la tecnología de Intranet buscando un enfoque estratégico para su uso. Se determina que paralelamente a la adopción de la tecnología se demanda una reforma organizacional para afrontar los nuevos paradigmas. Se justificará la necesidad de una descentralización de la toma de decisiones, permitiendo la centralización de la comunicación y del control a través de la Intranet. Se define también el significado de las actividades conducidas por propósito, la importancia de habilitar a la organización con una herramienta que permita compartir la información, en base a lo cual se pueda innovar para tener una institución que aprende continuamente, orientada permanentemente al mejoramiento continuo y a la búsqueda de la excelencia. Trata también el problema de la sobrecarga de información y, analizando la tecnología de push y pull se consideran alternativas para enfocar la información en demanda. Finalmente se definen los roles, organismos y el marco de trabajo de una organización bajo una Intranet.

En el capítulo 3, se define el esquema de la organización de la información que se manejará electrónicamente; se describe una metodología para la definición de una arquitectura lógica de la información en la Intranet. Se hace un análisis funcional de la Armada, con el objetivo de determinar las interacciones entre los sectores y repartos que permitirá entender el flujo de la información en la Institución.

En el capítulo 4, se define los diferentes tipos de aplicaciones que podría tener el Intranet con el propósito de sugerir a la Armada en qué escenarios sería aplicable su uso. Definiendo las nuevas arquitecturas y patrones de diseño que guían el desarrollo del software y aplicaciones empresariales de una organización. Para ello se define la infraestructura tecnológica requerida y las necesidades de enlaces de comunicaciones.

El capítulo 5 es práctico, se implementa una Intranet piloto en el Instituto Oceanográfico de la Armada, definiendo roles, procedimientos y estándares para su manejo, así como un sistema de información que accede a una base de datos a través del Web; el sistema se diseñó basado en el paradigma orientado a objetos siguiendo la referencia UML e implementado con el lenguaje orientado a objetos JAVA.

CAPITULO 1

1. CONSIDERACIONES BÁSICAS SOBRE EL MANEJO ADECUADO DE LA INFORMACIÓN

En este Capítulo se resalta la importancia de la información en la Armada como elemento fundamental para la efectiva toma de decisiones en la conducción de las operaciones militares, así como en la gestión que permite alcanzar el alistamiento para éstas; estas decisiones deben ser necesariamente canalizadas a través de cadenas jerárquicas de mando para el control de los teatros de operación y los cuadros de situación en el ámbito administrativo. Se describe la evolución y el impacto de la nueva era tecnológica que fomentan las superautopistas de información y que les permiten a los mandos directivos disponer de cuadros de situación mas completos y precisos con los cuales pueden resolver en menor tiempo las acciones que ameritan tomarse y delegarse para su ejecución. Se destacan los beneficios que la nueva era de la información, y en forma

específica el potencial del web, aportará a las organizaciones conducidas por propósitos.

1.1 Importancia de la Información en el Ámbito Militar

Para analizar cual es la importancia de la información para una Fuerza Naval en un país que enfrenta constantes amenazas externas e internas en las puertas del nuevo siglo, hay que entender el efecto que tiene la tecnología en el equipamiento de los ejércitos. Las grandes velocidades, las armas de largo alcance, los lanzamientos transhorizonte, la guerra electrónica, los satélites de vigilancia, la informática y otros ingenios han tenido dos grandes efectos en las operaciones militares:

1. Ha aumentado la cantidad de información que debe ser procesada e intercambiada, a veces en forma casi instantánea, para la toma acertada de decisiones.
2. Se ha acortado el tiempo disponible para esa toma de decisiones.

Para solucionar este problema de contar con un tratamiento ágil, oportuno y adecuado de la información, de modo que se apoye efectivamente a la toma de decisiones del Comando, inicialmente se integraron todos los sistemas a nivel de *"buque"*, a continuación a nivel de *"fuerza"*, luego a nivel de *"área de operación"* hasta llegar a un nivel

amplio y total de integración de todos los *"teatros de operación: aéreo, terrestre y marítimo"* [1].

Esta capacidad coordinadora se ha obtenido gracias a los avances tecnológicos y la integración de las telecomunicaciones con la informática, dando paso a la telemática, definiendo lo que se conoce en el área militar como *"Sistemas integrados de mando y control"* [2].

Por muy sofisticados que sean los sensores y sistemas de armas con que cuente una fuerza, éstos pueden ser anulados por los de una fuerza más débil, si no se satisfacen algunos requerimientos del Sistema Integrado de Mando y Control [2].

- Las decisiones deben ser divulgadas a través de una cadena de MANDO y tomadas en el nivel más conveniente.
- La autoridad responsable debe ser capaz de ejercer el CONTROL de su área jurisdiccional, sus órganos de maniobra, sus unidades o buques, según sea pertinente.
- Las órdenes e informaciones deben ser transmitidas a la persona precisa, en el tiempo correcto, con la seguridad requerida, a través de un eficiente sistema de COMUNICACIONES.
- La INFORMACIÓN necesaria, en cantidad, calidad y oportunidad, debe ser procesada, presentada y divulgada.

1.2 Definición de un sistema de mando y control

Un sistema de mando y control es un conjunto de elementos, equipos, hombres y procedimientos, que permiten al Mando en sus variados niveles, disponer oportunamente de toda la información que lo capacita para tomar decisiones, y difundir sus órdenes a sus unidades ejecutoras, fuerzas amigas y superiores [2].

Un sistema de mando y control, no puede ser analizado tácticamente como un sujeto aislado, sino que debe ser considerado como parte integrante de los elementos básicos de combate, junto con la potencia ofensiva, capacidad defensiva y movilidad. Estos elementos, concurren como un todo indivisible en procura del "arte de crear y mantener condiciones favorables para obtener la mayor eficacia en el empleo de los medios". A pesar de ser cuatro los elementos, el de mayor importancia relativa es el sistema de mando y control, por cuanto permite al hombre responsable de tomar decisiones, emplear con voluntad inquebrantable los otros elementos de combate para someter al enemigo y obligarlo a actuar de acuerdo a nuestras propias intenciones.

Un sistema de mando y control debe disponer de medios que le permitan realizar las siguientes operaciones [2]:

- Obtener información y almacenarla.
- Establecer el panorama en el campo táctico.
- Evaluar sus objetivos y las amenazas.
- Ayudar a la toma de decisiones, sugerir sistemas de armas activos o pasivos a utilizar, y acciones a ejecutar.
- Controlar y/o cooperar en la acción de otros sistemas, como por ejemplo: sistemas de guerra electrónica, sistemas de armas, sistemas sensores, etc.
- Intercambiar y diseminar la información en tiempo real.

Para cumplir las operaciones antes enumeradas, los sistemas de mando y control normalmente se subdividen en cuatro subsistemas [2]:

1. Subsistema de obtención de información.
2. Subsistema procesador de información.
3. Subsistema de presentación.
4. Subsistema de comunicaciones.

La información es por tanto un elemento fundamental en el cumplimiento de la misión de la Fuerza Naval, en todos sus niveles de operación: estratégico, táctico y operacional; el manejo óptimo de ésta con los medios disponibles a través del uso adecuado de la tecnología de información es una meta organizacional.

1.3 Proceso de Obtención de Información

Dentro del contexto de los sistemas de mando y control, definiremos la información como el elemento que alimenta las diferentes funciones o tareas necesarias para que la organización opere: la compilación del panorama táctico, evaluación de objetivos y amenazas, ayuda a la toma de decisiones y cooperación a la acción de los sistemas de armas. Para que cada función o tarea se lleve a cabo debe apoyarse en información previamente procesada, que normalmente se conocerá como *"Inteligencia básica"* dentro de un proceso como se muestra en la Figura 1.1 [2].

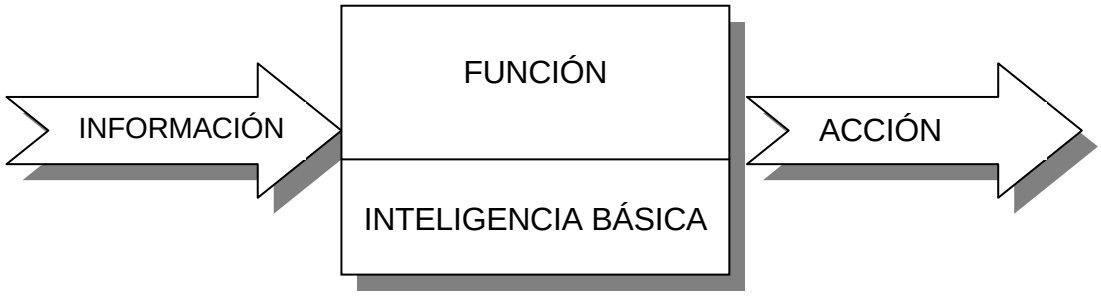


FIGURA 1.1. PROCESO DE PRODUCCIÓN DE INTELIGENCIA BÁSICA

La recolección de información así como su posterior procesamiento y diseminación es fundamental, por tanto es una actividad constante, amplia y de una profundidad tal que no se limita al panorama táctico, sino a todos los niveles de operación de una fuerza. La información o inteligencia son los ojos de las operaciones [2].

Este es un ejemplo claro de que hay distintos enfoques y circunstancias en que la información conduce las funciones y no solo las funciones producen información.

En la era de la información, donde los medios electrónicos han permitido desarrollar las superautopistas de información, es necesario encontrar el enfoque adecuado para poder explotar a este conjunto de elementos en forma óptima, convirtiéndolos en parte integrante de los subsistemas de obtención, procesamiento, presentación y comunicación de información, alcanzando el Sistema de Mando y Control, una profundidad en todos los niveles de operación de la Fuerza [1].

1.4 La Era de la Información

Para describir la era de la información revisaremos el paradigma operacional en que ésta se basa, *"Distribuir la información disponible, de modo que se genere nueva información de mejor calidad que la predecesora".* Para entender el modelo de este paradigma, vamos a revisar una teoría de patrones de evolución de la información conocida como *Bionímica* de Michael Rothschild [3].

Las primeras manifestaciones de patrones de información fueron codificaciones en fórmulas químicas orgánicas (cadenas nucleicas), a

partir de las cuales surgieron las formas más precarias de vida, se evolucionó poco a poco para dar paso al DNA, produciendo más y mejor información. Estas formas lograron ser más eficientes y alcanzar la capacidad reproductora, formándose una estructura organizacional ocasionando la primera revolución en la generación de información. La evolución fue en este caso la membrana nuclear, la revolución la reproducción sexual [3].

La mezcla de información crea nueva información que no existía en ningún sistema anterior.

Posteriormente, con la aparición de los primeros seres pensantes (el homo sapiens), estructuras más complejas ya tenían la ventaja de heredar genética y socialmente en muchos casos la cultura y costumbres; la búsqueda por mejorar y subsistir genera una serie de mecanismos capaces de crear información en mayor escala, a punto que al aparecer los primeros mecanismos de escritura metódica nace la información intelectual.

Con el paso del tiempo, en el siglo XV, las barreras del espacio (geografía) y tiempo, limitaban la capacidad de compartir ideas y conocimientos. Aún cuando la comunicación escrita era mejor que la verbal para estos propósitos, las posibilidades se limitaban al número de copias disponibles del escrito. Elaborar una copia era un proceso

lento y tedioso a tal punto que existía para tales propósitos oficios especializados, los "escribanos". El poseer el conocimiento, era una fuente de poder y prestigio limitado a unos pocos privilegiados.

En 1450, acontece otra revolución de la información, Gutenberg inventa la prensa mecánica de impresión y con ello el poder de crear y difundir información creció exponencialmente. La tecnología es evolucionaria, puesto que era algo relativamente fácil de hacer una vez que el ingenio facilita los planos; sin embargo el efecto organizacional y social fue en sí la revolución. De repente, ideas y conocimiento podían ser ampliamente distribuidos, pero en cantidad, surgiendo la necesidad de identificar y validar la calidad de la información, el mecanismo para ello sería "el método científico" y el nombre con que se le conoce a este período es "la revolución científica" [4].

La nueva información producida por la revolución científica, tomó forma con los inventos mecánicos y físicos de la "revolución industrial"; además la imprenta permitió desarrollar la educación pública, la democracia y a fortalecer los principios fundamentales del humanismo como son: libertad, igualdad y fraternidad. La humanidad y la cultura se transformaron radicalmente, debido a la mezcla de ideas que la imprenta de Gutenberg originó [4].

Luego de la revolución industrial, con las semillas que está dejó vino la siguiente escena, "la era electrónica". Dentro de este progreso constante, el advenimiento del World Wide Web parece ocupar una posición similar a la que ocupó la imprenta de Gutenberg en su época. Esta evolución nos ha puesto en el comienzo de la escena de una nueva revolución, la que afectará todos los aspectos de nuestras vidas, desde el cómo se hacen los negocios, hasta el cómo se gobierna; los efectos serán en lo personal, en lo organizacional y en lo social.

En la Tabla I se resume los principales hechos hasta aquí enunciados, clasificándolos en fenómenos biológicos, técnico mecánicos y técnico electrónicos. Cómo se puede evidenciar en esta tabla, las fases de la evolución tienen un patrón muy particular, cada vez los avances alcanzados constituyen un adelanto que no es propio de la fase en que estos se basan, sino que son un resultado sinérgico de todo lo evolucionado hasta ese punto.

TABLA I

PATRONES DE EVOLUCIÓN DE LA INFORMACIÓN [4]

Evento	1ra.Explosión de la información	2da.Explosión de la información	3ra.Explosión de la información	4ta.Explosión de la información	5ta.Explosión de la información	6ta.Explosión de la información
Biológico						
Formación de la tierra (4600 ' de años)	1ra. Cadena nucleica (4200 a.)	Aparición del DNA (4000 a.)	Célula con núcleo (1500 a.)	Comienza la reproducción sexual (900 a.)	Explosión Cambrian	Aparición del primer Hominido
Mecánico						
Aparición del moderno Homo sapiens (200mil años)	Primeros escritos paleolíticos (35000 a.)	Escritos de sumarios por antiguos escribanos (5000 a.)	Primera prensa de impresión (Gutenberg) (535 a.)	Comienzo de las ciencias (475 a.)	Revolución industrial (190 a.)	Comienzo de la era electrónica (100 a.)

Electrónico				
Computador digital (55 años)	Programas de Sofware (45 a.)	Networking (redes de computadoras) (30 a.)	Worl Wide Web (3 a.)	**La nueva era de la información**

Es decir, esto prueba que se ha creado más y mejor información que las fases antecesoras. Es importante también considerar, que los lapsos de tiempo que toma una fase para evolucionar, cada vez son más cortos. Podemos comparar por ejemplo, que las primeras computadoras tardaron 55 años para evolucionar, las primeras redes de computadoras 33 años, luego tan solo pasaron 3 años para que evolucionara el World Wide Web, y ponernos en la puerta de entrada a una nueva era, “La Era de la Información” [4].

Ya se ha evidenciado que los antiguos controles de información han fracasado para esta nueva era. Hay que redefinir nuestras estructuras contestando las siguientes preguntas: ¿Cómo voy a acceder a la información? ¿Cómo voy a controlar el acceso a la información? ¿Quién decide que información debe ser controlada? ¿Cómo voy a

saber que calidad de información tiene el web de la organización? ¿Cómo voy a mantener la explosión de generación de información?

Ya estamos viviendo la era de la información, y es urgente para ello adoptar una actitud adecuada que nos permita encontrar un enfoque correcto de nuestra visión, misión y objetivos acordes con esta era.

1.5 La Información Influye en la Evolución de la Organización

¿Cuáles son los factores que nos obligan a adoptar un nuevo enfoque de cara al nuevo siglo y a la era de la información? Como cualquier cosa en el mundo en la medida que crece, se complica. Una organización, cuando crece (escalabilidad), se enfrenta especialmente a las siguientes complicaciones [4]:

- ✓ Latencia organizacional.
- ✓ Inercia.
- ✓ Deformación.

De estas quizás la más crítica es la latencia organizacional o "relación superficie versus volumen" no adecuada. Un ejemplo práctico que nos ayuda a comprender este principio es cuando necesitamos preparar bastantes papas fritas en un tiempo relativamente corto, para lograrlo debemos cortar las papas en trozos muy pequeños, mientras más

pequeños sean los trozos, más rápido se cocinarán. Esto se debe a que el centro de un trozo pequeño, está más cerca de la superficie en contacto con el aceite hirviendo que el centro de un trozo grande. Tienen una relación adecuada de superficie vs. volumen.

Este principio se aplica también en las organizaciones, si nos imaginamos a una organización como una esfera, y vemos a la vista superior de la esfera como aquella porción de la organización que reacciona para interactuar con sus clientes y su mercado, mientras que el volumen de la esfera representa el tamaño y la complejidad de toda la organización, y el radio de esta esfera, representa el número de capas que la organización tiene; en la medida que la vista superior tiene que crecer como consecuencia de un cambio en el mercado o aumento de éste, el volumen también debe crecer para soportar el aumento de la superficie de ésta vista superior. En ausencia de un cambio estructural, el volumen deberá crecer al cubo mientras que la superficie crece al cuadrado, en relación al aumento lineal de capas en la organización, representado por el crecimiento del radio. Esto crea un límite natural de crecimiento para que una organización pueda ser efectiva [4].

La Figura 1.2 muestra la situación de muchas organizaciones hoy en día, las que están orientadas a un crecimiento sostenido en ausencia de cambios estructurales ocasionando una mala relación de superficie vs.

volumen de 2:4:8. "Las capas organizativas (radio) tendrán que duplicarse, la complejidad y tamaño de la organización (volumen), crecerá 8 veces más rápido, para soportar una expansión o crecimiento del mercado (área) al doble de lo original, de 2 a 4". La causa principal de éste fenómeno es que las organizaciones típicamente mantienen una estructura piramidal, con un modelo de gestión con toma de decisiones centralizadas [4].

FIGURA 1.2. LATENCIA ORGANIZACIONAL

La segunda implicación con que tratar al momento de enfrentar la escalabilidad es la ***inercia.*** Como se representa en la Figura 1.3, una organización grande, tiene más puntos que coordinar, hay más capas que la información debe atravesar en las dos vías (burocracia), tanto al

adquirir los datos como al informar el curso de acción a tomarse, por lo que se vuelve lenta para reaccionar. A esto hay que añadir la enorme cantidad de datos adquiridos que deben ser analizados por la dirección central por lo que el comportamiento de una organización en esta situación resulta muchas veces incomprensible. La solución adoptada en muchos casos ha sido la reducción de capas administrativas, eliminar mandos medios y organismos de soporte; pero esto no resuelve el problema. Recuerde que una vista superior tiene que tener un volumen apropiado para soportarla. Sin el volumen, la superficie se deformaría y colapsaría. Aún la existencia de sistemas informáticos que aligerarían el tiempo para la toma de decisiones, no resolverían el problema, mientras la toma de decisiones esté centralizada [4].

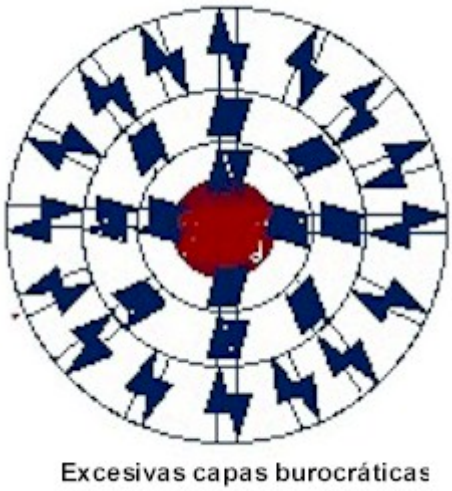


FIGURA 1.3 INERCIA ORGANIZACIONAL

La tercera implicación que las organizaciones enfrentan durante la escalabilidad, es la ***deformación.*** Si el volumen crece dos veces más rápido que la superficie, la gravedad empieza a deformar la estructura de la superficie. Cuando una organización comienza a crecer, empieza a mostrar síntomas de deformación, especialmente debido a la ruptura de la comunicación. Esto se manifiesta de diferentes formas, como estrés interno (conflicto dentro de los grupos de trabajo), rigidez en la organización (actividades burocráticas no saludables) y pérdida del control de la organización. Resultado de esto, vemos que existe un límite natural de crecimiento para las organizaciones que centralizan la toma de decisiones [4].

Los comandos y direcciones esperan que una nueva tecnología aumente tanto la productividad organizacional como la productividad personal. Esperan mejorar los elementos que permitan tomar mejores decisiones, mejorar la calidad de la información así como hacer de esta algo más visible.

Es aquí donde la tecnología se torna en una importante herramienta. Las comunicaciones electrónicas disponibles con las redes de datos de alta velocidad, gran ancho de banda y amplio alcance, facilitan el manejo de nuevos paradigmas, como el de mando y control distribuido en cuanto a la capacidad de toma de decisiones, y una estrecha

comunicación y coordinación centralizada, los que cubren las necesidades del entorno organizacional actual.

En el pasado, el uso de supercomputadores o mainframes, basaba todo el computo real en un computador compartido; en el modelo clásico cliente servidor, en el que se utiliza accesos remotos por parte de clientes, a una base de datos en un servidor, la tecnología se basa en la generalización de la diversidad, haciéndola ver similar en un esquema estructurado, y ésta no es la respuesta final a los problemas de cómo tratar eficientemente a la información, especialmente porque se dedican a centralizar el control en una base de datos, y por tanto la toma de decisiones permanece centralizada, las herramientas de trabajo en grupo o "groupware", por otra parte, aún carecen de estándares abiertos y se centran en las tecnologías propietarias. La única innovación que enfrenta eficientemente un nuevo y adecuado modelo donde la toma de decisiones es distribuida y tiene una comunicación y coordinación centralizada es el Web. La tecnología en que se basa el Intranet/Internet está inspirada en un modelo de toma de decisiones distribuidas. Las decisiones que permiten al Internet cumplir su función son tomadas en subsistemas independientes auto-regulables, en vez de centralizarse en el punto de origen del mensaje o algún coordinador/controlador central. Si bien es cierto el modelo para su arquitectura es el cliente/servidor, éste ha sido redefinido, y a diferencia

de las aplicaciones cliente/servidor clásicas, la única aplicación que se requiere instalar en la estación cliente es un navegador web, lo que se hace una sola vez, puesto que las aplicaciones desarrolladas se encuentran instaladas íntegramente en el servidor web, o en uno o más servidores corporativos de aplicación, aplicando el concepto del cliente universal (navegador web), y minimizando considerablemente la administración de las estaciones clientes en un ambiente distribuido, donde no se requiere volver a instalar más software especial [4], [7], [11].

La tecnología web es diferente a los esquemas tradicionales de otras épocas. Es fácil de utilizar, fácil para publicar información y fácil para acceder a la información. Así que cualquier cliente con acceso a la red puede publicar o acceder a la información disponible en cualquier plataforma de la red. Adicionalmente, gracias a la acogida que ha tenido el modelo de desarrollo para una arquitectura basada en web, el desarrollo de aplicaciones web es más fácil que con los enfoques tradicionales de aplicaciones. Una analogía similar sería comparar la explosión de los sistemas de escritorio dada la revolución de los microprocesadores. En este caso estamos enfrentando a una administración de información distribuida y no una computación distribuida [4], [7], [11].

Los beneficios que se obtienen con el web son mejorar la comunicación y permitir a la organización innovar. Una buena comunicación permite mejorar la toma de decisiones, la productividad y la eficiencia. Tal como la imprenta de Gutenberg fue un gran habilitador de nuevas oportunidades, permitiendo a las personas comunes publicar y leer información en papel, el web rompe las barreras para que la persona común pueda publicar y leer información en el mundo de la información electrónica.

La publicación electrónica aumenta la velocidad y el alcance de la producción de información de modo que ésta fluya por todas las extensiones de la organización a un grado imposible de alcanzar con medios impresos en papel. La tecnología web hace que la publicación electrónica sea fácil, barata y accesible para una persona común, también mejora el acceso a la información basándose en la metáfora de apuntar y seleccionar, generalmente no se requiere de comandos ni menús, sino de un buen diseño de una arquitectura lógica de la información en los sitios web habilitando un acceso no lineal a información no estructurada, y por tanto diversa, de acuerdo a los intereses y necesidades de los usuarios. Pero estas mejoras son solo los habilitadores de una evolución. El hacer de la información algo más visible y natural para permitir una difusión mucho más extensa, y por otro lado, el facilitar la publicación en este mundo electrónico, le da a la

organización la oportunidad de tener una verdadera mezcla de ideas. Ambos ingredientes son componentes básicos del paradigma en que se basa la era de la información. Esta capacidad alcanzada para compartir electrónicamente con rapidez la mezcla de información obtenida, es lo que creará la revolución en el nuevo modelo de comportamiento organizacional [4], [7], [11].

Los sistemas de información basados en el modelo cliente/servidor tradicional, tratan de hacer de la diversidad, algo estructuralmente similar a almacenarse en un esquema de base de datos. El web tiene el potencial de utilizar la información distribuida y la diversidad no estructurada, en un esquema de administración del conocimiento.

Actualmente en muchas organizaciones existen sistemas manuales o informáticos que almacenan estructuradamente datos. Pero son las ideas lo que dan significado a esos datos; las ideas son las que nos permiten compartir el contexto de nuestras experiencias y explorar nuevas posibilidades para el futuro. Y son esas ideas y esa mezcla de información lo que se consigue en el web. Este nos permite romper las barreras organizacionales y geográficas alcanzando beneficios que antes no estuvieron disponibles.

Quizás el cambio más significativo con una Intranet es la habilidad de innovar y aprender en la organización. El acceso a ciertos datos nos

permitirá tomar mejor una decisión para ejecutar una cierta acción específica; pero es la impredecible capacidad creativa del hombre, para la generación de nuevas ideas, lo que asegura la ventaja competitiva, el éxito y el triunfo.

El ingrediente básico para la creatividad humana es la mezcla y evaluación de ideas; las fallas o errores cometidos en el proceso, no son una pérdida de tiempo; son pasos necesarios que nos permiten practicar la innovación.

"La habilidad de aprender e innovar", este es el mensaje de todos los libros de administración moderna cuando hablan de *"la búsqueda de la excelencia"*. Las organizaciones más exitosas son las que valoran y enfrentan las contribuciones que nacen del compartir ideas entre todos sus miembros. Un Intranet habilita la capacidad de compartir información y de mezclar ideas en una gran escala [8], [9].

En una organización tan amplia y diversa como la Armada, resulta imprescindible contar con un medio de comunicación y distribución de información que permita establecer comunidades virtuales. Una comunidad virtual se compone de un grupo de individuos con intereses comunes, son grupos que comparten ideas para someterlas a un proceso de evaluación/depuración, a tal punto que como resultado de este proceso se obtiene información con características de inteligencia

básica o conocimiento. Las características propias de la Fuerza Naval, en las que el personal por razones diversas debe separarse del área en que se ha especializado, sea esta las operaciones de superficie, submarinas, infantería, aeromarítimas o investigación oceanográfica, a cumplir anualmente con los transbordos, cursos de ascenso y requisitos de embarque, frontera, etc. es imprescindible mantener un medio adecuado que permita a estos elementos permanecer asociados a sus comunidades en forma virtual. Esto es lo que una Intranet faculta, es la tecnología adecuada para operar las organizaciones en la era de la información.

Muchas de las organizaciones tienen ya la infraestructura y las actitudes necesarias para adoptar una Intranet: Tienen la necesidad y tienen el hardware, la tecnología de Intranet conjuga el software necesario que hace a todo esto trabajar.

El uso del web como un medio de comunicación y coordinación interna en grandes organizaciones, tiene un potencial de generar profundos efectos en la forma en como hacemos las cosas y como trabajamos.

La tremenda simplificación técnica de una Intranet se debe a que está basada en estándares de tecnología abierta y pública. Una Intranet no es una tecnología revolucionaria, pero puede crear un cambio

revolucionario en la medida que la organización comienza a producir información.

1.6 Beneficios de la Tecnología Web

El web es habilitado por una serie de estándares ampliamente difundidos para crear y comunicar información a través de las redes de datos. Estos estándares proveen seis poderosos beneficios:

1. **Independencia de la plataforma.-** La información puede ser creada, almacenada, visualizada y transferida sin necesidad de implementar algún esquema de traducción de formatos, a través de diferentes plataformas de hardware, sistemas operativos y software.

2. **Transparencia de la información.**- La información puede ser recuperada desde cualquier parte del web, sin que el usuario esté consiente de la ubicación física del servidor de información, que clase de máquina o sistema operativo utiliza, o que comandos en la red fueron necesarios para proveer de la información.

3. **Facilidad de uso.**- Crear páginas web e hiperenlaces es tan fácil como utilizar cualquier procesador de palabras.

4. **Cliente universal.**- Los navegadores Web permiten al usuario interactuar con un interface común para todas las aplicaciones, por lo que los sistemas son fáciles de utilizar.

5. **Eficiencia en los costos.**- La distribución de la información es eficientemente menos costosa que la distribución de información basada en papel o en persona. Se reducen los costos de impresión, distribución, correo, fax, actualización, almacenamiento y recuperación.

6. **Eficiencia en el tiempo.**- Los usuarios controlan por ellos mismos el flujo de información, reduciendo el tiempo destinado a la ordenación, clasificación y evaluación de la información mucha de la cual termina en un basurero.

Explotar estos beneficios, implica algo más que instalar el hardware, software y publicar páginas web, requiere del diseño cuidadoso y de la implementación de una infraestructura adecuada que desarrolle las habilidades necesarias a través de un entrenamiento apropiado.

Para enfrentar con éxito una aproximación formal a esta tecnología, que nos habilita a enfrentar eficientemente a la era de la información, hay que tener presentes los siguientes principios básicos [4]:

- Latencia organizacional (efectos de ratios de superficie y ratios de volumen) descentralizar la organización
- La información conduce las funciones vs. Las funciones generan información
- Empujar (push) información vs. Halar información (pull)
- Soporte auto-servicio vs. Soporte hágalo por mí
- Comunicación/coordinación vs. Comando/control
- Tomas de decisiones distribuidas vs. Control central
- Acceso a la información vs. Calidad de información
- Contexto de la información vs. Contenido de la información
- Estandarización del conocimiento
- Explotación de lo desconocido

A lo largo de esta tesis, se evaluará permanentemente cuando uno u otro extremo de cada principio mencionado es útil y aplicable.

CAPITULO 2

2. IMPACTO DE UNA INTRANET EN LA ORGANIZACIÓN

2.1 ¿Qué es una Intranet?

El término Intranet en la actualidad es algo engañoso conceptualmente. De hecho, el verdadero contraste conceptual es con el World Wide Web. Ésta distinción es importante porque el término Internet se focaliza en las redes físicas y técnicas, mientras que el World Wide Web se focaliza en el contenido de información accesible a través de esa infraestructura física y técnica. Intranets y Extranets, como el World Wide Web son colecciones de contenido de información, que utilizan la misma infraestructura física y técnica. Un Intranet es el conjunto de información compartido por un grupo bien definido o una comunidad, dentro de una organización.

Una Intranet es la aplicación de la tecnología, protocolos y aplicaciones del Internet en el entorno privado de una organización.

Hasta cierto punto podríamos considerar justificada la adopción de la tecnología de Intranet por las razones cubiertas en el capítulo anterior, pero es necesario contar con una actitud adecuada conforme a la era de la información.

Las metas de una Intranet pueden establecerse dentro de la parte técnica en los proyectos que la organización piense implementar, dado que resulta interesante adoptar una tecnología tan novedosa que suena en todas partes. Poner las necesidades de suministros electrónicamente en el web para que las conozcan nuestros proveedores o establecer un sistema de correo electrónico interno, no son razones lo suficientemente claras como para introducir una nueva tecnología tan fundamental como la de Intranet [11].

Los Comandos y Direcciones esperan que la nueva tecnología aumente tanto la productividad organizacional como la productividad personal; esperan mejorar los elementos que permitan tomar mejores decisiones; mejorar la calidad de la información así como hacer de esta algo más visible.

Las expectativas del personal de menor rango van a ser bastante diferentes. Ellos se interesarán en como se les facilitará el acceso a la información, como el intranet les va a ahorrar tiempo y esfuerzo. Desde este punto de vista, aparentemente hay razones para auspiciar un proyecto de Intranet, garantizar un acceso fácil a la información y alguna reducción de esfuerzo y tiempo se puede alcanzar con una implementación técnica. Pero mejorar la calidad de la información, la toma de decisiones y la productividad de la organización no se puede alcanzar tan solo con una implementación técnica. Se requiere el desarrollo de una infraestructura organizacional y administrativa adaptada a las nuevas características de la era de la información.

2.2 La Toma de Decisiones Descentralizada

La estructura organizacional de la Armada, está concebida de modo que se lleven a cabo las funciones necesarias que permiten garantizar el cumplimiento de su misión. Estas funciones son delegadas a través de la Cadena de Comando, entre un conjunto de Comandantes y Directores de grandes sectores especializados en tareas específicas de cada uno de estos. A su vez cada gran sector incluye bajo su dependencia un conjunto de repartos con tareas más puntuales, de modo que toda la organización opera armónicamente en busca de cumplir los objetivos planteados por el mando superior. De ésta

manera, es imprescindible adoptar una postura que en base a delegación de responsabilidad y autoridad, descentralice la toma de decisiones en los niveles intermedios de mando. A pesar de existir esta distribución de toma de decisiones, existen doctrinas y procedimientos muy detallados que rigen las acciones dentro de un marco jerárquico burocrático, por lo cual es necesario alcanzar un punto de equilibrio entre la toma de decisiones distribuidas y el comando centralizado. Las limitaciones que existían en el pasado, ahora superadas por los avances tecnológicos, no permitían delegar en la medida deseada esta toma de decisiones, y si recordamos el efecto analizado con respecto a la latencia organizacional (relación de superficie vs. volumen), vemos que es indispensable contar con un medio efectivo y flexible que coordine a todos estos mandos intermedios, de modo que se pueda garantizar una verdadera delegación y distribución de la toma de decisiones.

La distribución de toma de decisiones es fundamental porque permite a la organización probar cada vez más ideas nuevas, buscando rápidamente el camino al mejoramiento continuo y sostenido. La creatividad y el aprendizaje están directamente relacionados con el número de ideas nuevas probadas.

En la administración moderna y en todo proyecto de reingeniería, se define como meta la necesidad de distribuir obligaciones y responsabilidades (decisiones). Los puntos de contacto, donde se está más cerca de la acción miran los problemas y las oportunidades primero que nadie. Es ahí donde están los funcionarios más experimentados aplicando los procedimientos actualmente establecidos, y por tanto son quienes saben como buscar mejoras.

Aunque es indispensable que en una organización militar como la Armada exista un comando y control centralizado, el paradigma de la centralización ha quedado corto en sus posibilidades para atender las necesidades de una organización moderna, que demanda eficiencia en el uso de sus recursos y eficacia en los resultados, es decir alta efectividad. Dado el tamaño de la Armada y la diversidad de sus funciones, resulta muy difícil dirigir y coordinar todas éstas garantizando el cumplimiento de la misión, sin que se invierta esfuerzo y recursos considerables. Las razones expuestas anteriormente, la escalabilidad, la inercia y la deformación, influyen determinantemente en las operaciones que se llevan a cabo en todos los niveles.

La tecnología de Intranet por sí sola, no puede crear una infraestructura de organización, procesos y métodos que soporte la creación y la administración de información en ambientes independientes y

distribuidos. Sin ésta infraestructura no existe una forma eficiente para encontrar la información, y, el contenido crecería en forma caótica, ineficiente y desordenada.

La infraestructura de los sistemas basados en papel ha sido refinada y pulida durante muchos cientos de años, y por tanto está sumamente integrada con la forma en como operamos los procesos y procedimientos en nuestra organización con nuestros conceptos de administración.

Las estructuras organizacionales que se han desarrollado alrededor de la administración de la información en papel son altamente centralizadas. Las características de la publicación en papel provoca centralización. Aún cuando las decisiones tomadas centralizadamente pueden publicarse y enviarse a toda la estructura jerárquica, la retroalimentación es muy pobre. Así mismo existe una gran dificultad para acceder a la información no administrada por la estructura central [4], [8].

Una vez que las copias han sido distribuidas, la administración de actualizaciones y cambios se vuelve costosa y en muchos casos imposible de mantener.

2.3 Control y Comunicación: La Clave para las Actividades Conducidas por Propósitos

En el corazón de la nueva infraestructura organizacional requerida está el paradigma operacional, el que define lo que constituye una organización funcional y efectiva. Las organizaciones militares tradicionales están enfocadas en el modelo de mando y control centralizado. La organización está diseñada para que la información sea llevada a un sitio central de comando, donde se establece el curso de acción distribuyendo las decisiones tomadas de regreso a toda la organización. Mientras más grande es la organización, el número de pasos intermedios aumenta así como también la cantidad de información a ser procesada. Aún cuando los medios electrónicos e informáticos han logrado aumentar la velocidad con que se transmite la información, incluso eliminando ciertos pasos intermedios, no han disminuido la cantidad de información a ser procesada o el número de decisiones a ser tomadas. Aún con la nueva tecnología disponible, el paradigma del comando y control centralizado parece haberse quedado corto en sus límites [4].

Pero, ¿Cómo una organización puede soportar efectivamente la dirección de actividades hacia sus metas sin alguien a cargo? El paradigma operacional define un modelo de mando y control distribuido,

pero tiene un cuerpo en teoría, el que explota la centralización de las comunicaciones y su capacidad coordinadora, para evitar el flujo de la información en sentido vertical, canalizándola más en el sentido horizontal [4]. En la teoría de sistemas generales de Ludwig von Bertalanffy, se explica que todos los sistemas comparten ciertas características que les permite funcionar como sistemas, y no como un tipo o nivel de organización [5]. Un premio Nobel de economía, Herbert Simon en su obra, "La arquitectura de lo complejo", demuestra como un sistema está compuesto de subsistemas estables independientes, y estos pueden afrontar mejor todo tipo de perturbaciones que aquellos sistemas construidos directamente por componentes [6].

El éxito de las manifestaciones en Filadelfia, mientras se llevaban a cabo las Convenciones Nacionales del Partido Republicano de Estados Unidos de América en el año 2000, se debió a que los manifestantes coordinaban de manera distribuida sus tácticas, transmitiendo por teléfonos celulares permanentemente su ubicación y la ubicación de la policía, debilitando sistemáticamente los dispositivos de control. Organizados como insectos, sin depender de unos pocos líderes, con capacidad de toma de decisión distribuida, y, comunicación y coordinación centralizada, la manifestación logró su propósito. La policía tuvo que detener a toda persona que utilizaba su teléfono celular

(instrumento de crimen) durante las manifestaciones para eliminar ésta comunicación “viral” de alta efectividad [12], [13].

Para que un sistema funcione como tal, en vez de cómo una colección de partes, debe contar con métodos de auto-organización e incluso comportamiento. Si el comando y control se distribuye a los subsistemas, tal como se muestra en la Figura 2.1, entonces se deben buscar formas de auto-organización entre ellos.

FIGURA 2.1. MODELO DE TOMA DE DECISIONES DISTRIBUIDAS

Lo que el sistema más complejo provee es comunicación y coordinación para los subsistemas auto-regulables. Dentro de esta distribución de toma de decisiones, coexisten dos modelos [4]:

- ✓ Los Ecosistemas.
- ✓ Los Conducidos por propósitos.

El modelo de los ecosistemas es conducido caóticamente, está enfocado en la supervivencia que es lo que lo obliga a buscar la eficiencia y estabilidad, los ecosistemas son evolutivos en función de la demanda del momento y no tienen propósitos concienzudos [4].

El modelo de los sistemas conducidos por propósitos, se aplica la razón para obtener un juicio de acuerdo a los propósitos propuestos concienzudamente. Los seres humanos tienen sistemas conducidos por propósitos y aunque el conocimiento se lo adquiere por competencia, hay otros puntos claves que ocasionan la estabilidad y diversidad en los sistemas más complejos.

En la Figura 2.2, tenemos una matriz que muestra los cuatro modelos que han sido discutidos entre éste capítulo y el anterior. En un eje ésta matriz cuantifica la distribución de la toma de decisiones, y en el otro eje la distribución de la comunicación [4].

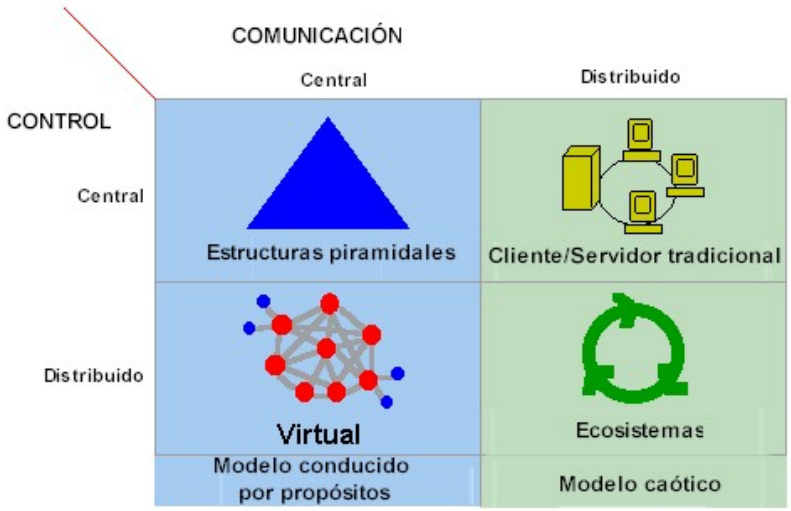


FIGURA 2.2. MODELOS DE CONTROL Y COMUNICACIÓN CENTRALIZADOS Y DISTRIBUIDOS

El nuevo paradigma operacional busca moverse desde el modelo de comando y control centralizado, al modelo de comando y control distribuido con una comunicación y coordinación centralizada.

Analizando la Figura 2.2, vemos que la típica estructura organizacional piramidal del siglo XX, es un ejemplo de sistemas diseñados alrededor de modelos tanto de toma de decisión como comunicación centralizados. Estas organizaciones están dirigidas por una persona en el cargo superior, auxiliado generalmente por un grupo asesor o Estado Mayor que expande su capacidad de tomar decisiones.

Un buen ejemplo del modelo de control centralizado y comunicación distribuida es la computación basada en la arquitectura cliente/servidor clásica. Sin embargo en organizaciones grandes, aún cuando las decisiones centrales tienden a conseguir un propósito, la comunicación distribuida peca de presentar demasiadas oportunidades para los errores y la falta de precisión de la información.

Con una estructura centralizada de comunicación y coordinación, que es el modelo de sistemas complejos trabajando por conseguir un propósito común (conducido por propósitos), se desarrolló el modelo para la tecnología de Web. Los organismos superiores son otro ejemplo. El sistema nervioso provee un método de coordinación y comunicación centralizado, pero casi todas las actividades del cuerpo son administradas localmente, reaccionando y ajustándose a las condiciones inmediatas del ambiente [5].

En un modelo de toma de decisiones y control distribuido, con comunicación y coordinación centralizada, se basan los sistemas de innovación adaptiva, esto quiere decir que sus subsistemas tienen la habilidad para adaptarse a las condiciones locales [4].

2.3.1 Innovación Adaptiva

Cada elemento de un proceso u operación (subsistema auto-regulado) se encuentra en un ambiente dinámico, en constante cambio, incluso volátil. Este subsistema auto-regulado subsiste dándole un valor agregado a la misión de la organización, adaptándose a éstas condiciones dinámicas del ambiente [4].

El poder de este nuevo modelo organizacional es su maleabilidad y flexibilidad. No toda la organización debe responder a una amenaza o una oportunidad, tan solo responden las partes afectadas. Hay mentalidades más creativas y mayor responsabilidad tratando de resolver el problema que lo que cualquier control centralizado pueda manejar, y por tanto se generan mejores respuestas al problema. Este proceso se lo conoce como innovación adaptiva [4].

Con la innovación adaptiva una implementación que se enfoca en crear las infraestructuras adecuadas e impartir el conocimiento y las habilidades demandadas tiene mayor oportunidad para el éxito, dado que [4]:

1. Un pequeño esfuerzo incremental entre todas las unidades en una organización hábil para la implementación, provee un resultado superior que un gran esfuerzo centralizado.

2. Si las herramientas y los enfoques son adecuados, el tiempo y esfuerzo dedicado a mejorar va a aumentar desplazando los esfuerzos y actividades que sean menos útiles.

3. Los usos y la calidad de información va a mejorar con el tiempo si se desarrolla una comunicación y coordinación espontánea y adecuada entre las unidades, debido a la necesidad de compartir ideas, competir y por la presión de la demanda del compromiso.

El uso de computadoras en los escritorios aumenta los costos computacionales, pero disminuye la necesidad de secretarias y virtualmente ha eliminado las máquinas de escribir. La implementación de una red inter - organizacional TCP/IP aumenta los costos de networking, pero generará ahorros en fotocopias, almacenamiento, impresión, distribución e incluso movilización. Una implementación de Intranet, incluso reduce el número de personal para labores manuales al eliminar funciones requeridas en los sistemas actuales basados en papel; éste personal puede ser reentrenado para ejecutar tareas con mayor valor agregado.

Con todo esto en mente, la justificación de una implementación actualmente se concibe más con la idea de reducir costos, que con la idea de oportunidades nuevas que se puedan dar [7].

2.4 Ciclo de Vida de la Administración de la Información

La información organizacional generalmente lleva contenido que habilita al líder en la toma de decisiones. Una organización amplía su habilidad de controlar sus recursos dividiendo el trabajo necesario para alcanzar una meta entre múltiples individuos o suborganizaciones. Para ser eficientes y eficaces, es decir efectivos, las actividades y el progreso deben ser coordinados. Una razón importante para compartir la información son los acuerdos logrados en la coordinación de tareas para alcanzar los objetivos [8], [9], [10].

Un requerimiento para una coordinación exitosa es la consistencia de la información. No existe efectividad si la existencia de información vital es desconocida por un individuo que la necesita. No existe efectividad si un equipo de trabajo está tratando de alcanzar un consenso y sus miembros están operando basados en información diferente, incompatible e inconsistente. Hay cierta información que se vuelve obsoleta y requiere ser permanentemente actualizada. Las

organizaciones basadas en sistemas de papel, han estado tratando de resolver este problema durante siglos.

La actualidad e integridad de la información es un problema fácil de atender si su contenido no cambia, así la coordinación no es compleja y la información puede estar centralizada para ser distribuida cuando se la requiera. Sin embargo, esa es una característica poco común en estos días, los ambientes distribuidos por tanto necesitan coordinar su información de una manera diferente, y esto demanda una estructura administrativa y procesos diferentes.

2.4.1 Acceso, Poder e Innovación

> Una característica clave de la tecnología de Intranet, es la habilidad para delegar el control de la administración de la información electrónica a los creadores de información, sin necesidad de que intervengan directamente en el proceso los especialistas en tecnología de información. Así el control de la información fluye desde su creador hacia el usuario de la información. Si los usuarios tienen la facilidad de recuperar la información y verla cuando la necesitan, la información ya no debe ser enviada a los usuarios cada vez y cuando. Así la actividad de publicación puede separarse de la actividad de distribución automática [11].

Para hacer que esto funcione no solo se necesita una nueva infraestructura tecnológica de información, se necesita un profundo cambio en actitud y cultura. Como técnicos, debemos pensar en como resolver los problemas dando herramientas e infraestructura que permitan a los creadores de información ser lo que son. Como creadores de información debemos concentrarnos en publicar y no distribuir información. Como usuarios debemos concentrarnos en nuestra responsabilidad de determinar y controlar los cambios en la información que necesitamos, y adquirirla cada vez y cuando la necesitemos.

Este paradigma operacional afecta a tres características organizacionales: Administración, Comunicación y Liderazgo [4].

Implicaciones para la Administración, la estrategia de implementación de una Intranet involucra el desplazamiento de varios principios típicos de administración.

Con el paradigma de toma de decisiones centralizadas, la implementación de un Intranet consistiría en lo siguiente: Determinar que departamentos van a participar y que funciones tendrán cada uno en el desarrollo, y luego entregar los recursos a cada departamento para que hagan su parte del trabajo delegado. Esto quiere decir aplicar el lema **"Lo haremos por usted".** El

paradigma de toma de decisiones distribuidas mira a la Intranet como una utilidad, y se concentra en identificar y alcanzar los requerimientos de infraestructura para luego repartir el conocimiento, las habilidades y las herramientas a todos los departamentos o suborganizaciones, así ellos podrán implementar cualquier proyecto que ellos piensen tenga sentido participe en el proceso de compartir información. Esto quiere decir aplicar el lema **"Habilitar a todos para que ellos mismo lo hagan"** y es la base del modelo de innovación adaptiva [4].

En la práctica, llegar a un acuerdo para un gran proyecto central, toma más tiempo que distribuir las bases del conocimiento, las habilidades y las herramientas. Una vez alcanzado el acuerdo, el esfuerzo para un desarrollo centralizado rápidamente se torna en una sobrecarga. Este es un ejemplo del problema de una mala relación de superficie vs. volumen, o latencia organizacional. Basándose en el análisis de muchos proyectos, se determina que el tiempo que toma llevar a cabo un proyecto centralizado, permite desarrollar un proyecto por cada uno de los departamentos, y al final las diferencias en cuanto a cantidad, calidad y responsabilidad del contenido es enorme, por su puesto a favor de los pequeños esfuerzos coordinados. A pesar que los dos enfoques requieren de la implementación de una infraestructura

técnica; en el enfoque centralizado los departamentos generalmente se ven frustrados esperando su turno y por tanto muchas veces comienzan sus propios proyectos aislados. Una ruta al caos [4], [11].

Implicaciones para las Comunicaciones, tiene que ver con el modelo “empujar” (push) y el modelo “halar” (pull). Las implicaciones en la comunicación tienen mucha más influencia en la actitud personal que las implicaciones en la administración y el liderazgo, debido especialmente a los avances tecnológicos alcanzados. En el proyecto no solo debemos preocuparnos por proveer información, sino especialmente en la lógica para hacerlo. Así podemos revisar un número de actitudes típicas adoptadas a lo largo y ancho de la organización:

TABLA II

EMPUJAR Y HALAR: LOS PRODUCTORES DE INFORMACIÓN

PUBLICADORES	
Mentalidad de empujar (push)	**Mentalidad de halar (pull)**
Yo sé lo que necesitas y te lo enviaré.	Yo conozco mi misión y mi audiencia.
Yo no sé lo que necesitas, pero te envío todo.	Yo pongo la información disponible en base a la demanda.
No me interesa si lo necesitas, te lo envío de todas maneras.	Yo mido la utilidad de mi información y la mejoro constantemente.

Hoy en día todos nos enfrentamos al grave problema de la información que nos es empujada, especialmente a través del correo electrónico. Las Tablas II y III, muestra la actitud de los publicadores y especialistas del dominio, en los esquemas de empujar y halar la información. Cuando el publicador nos empuja la información, el tiene el control del flujo de ésta, y determina que información, como y cuando enviarla. El especialista del dominio al momento de tomar una decisión evalúa la información que el publicador determinó que le era útil y no sabe ciertamente si aún está actualizada, siendo el modelo por tanto limitado para las posibilidades actuales.

Cuando es el especialista del dominio quien hala la información, y por tanto mantiene el control del flujo de la misma, al tomar una decisión lo hace con información útil y actualizada, estando conciente que es su responsabilidad determinar que información es válida. Los publicadores se preocuparán en mejorar sus contenidos en base al análisis de los sistemas de retroalimentación, o por simple estadística de los accesos.

TABLA III

EMPUJAR Y HALAR: USUARIOS DE INFORMACIÓN

ESPECIALISTAS DEL DOMINIO	
Mentalidad de empujar (push)	**Mentalidad de halar (pull)**
Alguien necesita visitarme.	Yo establezco mis propias citas o visitas.
Alguien necesita decirme que información está disponible.	Yo se como buscar información cuando lo necesito.
Alguien necesita decirme que información necesito.	Mi obligación es determinar que información necesito.

Si el esquema de halar información por parte del especialista del dominio es más adecuado, contamos con diversos métodos que permiten ahorrar tiempo al evitar que revisemos información que posiblemente no ha cambiado, a través del uso de agentes. Los agentes pueden “empujar información” pero en base a ciertas reglas establecidas de manera personalizada por el especialista del dominio, por lo que es éste quien aún mantiene el control del flujo de la información. Así podemos establecer que cada que cambie una página o un sitio completo, seamos notificados; o suscribirnos a listas de distribución de información en base a nuestras preferencias.

Implicaciones para el Liderazgo, hay muchas y tienen que ver especialmente con la resistencia al cambio. Hay tres tipos de resistencias a una adopción del web: primero, aquellos que no entienden las complicaciones organizacionales y el paradigma propuesto; segundo, aquellos que temen perder el poder con el nuevo paradigma; y finalmente, aquellos que reconocen que el cambio es necesario, pero quieren retardarlo un poco para ganar tiempo buscando una mejor posición en la organización. Estas reacciones son más organizacionales que tecnológicas. Los líderes en la era de la información deben proveer una visión, estimular la diversidad y mezcla de ideas, y motivar un crecimiento transparente de la información propiciando compartirla y no esconderla. La Intranet es la herramienta ideal para alcanzar esto.

2.5 Reducción de la Sobrecarga de Información

La sobrecarga de información, es algo común en nuestros días. No es de sorprenderse si miramos la bandeja de entrada de un trabajador promedio, y encontramos que está llena de mensajes e información que alguien le envió ***"por si acaso la necesita"***. Esto pasa tanto en sistemas basados en papel como en sistemas electrónicos. Mucha de esa información sufre algún tipo de desfase, en unos casos llega tarde y

en otros antes de que la necesitemos. De todas maneras nuestra bandeja de entrada está llena de información que no hemos solicitado. El trabajador probablemente archivará la mitad de la información que ha recibido ***"por si acaso"***. Cuando se requiere la información, debe enfrentarse a un gran volumen de archivos en un sistema de información personal manual o asistido por computador, el que además puede enfrentar complicados problemas como incompatibilidad de formatos o medios.

El invento de las fotocopiadoras hizo de la información ***"por si acaso"*** algo aún más difícil de manejar. En vez de enfrentarnos a unas pocas copias de papel carbón, ahora nos pueden bombardear con verdaderas montañas de copias de un documento, folleto o catálogo. El correo electrónico ha llevado a este problema a verdaderas situaciones críticas. Un publicador puede almacenar una lista de distribución y con un simple comando enviar un documento a un número virtualmente ilimitado de destinatarios, información ***"por si acaso"*** la necesiten. Todos enfrentamos ese problema en el correo electrónico de Internet, cuantos mensajes nos llegan con un mensaje en las primeras líneas ***"...si no le interesa el....., elimine por favor este mensaje..."*** Esto ocasiona que el trabajador pierda tiempo evaluando la información y eliminando todo lo que sea "irrelevante" [4], [8], [9].

Tal como se muestra en la Figura 2.3, la sobrecarga de información impide que el funcionario procese todo lo que recibe a tiempo, por lo que esta información normalmente al ser evaluada, sufre ya un desfase en el tiempo, tendiendo a estar permanentemente desactualizada. Además luego de ser brevemente evaluada, mucho de lo recibido es irrelevante.

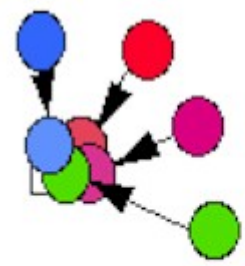


FIGURA 2.3. INFORMACIÓN DEL TIPO "POR SI ACASO" EN EL MODELO DE EMPUJE

La alternativa a la información ***"por si acaso"***, es la información **"justo a tiempo"**, o mejor conocida como **información en demanda**. Esta ha sido la promesa de las redes de computadoras, pero que ha fallado más que todo por la falta de conocimiento de este potencial. Históricamente, han existido dos enfoques para enfrentar la entrega de información **"justo a tiempo"**. El primero, dejar la información distribuida entre los sistemas y las aplicaciones; tal como se muestra en

la Figura 2.4. Para acceder a la información el usuario tiene que aprender múltiples procedimientos muy complicados para navegar, encontrar y acceder a la información. Una vez allí, deberá enfrentarse a varias interfaces, puesto que cada sistema requiere tratar con una interface diferente y por tanto conocimientos diferentes. El efecto de esto es que el usuario prefiere ignorar la información **"justo a tiempo"**, y su potencial.

FIGURA 2.4. LOS PRIMEROS MODELOS DE INFORMACIÓN EN DEMANDA

Para resolver este problema muchas organizaciones han decidido agrupar toda la información en un solo sistema maestro, así los usuarios solo se enfrentan a una sola interfaz y a un solo método de acceso, tal como se muestra en la Figura 2.5. Sin embargo dado que se centraliza el manejo de toda la organización en un solo sistema, éste se vuelve demasiado complejo y por tanto costoso. El costo de mantener

estos sistemas es elevado, y el ingreso de información al sistema puede también demandar el conocimiento de expertos. La complejidad de estos sistemas hace que sea difícil modificarlos y utilizarlos. Las herramientas diseñadas para su administración están basadas en premisas de datos discretos y operaciones transaccionales. La administración de las mejoras a las interfaces relacionadas con los manejos de versiones de la parte cliente, normalmente es un costo oculto que demanda un enorme esfuerzo especialmente si la organización es grande y geográficamente distribuida, actualmente tampoco es esta la solución para resolver los problemas de una organización en la administración de su información [4], [8], [9].

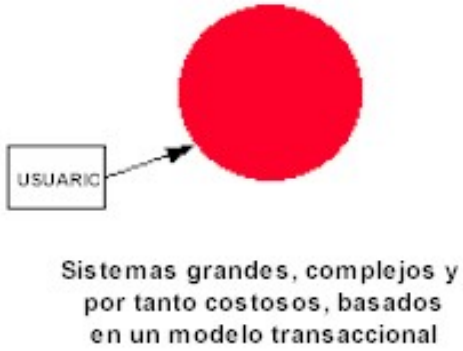


FIGURA 2.5 INFORMACIÓN EN DEMANDA BASADA EN EL MODELO CLÁSICO CLIENTE/SERVIDOR

La tecnología web ofrece un nuevo enfoque para la entrega de **"información en demanda"**, debido a que soporta el control

distribuido, la publicación, el acceso y el manejo de la información; sin requerir de la complejidad de los grandes sistemas centralizados. La información es publicada por los creadores sin necesidad de programadores especializados, o de ingresar información como datos estructurados, ni ver la misma a manera de reportes. Tal como lo muestra la Figura 2.6, con el uso de los navegadores web, **"el cliente universal"**, el usuario puede acceder a múltiples formatos de información (multimedios) con una interface universal, fácil de utilizar, siendo para él transparente qué tipo de aplicación, sistema o plataforma es la fuente de los datos que él demanda. Este simple cambio tecnológico, revolucionó nuestras estructuras de administración de información y por tanto las estructuras organizacionales [4], [8], [9].

FIGURA 2.6. INFORMACIÓN EN DEMANDA BASADA EN EL CLIENTE UNIVERSAL

2.5.1 Potenciando al Individuo

La característica clave de ésta tecnología es permitir el flujo de la información desde los creadores de ésta a los usuarios de la misma. Si el usuario tiene la capacidad de recuperar y visualizar la información cuando la necesita, no hay necesidad de tratar con la información ***"por si acaso"***. La publicación es aislada de la distribución automática, por tanto no nos llenamos de datos y documentos irrelevantes, tan solo solicitamos lo que requerimos en ese momento, preocupándonos más de hacer una buena evaluación del material de nuestra incumbencia en las circunstancias particulares al momento de tomar una decisión.

Hacer que esto trabaje no solo demanda una implementación tecnológica, ni un cambio estructural de la organización como vimos anteriormente, demanda un cambio de actitud y de cultura de trabajo. Como creadores de información debemos preocuparnos de entrenarnos para crear información y no para distribuirla. Como usuarios de información debemos preocuparnos responsablemente de determinar y controlar nuestras necesidades cambiantes de información, así como adquirir activa y eficientemente ésta cuando la necesitemos.

2.5.2 TRANSFERENCIA EFICIENTE DE LA INFORMACIÓN

Se discutió previamente la ineficiencia de la distribución de información del tipo ***"por si acaso"*** en los sistemas basados en papel. Otra ocasión en la que transferimos información de este tipo es en la educación y entrenamiento. La forma tradicional de entrenamiento cara a cara, es típicamente rica en información ***"por si acaso" o "desfasada"***. El contenido es una bandeja llena de datos que ni el estudiante ni el instructor saben exactamente si los necesitan actualmente para realizar el trabajo, así que está ahí ***"por si acaso"***.

Si existe una forma eficiente de encontrar y acceder la información en demanda, el modelo tradicional de educación y entrenamiento cambiaría. El entrenamiento se podría enfocar en las habilidades, mientras que el contenido específico se lo provee en demanda en la medida que se lo requiera.

El modelo en demanda tiene otras ventajas, la tecnología de transferencia de información tradicional está basada en lotes, lotes de información que se crean para ser transferidos como documentos para la educación o entrenamiento tradicional. Ya que la información se empaca en lotes, cuando una porción de esta ha cambiado, no hay un mecanismo instantáneo que actualice la

parte correspondiente del lote, así, en la medida que transcurre el tiempo el lote está desactualizado, se vuelve obsoleto mientras la información nueva no está incluida en el aún. La forma de solucionar esto es re-ensamblando el lote, y reenviándolo cada vez que ocurra un cambio en la información. Esto es ineficiente y demanda esfuerzos que se podrían evitar.

La tecnología web soporta la creación y administración de la información en forma distribuida. Así la porción del contenido puede actualizarse en la medida que la información cambie. Si se establece la infraestructura adecuada, la información es fácil de encontrar y acceder cuando y donde sea necesario. Esto reduce tanto el tiempo necesario para entrenamiento y la cantidad de información que un empleado requiere absorber en su debido tiempo.

2.6 Diferencias Medulares en las Herramientas Disponibles [4]

Existe un conflicto en dos áreas del Intranet: en la creación del contenido y herramientas administrativas, y las herramientas de trabajo en grupo.

El Web provee el mayor avance en comunicaciones electrónicas, basándose en un contenido estandarizado. Pero el estándar no solo

tiene que ver con el contenido, su factibilidad de uso en multi-plataformas, etc. Tiene también que ver con que cualquier tipo de herramienta con capacidad de edición HTML pueda hacer cambios en el contenido. La estandarización permite obtener un mismo resultado de las herramientas que se utilicen, independientemente de la marca del fabricante del producto. Es decir puedo usar cualquier producto del mismo tipo sin importarme que sean de distintos fabricantes.

En las áreas de productos de administración de sitios, hay dos funciones principales que estas herramientas apoyan: una es la habilidad para encontrar eficientemente contenido (estructuración, indexación y búsqueda), y la otra es la administración del contenido (disponibilidad, actualización e integridad). En este tipo de herramientas también hay un enfrentamiento entre los enfoques centralizados y descentralizados.

Cualquier producto que requiera el paso del contenido del Intranet por un punto en particular para ser publicado, sea un servidor, una persona o una aplicación, forja la adopción de un modelo centralizado y es un potencial cuello de botella para la organización. Generalmente esto sucede cuando se requiere crear y mantener un índice único general.

En el modelo distribuido, los índices de la Intranet residen en algunas ubicaciones, no nos importa donde. El contenido del índice es creado y

mantenido por descubridores automatizados que siguen los enlaces creados construyendo un mapa de objetos y enlaces en su paso. Así, sin necesidad de pasar por un cuello de botella, se tiene una vista de todo el contenido disponible en la Intranet.

La automatización de flujos de trabajo o workflow, son esquemas recientes en las herramientas de Intranet. Mensajes de correo electrónico, formularios, boletines, etc son un ejemplo típico de esquemas automatizados. Lo que distingue a un paquete de workflow de las herramientas de Intranet, es la habilidad de controlar y manejar los procesos programados. Esta es un área de mucho interés que debe ser seguida de cerca en un futuro cercano, porqué la Intranet y el web tienden a coordinar actividades vía mensajes; mientras que los workflow son aplicaciones de bases de datos que usan variables comunes para coordinar actividades, implementando el concepto de documento - trámite. Ambas tienen fortalezas y debilidades, pero ya se está viendo aplicaciones con una mezcla de los dos enfoques.

Compartir datos es la base para los workflow, esto se consigue en unos casos replicando bases de datos y sincronizándolas cuando sea posible; y en otros, gracias a que hoy es posible lograr una autodescripción de las reglas de un proceso en una máquina de workflow, gracias a tecnología emergentes como XML. Los fabricantes

de éste tipo de herramientas están tratando de utilizar la tecnología de Intranet para sus nuevas versiones de workflow. En otros casos se desarrollan interfaces (API) con las máquinas de workflow tradicionales.

Al establecer políticas de Intranet, la organización tiene que direccionarse a estándares web en el largo plazo, para permitir una mayor flexibilidad incorporando nueva funcionalidad a futuro. Los estándares propietarios deben extenderse a lo mucho al corto plazo, para ser reemplazados en el mediano plazo.

Administrar sistemas distribuidos nos enfrenta a interesantes cambios que no se encuentran en ambientes centralizados. El mayor de estos es cambiar la actitud de control por la actitud de habilitar la toma de decisiones y acciones independientes. Sin una organización estandarizada, se pierde la capacidad de comunicación y coordinación efectiva de actividades. Los cambios están orientados a proporcionar una estructura que facilite la comunicación y coordinación en forma centralizada, sin afectar la toma de decisiones y actividades distribuidas, haciendo a la organización fuerte y flexible.

La tecnología web hace de la producción y publicación de información algo fácil, al igual que la recuperación y visualización de ésta. Lo que no es fácil es encontrar información relevante creada en este ambiente independiente. De lo que la tecnología web carece es de un canal

adecuado de distribución y mercadeo de la información creada, sin este canal no hay una forma eficiente de encontrar la información. Las organizaciones a lo largo de los años han refinado el funcionamiento de estos canales en los sistemas basados en papel, y estos canales están tan integrados a la forma en que opera la organización, que no lo visualizamos como un canal de distribución sino como los procesos y procedimientos para hacer nuestro trabajo. Esto forma el marco de trabajo de las organizaciones actuales.

2.7 MARCO DE TRABAJO PARA LA INFORMACIÓN EN UNA INTRANET

2.7.1 USUARIOS/AUTORES/AGENTES/PUBLICADORES [4]

La clave para entender este marco de trabajo es la definición de algunos roles. Estos son roles y no posiciones ya que un solo individuo puede además de su trabajo normal abarcar uno o más roles; o varios individuos tener el mismo rol. El entendimiento de estos roles nos ayudarán a comprender el marco de trabajo en una Intranet.

Los Usuarios, acceden y visualizan la información. Existen varias razones para que un usuario acceda a la información, y estas pueden cambiar entre una sesión y otra. El punto importante es

que el usuario esté donde esté, deberá encontrar un valor agregado para él que resuelva sus necesidades de información. Si el método de acceso a la información demanda un esfuerzo mayor al valor que él espera obtener de ésta, el usuario no volverá a utilizar el sistema o buscará otra forma de obtener la información.

Los Autores, crean la información. En los medios tradicionales, crear y estructurar son tareas íntimamente relacionadas, las rutas de acceso a la información son lineales, y toda la información relacionada está junta y se entrega junta. Si se requiere una ruta de acceso diferente o una combinación de información diferente, es mejor construir la estructura en un nuevo documento replicando la información en vez de utilizar índices externos que relacione la información.

En el mundo web con los vínculos o hiperenlaces, la estructuración en la creación de información ha cambiado. Esto se debe a algunos factores: primero, los vínculos permiten al usuario escoger el orden en el cual quiere acceder a la información. Así mientras el autor sigue creando una estructura, ésta debe ayudar al usuario a determinar sus necesidades actuales de información valiosa para él; y deja de ser el autor quien determine las necesidades del usuario "a priori".

Segundo, cuando una información es referenciada o recombinada, es mejor utilizar un vínculo que copiar la información de un lugar a otro. Aún cuando esto puede y debe ser realizado por un agente o broker, es un concepto que los autores deben comprender. Exactamente igual que en una base de datos, la meta es reutilizar la información en vez de crear copias que deban ser continuamente sincronizadas. Esto implica que el autor debe tener presente una estructura que permita la reutilización de módulos antes que una estructura lineal.

Los agentes o brokers, son la clave para encontrar la información. Esto es cierto tanto en el mundo del papel como con la tecnología web. Cualquier tecnología que permita la creación independiente de información, ocasionará a los usuarios dificultad para encontrar lo que ellos necesitan. El agente de información provee este servicio. Nosotros utilizamos a un agente de información cuando acudimos a un directorio, a una guía de TV, a una librería. Por tanto en una organización cuenta con personas encargadas, dentro o fuera de ella, de determinar y recolectar la información que el resto debe conocer. Son los agentes los que más ven alterado su trabajo por esta tecnología. Pueden utilizar el navegador web para explorar la información y entregar los resultados; pero el impacto más dramático es cambiar la entrega

de lotes empacados de información a manera de inmensos reportes, por la entrega de rutas de acceso a la información. Esto es muy importante que se comprenda, porque esto cambia la forma de entrega y el enfoque de los agentes o brokers tradicionales [4].

La entrega en el pasado podía consistir en un lote de documentos de 300 páginas. En el mundo del web, puede ser una página con varios vínculos. En el lote de documentos, el agente necesita enormes cantidades de tiempo, cortando y pegando información de varios documentos para luego editar un informe final de "300 páginas". Con la tecnología web, él puede pasar ese tiempo entendiendo las necesidades de los usuarios, estableciendo un procedimiento para ello, y buscando las rutas de acceso más comprensibles para dar el mejor soporte a esas necesidades.

Los Publicadores, hacen que la información esté disponible. Las organizaciones demandan una administración de información que les permita coordinar y comunicar en forma predecible y eficiente. Cierto tipo de información requiere actividad directa. La información se vuelve obsoleta pronto. Otro tipo de información requiere revisión y aprobación. Esto sucede tanto en el mundo de papel como en el mundo web, la diferencia es que para el mundo

de papel han pasado 400 años para construir una infraestructura que soporte las necesidades de administración de información. De hecho, la burocracia y los procesos organizacionales son nada más que infraestructura que soporta al mundo de papel. En las organizaciones hay publicadores encargados de publicar la información oficial que tiene una organización [4].

Los publicadores tienen necesidades muy diferentes de acceso a la información que los usuarios y los agentes. Ellos necesitan una infraestructura que les permita en forma eficiente administrar el contenido de la información que ellos son responsables. Por esto el marco de trabajo en una Intranet, debe soportar dos estructuras de páginas diferentes así como dos tipos diferentes de páginas. Las unas para los usuarios y agentes, y las otras para los publicadores y administradores. A la segunda estructura se la llama el **"mapa de administración"**, y las páginas que contiene ésta estructura, páginas de mapeo. Las páginas de mapeo se crean basándose en algunas reglas, y una vez creadas no requieren de mayor esfuerzo para mantenerlas. Los cambios son mínimos y no demanda mucha actividad [4].

2.7.2 REVISIÓN DEL MARCO DE TRABAJO

La Figura 2.7 [4], muestra los componentes básicos de este marco de trabajo. El techo representa las metas de la organización, la razón para crear éste marco. La infraestructura tecnológica: hardware, software, redes de datos, protocolos y estándares, como base. Las columnas proveen el soporte para que la organización alcance sus metas apoyados en la infraestructura tecnológica. Incluyen las funciones de publicación, aprobación y descubrimiento de la información.

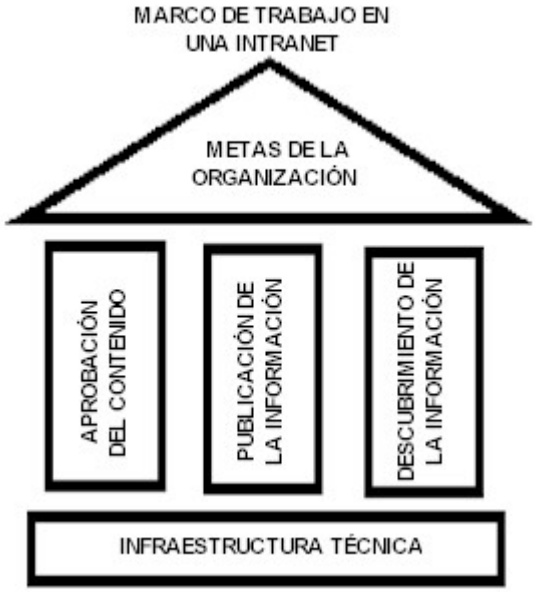


FIGURA 2.7. MARCO DE TRABAJO DE UNA ORGANIZACIÓN BAJO UNA INTRANET

2.8 ¿Quiénes son los Actores?

La información formal de una organización en una Intranet, se soporta definiendo una política de administración y los roles necesarios para llevarla a cabo, para que soporten los siguientes procesos:

- Actividades dirigidas por objetivos
- Comunicación y coordinación
- Verificación de contenido
- Actualización de la información
- Protección de fallas de disponibilidad
- Protección de pérdidas

En la medida que el medio de comunicación migra del papel a los medios electrónicos de una Intranet, los roles de la organización deben ser revisados para explotar las fortalezas y mitigar las amenazas de la nueva tecnología.

2.8.1 Roles para la Administración de una Intranet

La información formal de una organización se soporta definiendo roles. En organizaciones donde el papel es el medio primario de comunicación, los roles relacionados con la información están íntimamente atados con los roles funcionales de la organización. Con el uso de medios electrónicos para soportar el manejo de la

información estos roles fueron apartados a especialistas en la tecnología de la información (Departamento de Sistemas de Información en organizaciones desarrolladas). Esta separación forzosa ha creado un ambiente complejo y hasta cierto punto inflexible y poco adecuado para el trabajo. Los especialistas en tecnología de información debido a su falta de experiencia con las actividades funcionales de una organización, suelen ofrecer a duras penas el desarrollo de aplicaciones con una interfaz de usuario algo óptima, muchas veces asumían mucha filosofía teórica que distanciaba de la realidad práctica, y por tanto de las necesidades que los usuarios requerían. La demanda de devolver la administración de la información a las áreas funcionales y permitir a los especialistas de sistemas preocuparse de los aspectos propios de su área, es uno de los principales intereses de una Intranet.

Muchas organizaciones han reconocido que la información no es solo un resultado de los procesos, sino una fuerza que guía el funcionamiento de sus sistemas y la conducción de sus actividades. Eso ha creado una nueva perspectiva de lo que constituye el valor real de muchos roles funcionales; así como la creación, administración, comunicación y aplicación de la información. Sea en el área de Recursos Humanos, Financiera o

Ingeniería, el rol primario de un administrador en el pasado no se concibió en términos de administradores de información. Para alcanzar un verdadero beneficio de una Intranet, esto debe cambiar. Los administradores necesitan entender como la información les permite desempeñar mejor sus funciones y por tanto enfocar sus roles desde esta nueva perspectiva. Varios analistas y visionarios del final de este siglo, señalan sin duda alguna cual es el papel de la información en el éxito del futuro. Un connotado autor, Peter Drucker, se refiere a la sociedad post - capitalista, llamándola "la sociedad del conocimiento" [8]; otro, Jonathan Galbraith, dice:

"**El dinero fue el motor de la sociedad industrial. Pero en la sociedad de la información, en la que vivimos, el propulsor, el poder, es el conocimiento. Hemos visto emerger una nueva estructura de clases en donde la división se establece entre quienes tienen la información y quienes se ven obligados a actuar dentro de la ignorancia. La nueva clase dominante extrae su poder no del dinero, ni de la propiedad de la tierra, sino de los conocimientos."** [9]

Sin embargo, el conocimiento no es tomado como pura idea mental, sino con la amplia concepción griega del saber; puesto que es creador de la acción, origen de los hechos que culminan en éxitos sobresalientes, formador de visiones valiosas que guían responsablemente el trabajo, la justicia y la vida. Dentro de las tendencias adaptivas más aceptables que las organizaciones han

adoptado, para enmarcarse en ésta nueva sociedad del conocimiento, vemos la evolución de los jefes y administradores funcionales, a convertirse en líderes facilitadores del éxito de sus colaboradores. La receta no es fácil de seguir, es compleja y demanda la existencia de valores.

La palabra valor alude a la potencia, el sentido o la preferencia que encausan los esfuerzos humanos, e incluye tres acepciones: ética (principios), económica (valía) y sicológica (valentía). Existen valores, lo que vale y atrae a los individuos. Hay valores finales como: misiones, visiones y metas; valores instrumentales como: estrategias, tácticas y procedimientos. Se menciona así mismo, eficiencia, flexibilidad, transparencia, creatividad e innovación. Pero todos los valores para que cumplan su función atrayente, habrán de ser valores compartidos y difundidos en la organización; deberán ser comunicados a todos los miembros involucrados; y aceptados en el mayor consenso general posible de alcanzar.

Administrar el conocimiento y tener una organización que aprende, demanda reflexionar un poco sobre estos términos.

Aprender es un verbo. Es el proceso de encontrar o inventar formas de hacer algo, de la nada [10]. Si nosotros utilizamos procesos inflexibles y estáticos para hacer algo, no podemos

aprender porque la forma de hacer determinada acción ya es conocida, alguien ya la descubrió y la estandarizó. La Intranet, dada su falta de estructura, se convierte aquí en un terreno fértil que permite explorar nuevas formas de hacer las cosas, lo que permite tener una organización que aprende.

El conocimiento por otra parte, es un repositorio de lo aprendido [10]; puede ser explícito al estar plasmado en libros o manuales evidentemente fáciles de publicar en el web; o implícito en procesos, experiencia, actitudes y formas de actuar no documentadas.

El aprendizaje y el conocimiento no son funciones organizacionales, sino que se dan a nivel de individuos. La organización aprende solo si el individuo imparte sus conocimientos o cambia la forma de llevar a cabo un proceso establecido. Es por esto que una organización que desea aprender constantemente, debe encarar una difusión de ideas a partir de sus aprendices individuales.

Si se provee de un esquema que permita a éste individuo compartir lo que aprende, sus experiencias y visiones, a través de un medio de difusión como el web, podemos tener una enorme base de conocimiento organizacional.

El aprendizaje y el conocimiento son altamente iterativos. Cuando un "aprendiz potencial", se enfrenta a una situación caótica en la que no sabe que hacer o como actuar, tomará uno de los tres caminos siguientes [4]:

1. Buscará en una base de conocimiento si alguien antes se encontró en su situación actual, de modo que probablemente la solución a su problema ya fue encontrada antes, alguien en la organización invirtió tiempo y esfuerzo solucionando el mismo problema; si es así, el individuo aprendió de la base de conocimiento organizacional, o a su vez al revisar la solución, la recordó de su propia estructura mental de conocimientos. Es decir se evitó el “volver a inventar la rueda”. Incluso en éste proceso, puede que el nuevo aprendiz identifique nuevas variables que condicionan a que la solución conocida no sea ya la mejor, entonces partiendo de una base, se mejora, se innova y se actualiza la base de conocimiento.

2. El puede encontrar varias circunstancias similares, pero no exactamente iguales en la base de conocimientos, que le permitirán inferir la solución a su problema combinando piezas de conocimiento e ideas del sistema, creando nuevo conocimiento en el proceso que será compartido con la

organización. Este es un ejemplo claro de la validez del paradigma de la era de la información.

3. El aprendiz podrá generar nuevo conocimiento, tratando con múltiples acciones y evaluando los resultados, hasta determinar la mejor alternativa, la que será expuesta en la base de conocimiento. Nótese que esta forma de generar conocimiento define la sabiduría, y la sabiduría no nace de una base de conocimiento, sino de un proceso de evaluación de alternativas que constituyen intentos fallidos previos, hasta aprender la forma correcta de resolver un problema.

La intranet por tanto, no es solo un eficiente medio de comunicación, sino que puede ser una base del conocimiento organizacional. Su ventaja sobre otros medios digitales previos, es su capacidad para manejar información no estructurada y el conocimiento implícito.

La forma como administrar el conocimiento en una intranet, es buscar significado a las colecciones de conocimiento dinámico, distribuido y asincrónico, que existe en el sistema nervioso organizacional, que es el ambiente digital de la organización.

Para manejar este complejo sistema de administración del conocimiento corporativo, se requieren de cinco roles para soportar el contenido formal de un Intranet [4]:

- ✓ El administrador del web.
- ✓ El webmaster.
- ✓ Publicadores.
- ✓ Editores.
- ✓ Autores.

Además se pueden determinar otros roles adicionales, en la medida que la organización alcance la masa crítica y desarrolle su cultura en éste lineamiento. Todos los roles son enfocados en el contenido y no en la tecnología.

El **administrador del web**, es el responsable de facilitar las oportunidades de colaborar entre las diferentes suborganizaciones o repartos involucrados en la organización, y de conducir la infraestructura administrativa del contenido de la organización. Este no es un rol técnico, aunque requiere un entendimiento básico de la tecnología empleada. El administrador del web es primeramente un conductor y un facilitador, en contraste con el webmaster que es el responsable de la infraestructura técnica y la

operación táctica. La misma persona puede tener ambos roles, siempre y cuando posea las habilidades necesarias en cada uno de ellos y tenga el suficiente tiempo.

El administrador del web preside el Consejo Organizacional del Web y podría reportar al Comando General o al Presidente Ejecutivo. Su nivel debe ser de Estado Mayor o de Alta Dirección.

El rol del **webmaster** es una extensión del rol anterior de un administrador de sistemas. Su responsabilidad principal es la instalación de la nueva tecnología, su administración y el soporte a los especialistas funcionales para que la utilicen efectivamente. El webmaster debe dar herramientas que permitan a los usuarios publicar, acceder y personalizar la información por ellos mismos y no hacerlo por ellos. El webmaster tiene responsabilidades en el entrenamiento de los usuarios.

Las organizaciones grandes suelen tener algunos webmasters, cada uno asociado con algún servidor en una suborganización. En este esquema es útil tener un webmaster principal, quien será responsable del soporte de todos los servidores web, coordinando actividades con los webmaster subalternos. Todos ellos forman parte del Comité técnico del web. Las responsabilidades del webmaster principal, también incluyen la administración del

sistema de correo electrónico, del DNS de la organización, las máquinas de búsqueda internas, los índices, herramientas de administración y agentes de análisis de uso de información.

Tradicionalmente el webmaster es responsable de contestar, direccionar y administrar el correo electrónico asociado a la dirección "webmaster@", pero en una organización muy grande esto puede ser un trabajo demasiado absorbente. Hay dos enfoques para solucionar esto, uno es dividir las funciones del webmaster en dos, una función administrativa quien se encargará del correo electrónico y la otra técnica que se encargará de las herramientas y soporte técnico a los usuarios. El otro enfoque es distribuir la carga del correo al "webmaster" dependiendo de la ubicación de la página de la cual se ha enviado el mensaje, entre los webmaster subalternos.

Los **publicadores** determinan que clase de información formal debe crearse y mantenerse en la organización. Cada área (Recursos Humanos, Finanzas, Ingeniería, etc) tiene un publicador.

Generalmente, estos son roles de los administradores de éstas áreas. La responsabilidad de la publicación oficial pertenece a los Comandantes o jefes de esas áreas, aunque casi siempre esta

responsabilidad es delegada. En la era de la información, esta delegación debe ser explícita, y la persona que quede a cargo debe consultar permanentemente al Comando o jefe responsable.

El publicador representa a su reparto en el Consejo Organizacional del web y puede crearse entre ellos un Foro Editorial dentro de la organización. Los publicadores tienen la responsabilidad de crear los procedimientos y políticas que tanto dentro de la organización como del reparto se seguirán. Dentro de las políticas se incluirán las características de la información en cuanto a su integridad y sentido, así como a su ciclo de vida. En las organizaciones grandes el publicador puede delegar el monitoreo y la implementación de las políticas a los editores, sin embargo la responsabilidad es del publicador.

El publicador es responsable de mantener su porción del Mapa de la Organización a su nivel y en niveles inferiores. El Mapa de la Organización es una herramienta utilizada para administrar el contenido del Intranet, el mismo que será discutido en el capítulo siguiente.

Los **editores** se encuentran en las áreas de servicios. Por ejemplo, Recursos humanos pueden tener editores en cada una de sus áreas, esto es Beneficios, Compensación, Retiros, etc. Un

editor suele ser un técnico de mercadeo para cada línea de productos. El editor determina que información oficial debe crearse para actividades específicas y administra la creación de esta información y los procesos para su actualización. Dentro de ésta categoría están los administradores de proyectos.

Los **autores** son quienes crean contenido.

La infraestructura para la administración de una Intranet, se resume en la Figura 2.8.

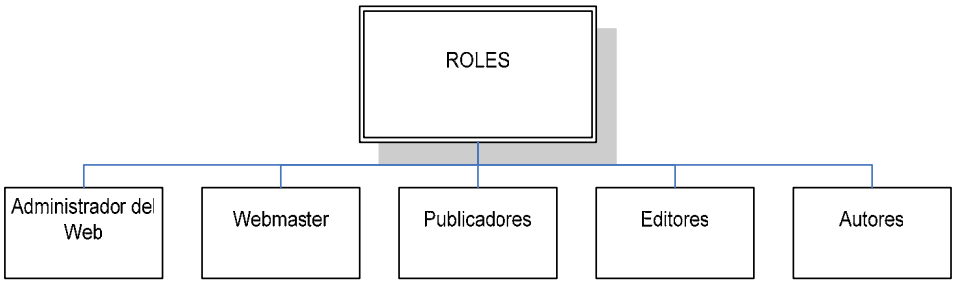


FIGURA 2.8. ADMINISTRACIÓN DE LA INFORMACIÓN EN UNA INTRANET

2.8.2 Roles Organizacionales

Las personas que estarán a cargo de los roles del Intranet requieren de entidades que provean el soporte a la comunicación

y coordinación. Las tres entidades básicas necesarias, tal como se indica en la Figura 2.9 son [4]:

- ✓ El Consejo Organizacional del web.
- ✓ El Foro editorial.
- ✓ El comité técnico del web.

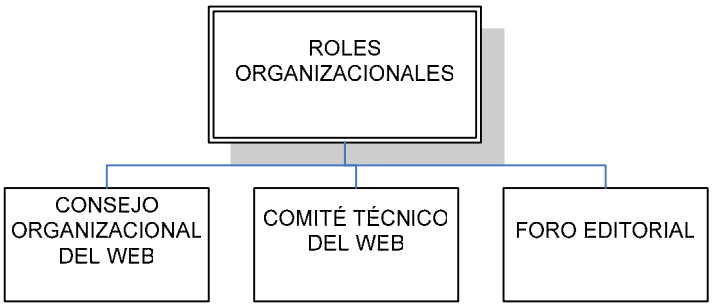


FIGURA 2.9 ORGANISMOS PARA LA ADMINISTRACIÓN DE UNA INTRANET

El **Consejo Organizacional del web** está constituido por los publicadores de toda la organización y es presidido por el Administrador del web. No le conciernen los aspectos técnicos, es responsable de establecer políticas, estándares y guías de estilo al más alto nivel. Aún cuando ésta es una actividad que consume mucho tiempo en sus inicios, pronto se vuelve una tarea que se ejecuta casi en segundo plano. El Consejo Organizacional del web

también es responsable de monitorear el Mapa de la organización para verificar su actualización y la adherencia a los estándares establecidos. Esta tarea también tiende a convertirse en una de segundo plano.

Las funciones que se mantienen a lo largo del tiempo en el Consejo Organizacional del web, es la de comunicación y coordinación, el compartimento de ideas, las aplicaciones y soluciones. Si los miembros asisten a las reuniones buscando formas innovadores de cómo hacer su información más valiosa y accesible, identificando como se puede hacer que la organización sea más efectiva creando y manteniendo su información, entonces el Consejo Organizacional del web se vuelve vital. Pero, si solo se enfoca en políticas y administración del mapa de la organización, sus reuniones pronto carecerán de importancia y la oportunidad de innovar se habrá perdido.

Dos aspectos emergen generalmente del Consejo Organizacional del web. Primero, como no es técnico, ellos descubrirán e identificarán oportunidades que requieran soporte técnico. Es por esto que es bueno que el webmaster principal, sea miembro de este Consejo. Él es el enlace entre éste Consejo y el Comité Técnico.

Segundo, si la organización ha decidido implementar páginas externas, el comité tiene que asegurar que éstas sean creadas y administradas de modo que se presente la misma imagen y presencia corporativa que la que existe en el Intranet.

La Figura 2.10 muestra la composición del Consejo Organizacional del web y sus integrantes.

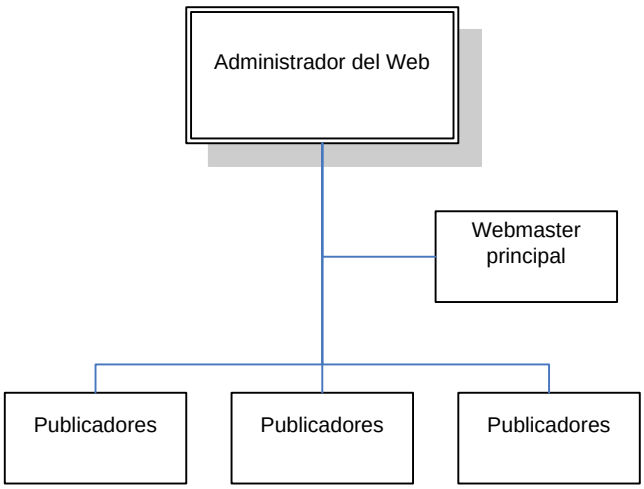


FIGURA 2.10. EL CONSEJO ORGANIZACIONAL DEL WEB

El **Foro Editorial** se crea en base a las necesidades que exista entre los editores. En organizaciones grandes, la administración de la información oficial es delegada a varios individuos. El Foro es una forma eficiente para que los publicadores coordinen

actividades, organicen la información e impartan y monitoreen políticas y estándares.

El Foro Editorial no se enfoca en la tecnología. Se enfoca en crear y mantener el contenido formal siendo eficientes en alcanzar los estándares tanto de la organización como del reparto. Se enfoca en la prensa de bajo nivel enviando sus necesidades emergentes al Consejo Organizacional del web.

Al igual que el Consejo Organizacional del web, es responsable del mapa de la organización en su respectivo nivel. Esta tarea es más compleja que la del Consejo porque tienen que enlazar el mapa de la organización al contenido que ellos administran. El Foro Editorial tiene más que ver con la creación y actualización de la presentación lógica del contenido y sus relaciones.

El **Comité Técnico del web** está constituido por los webmaster de la organización, tal como se muestra en la Figura 2.11. El webmaster principal lo preside. Su enfoque es técnico, se encarga de la definición de estándares técnicos. Este Comité también permite a los webmaster tener la oportunidad de compartir información de herramientas y enfoques innovadores que permitan a los autores, editores y publicadores ser más efectivos creando y manteniendo su propia información.

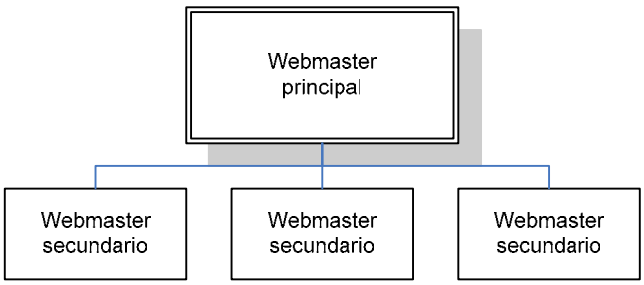


FIGURA 2.11. COMITÉ TÉCNICO DEL WEB

Como se indica en la Figura 2.12, podemos decir que el Intranet está constituido de [11]:

- ✓ **Gente:** La mejor de su clase.
- ✓ **Procesos:** Los mejores que se puedan obtener.
- ✓ **Tecnología:** Quien junta a la mejor gente entre sí con sus procesos.

FIGURA 2.12. ELEMENTOS ESENCIALES DE UNA INTRANET ORGANIZACIONAL

En el siguiente capítulo, se revisará el diseño de la arquitectura de la información, en donde se definirán los procesos que conforman el uso estratégico de la Intranet, para manejo y administración del conocimiento.

CAPITULO 3

3. PLANIFICACIÓN DE LA INTRANET

3.1 Clasificación de las Fuentes de Información [4]

Por lo menos existen tres tipos de fuentes de información en una organización, las que proveerán el contenido a la Intranet:

La información formal, que es la producida y refrendada oficialmente por la organización. Normalmente su exactitud, precisión, actualidad, confidencialidad, confiabilidad y relevancia del contenido, han sido revisadas. Es la información que más le concierne al Comando o Alta Dirección. Incluye los documentos formales que la organización genera sobre sus servicios, procesos y productos. Muchos de estos documentos son los primeros en ser considerados en una implementación de Intranet por su estatus oficial y el interés de su amplia difusión, dada la necesidad de su conocimiento por todos los miembros de la organización.

Información de grupos de trabajo/proyectos, la que se genera dentro de un grupo específico. Se utiliza para comunicar y compartir ideas, coordinar actividades o administrar el desarrollo de un proyecto. Una vez aprobado este o cuando se haya finalizado, su contenido eventualmente será luego de carácter formal. Con este tipo de información, el Intranet tiene un gran potencial, transformando los procesos de trabajo típicamente verticales, en procesos de trabajo horizontales, mejorando tanto la productividad personal como la organizacional. En el Intranet, la información de grupos de trabajo y proyectos no está listada en los directorios generales, y pueden ser sitios protegidos con claves de acceso y/o otros mecanismos de seguridad.

Información informal, notas, memos, reportes, presentaciones individuales y otros trabajos con contenido creativo. Es el resultado de la asimilación de la tecnología en los usuarios una vez identificado lo fácil que es publicar en el Intranet. No solo se refiere a las páginas web personales, sino también al tipo de comunicación y coordinación que se lleva a cabo cuando un individuo pone a consideración sus ideas, pidiendo comentarios o sugerencias vía correo electrónico, formularios de retroalimentación o con libros de registro de visitas. Aún cuando está fuera del alcance de la infraestructura formal, puede ser un punto de

contacto interesante entre el Comando o Alta Dirección y los miembros de la organización.

3.2 Calificación de la Información [14]

En una Organización Militar, además de la clasificación de las fuentes de información que virtualmente proveerán de contenido al web del Intranet, es necesario mantener la calificación de la información formalmente establecida como medida de seguridad de igual manera que se lo hace en las publicaciones en papel, esto es la clasificación de su contenido en:

- ✓ Información ordinaria.
- ✓ Información calificada.

Los documentos calificados a su vez y de acuerdo al grado de reserva , tienen las siguientes categorías:

- ✓ Secretísimo.
- ✓ Secreto.
- ✓ Reservado.
- ✓ Confidencial.
- ✓ Restringido.

A continuación se define brevemente las características de cada una de estas categorías:

Secretísimo.- Documentación o material que contiene información cuya revelación no autorizada podría incidir en un peligro excepcionalmente grave para la nación, con las siguientes consecuencias:

- ✓ Originar un rompimiento definitivo de las relaciones diplomáticas, un ataque armado o guerra contra el Ecuador.
- ✓ Comprometer los planes militares en vigencia.
- ✓ Afectar gravemente los intereses nacionales relacionados con seguridad, desarrollo científico o técnico del país.

Secreta.- Información o material cuya revelación no autorizada podría ocasionar graves consecuencias para la seguridad nacional, tales como:

- ✓ Poner en peligro las relaciones internacionales del Ecuador.
- ✓ Poner en peligro la efectividad de programas militares y políticas directamente relacionados con la seguridad nacional.
- ✓ Comprometer planes militares de defensa u operaciones de inteligencia.

- ✓ Comprometer planes, programas o proyectos de desarrollo científico o tecnológico, de importancia para la seguridad nacional.

Reservada.- Información y material militar que sin estar contemplados en las calificaciones de SECRETÍSIMO o SECRETO, requieren limitación en su conocimiento y distribución para evitar aspectos perjudiciales a la institución militar o seguridad nacional.

Confidencial.- Es aquella que debe ser conocida exclusivamente por la persona o funcionarios interesados en el asunto, y cuya difusión podría afectar investigaciones, y/o, autoridad y reputación de un miembro de las Fuerzas Armadas.

Restringida.- Es la que contiene información de conocimiento solo del personal de las Fuerzas Armadas, cuya difusión podría afectar actuaciones administrativas y originar interpretaciones o comentarios negativos para la institución militar.

Quienes tienen acceso a las diferentes clasificaciones son personal debidamente calificado por la Dirección de Inteligencia de la Armada, una vez que se cumplen los procedimientos reglamentados para dicho efecto. En el establecimiento de la política de seguridad del Intranet, trabajo que por su complejidad se encuentra fuera del alcance de la presente tesis, se deberán observar estas normas y cumplir con las

disposiciones establecidas para implementar los esquemas necesarios que provean los mecanismos de control de acceso a esta información, en base a las regulaciones vigentes y por los organismos calificados y con la autoridad de definición.

3.3 Roles para la Implementación y Administración de la Intranet

3.3.1 Algunas Palabras Previas

El Director de Planificación Estratégica, el Director de Desarrollo Administrativo e Informático, el Director de Organización y Doctrina, actuarán como delegados del Comandante General de Marina, pero con el respaldo de éste, para que con los especialistas en tecnología y sistemas de información puedan guiar a la Organización durante el diseño y la implementación del Intranet, observando las siguientes guías [11]:

1. **Conformar un Consejo para la implementación del Intranet.-** Este Consejo debe estar conformado primeramente por un número suficiente de usuarios finales, asegurándose de incluir gente con experiencia en el uso del Internet, tanto como gente sin ninguna experiencia en el uso de Internet. Los usuarios deben venir de todas las áreas que conforman la organización, asegurándose así que estas tengan

representantes en el Consejo. Además forman parte del Consejo el personal designado como Fuerza de Tarea para el diseño y la implementación del Intranet. Es muy importante que el Comando General o la Alta Dirección tengan una participación activa en el Consejo.

2. **Designar un responsable del proyecto.-** Se debe encontrar una persona clave que tenga un buen entendimiento de la tecnología de Intranet, y además tenga muy clara la visión, misión y objetivos de la organización. Esta persona clave debe tener mucha habilidad para trabajar con un grupo de personas con diferentes personalidades e intereses, y por tanto ser hábil para resolver conflictos, obtener consensos y tomar decisiones. Debe ser una persona capaz de obtener todo el respaldo del Comando General o la Alta Dirección, y por tanto ejercer la autoridad necesaria.

3. **Planificar adecuadamente el presupuesto.-** A pesar de que la tecnología de Intranet es relativamente barata, hay que hacer un análisis muy frío de que inversión es necesaria hacerse para reutilizar la infraestructura existente de modo que las redes de datos que ya existen y sus computadoras,

puedan integrarse debidamente considerando las mejoras tanto en hardware como en software que sean necesarias.

4. **Planificar cómo mantener actualizado el contenido.-** Uno de los más grandes beneficios del Intranet, es la habilidad de permitir a los usuarios un acceso rápido a información actualizada. Esto sin embargo significa que alguien debe mantener los sitios de información al día, por tanto se requiere de un cuidadoso diseño de la arquitectura lógica de la información que garantice esto.

5. **Mantener tecnología abierta.-** Se debe buscar software y hardware flexible y adaptable. Hay que evitar al máximo candados propietarios, y maximizar las alternativas adoptando productos basados en estándares - código abiertos.

6. **Adoptar una actitud hacia el soporte.-** Mientras no se supere la curva de aprendizaje, hay que ser paciente con las tareas de soporte, proveer mecanismos de ayuda en línea y planificar seminarios, talleres y cursos como parte de un plan de entrenamiento.

7. **Promover el Intranet.-** Desde un inicio hay que promover la idea de que el proyecto del Intranet es importante para la

organización. El proyecto debe tener un nombre de pila, por ejemplo "NavNet". Una vez que se dispone de contenido en los primeros sitos de información, hay que añadir valor agregado en él para capturar el interés de los usuarios y promover su uso.

3.3.2 Guía de Implementación de la Intranet

Lo idóneo para abarcar un proyecto de esta magnitud, el mismo que contempla resolver la administración de la información en la Armada, de acuerdo a las normas y posibilidades habilitadas por la tecnología propuesta, es empezar conformando la Fuerza de Tarea de la Intranet, la misma que tiene las siguientes metas:

- Entender las habilidades necesarias en administración, técnicas y reglas del negocio para desarrollar, implementar y mantener la infraestructura y aplicaciones planificadas para el Intranet.
- Determinar los recursos de personal requeridos para la implementación del proyecto y para el mantenimiento en su ciclo de vida.
- Desarrollar un plan de entrenamiento para la Fuerza de Tarea que se integre al plan de implementación del Intranet.

- Apuntalar y ampliar el expertismo interno con el entrenamiento que se considere necesario.
- Contratar expertismo externo para proveer las habilidades técnicas necesarias en el inicio y corto plazo.

3.3.2.1 Entrenamiento de usuarios

En términos generales, la tecnología de intranet es fácil de aprender y utilizar por las siguientes razones:

- Los recursos del Intranet (aplicaciones, documentos y datos) son accedidos a través de una sola interface, el navegador web como cliente universal.
- El nuevo paradigma de Intranet aumenta y extiende las habilidades administrativas, técnicas y las reglas de negocio existentes.
- El Intranet está basado en estándares y protocolos abiertos, asegurando así una flexibilidad en la asimilación de nuevas características técnicas, aplicaciones o servicios.

Por tanto las necesidades de entrenamiento se limitan al uso del navegador web para la mayoría de usuarios de la Intranet. El entrenamiento para productos adicionales y

aplicaciones específicas solo se requiere para aquellos usuarios quienes necesitan utilizarlas.

3.3.2.2 El equipo de desarrollo

El proceso de implementación de la Intranet puede incluir las siguientes fases típicas: evaluación, diseño, desarrollo, implementación y mantenimiento. En cada una de estas fases se requiere una mezcla particular de habilidades y experiencia, por lo tanto se debe contemplar los roles individuales requeridos para la planificación de recursos de personal.

Fase de evaluación.

Roles:

(Ver Apéndice A para la descripción de los roles)

- Administrador del proyecto.
- Comando General o Alta Dirección a través de su delegado.
- Director de tecnología de información de todas las áreas funcionales. (Director de Comunicaciones y Director de Informática).
- Representantes de los proveedores claves de tecnología.

- Analistas de la línea de acción de la organización (áreas de operaciones, logística, inteligencia militar, comunicaciones, organización y personal).
- Consultores con conocimientos estratégicos de la línea de acción de la organización y conocimientos técnicos.

Fase de diseño.

Roles:

(Ver Apéndice A para la descripción de los roles)

- Administrador del proyecto.
- Administradores de redes de las áreas involucradas.
- Responsables de la seguridad institucional. (Dirección de Inteligencia).
- Consultores con habilidades en el diseño de redes LAN y WAN, topologías, planificación de crecimiento y plataformas.
- Representantes de los proveedores claves de tecnología.

Para la implementación del contenido del Web:

- Arquitectos de información.
- Poseedores y desarrolladores de contenido.

Para la implementación de aplicaciones:

- Analistas de sistemas y de la línea de acción de la institución.
- Administradores de bases de datos y aplicaciones.
- Desarrolladores de aplicaciones.
- Administradores de aplicaciones de trabajo en grupo como: mensajería electrónica o grupos de discusión.
- Fuerza de Tarea de estandarización.
- Representantes de la Dirección de Educación, entrenamiento y soporte.
- Especialistas de otras áreas según sea necesario.

Fase de desarrollo.

Roles:

(Ver Apéndice A para la descripción de los roles)

- Administrador del proyecto.

Para la implementación del contenido del web expertos en:

- Arquitectos de información.
- Proveedores de contenido.
- Desarrolladores de contenido.
- Autores o programadores web, con conocimientos de HTML, XML, software de tratamiento de gráficas, sonido y video.

Para la implementación de aplicaciones expertos en:

- Administradores de bases de datos y aplicaciones.
- Desarrolladores de aplicaciones.
- Programadores.
- Inspectores de control de calidad.
- Desarrolladores de entrenamiento.

Fase de implementación.

Roles:

(Ver Apéndice A para la descripción de los roles)

- Administrador del proyecto.
- Administradores de redes de datos involucradas para: instalación, configuración, afinamiento de desempeño y pruebas.
- Administrador de aplicaciones para: instalación, configuración, afinamiento de desempeño y pruebas.
- Instructores.

Fase de mantenimiento.

Roles:

(Ver Apéndice A para la descripción de los roles)

- Administrador del sistema.

- Administrador de la red.
- Administrador de los servidores.
- Administrador de aplicaciones.
- Administrador de clientes.
- Soporte informático.
- Webmaster.

3.3.3 Normas para Establecer los Sitios Web

Una vez revisada la infraestructura lógica, que permite a la organización administrar el conocimiento disponible en la Intranet, las siguientes normas para el establecimiento de sitios web, se enfocan en la creación de contenido.

El web es un sistema de comunicación basado en hipertexto. Técnicamente, el web es un sistema para intercambiar datos a través de redes de computadoras, utilizando para ello software especial: un navegador web, y un servidor web.

El web habilita la diseminación y la recolección de información (a través de formularios hechos en HTML), por lo que es un sistema de comunicación interactivo que puede tener una audiencia de tamaño arbitrario, que va desde una sola persona (el creador), a un grupo o comunidad (alcance limitado de usuarios por ejemplo:

una intranet), e incluso a una audiencia masiva (alcance público, por ejemplo: el Internet).

Una metodología de desarrollo de información para el web

A diferencia del desarrollo de información para sistemas de comunicación tradicionales, en los que a pesar de reconocer la necesidad de revisar, mantener y reevaluar el contenido de la información; tarea que finalmente algún momento se detiene debido a la naturaleza de los medios en los que se codifica la información, sean estos: papel, CD-ROM's, etc., en el desarrollo de información para el web, lo primero que hay que reconocer es que la información que existe en un sitio, es dinámica y no estática; lo que demanda una metodología formal que garantice el buen funcionamiento del sitio como tal.

En la metodología que se define, se reconoce que la información de la audiencia pretendida para el sitio web es un elemento intrínseco, por lo que el desarrollador deberá: analizar, diseñar e implementar la información considerando permanentemente la audiencia pretendida. La información que se tenga de esta audiencia juega un rol crucial, y todos los procesos de la metodología mencionada dependen de la información que se tenga de la audiencia pretendida.

La metodología para desarrollar sitios web contiene la mayoría de elementos utilizados para desarrollar información en medios tradicionales; pero los procesos son más abiertos debido a que el producto final (el sitio web operativo), no es estático, sino que está sujeto a cambios permanentes en su contenido.

En la Figura 3.1 se ilustra los elementos de la metodología y sus procesos, los mismos que son descritos en detalle en el Apéndice B; la metodología mantiene a los elementos interconectados [7]:

FIGURA 3.1. ELEMENTOS Y PROCESOS DE LA METODOLOGÍA DE DESARROLLO DE SITIOS WEB

3.3.4 Acerca de los Servicios de una Intranet

Los servicios de una Intranet, corren sobre una red TCP/IP, y ofrecen las siguientes ventajas con respecto a las aplicaciones tradicionales [4]:

- ✓ **Uso de estándares y protocolos abiertos.-** Debido a que una Intranet está basada en los estándares y protocolos abiertos y públicos del Internet, sus aplicaciones no están atadas a soluciones propietarias. Esta flexibilidad asegurará la interoperabilidad con otras aplicaciones similares y sobre todo una inversión durable en el tiempo, libre del costo inmerso de un candado propietario.

- ✓ **Acceso restringido a la información.-** Los servicios de una Intranet, al ser de dominio corporativo, pueden tener un acceso restringido, implementado a través de un sinnúmero de métodos disponibles como: autenticación de usuario, certificación, protocolos seguros, encriptación y firewalls o corta fuegos.

- ✓ **Eficiencia en cuanto a los costos.-** Los servicios de una Intranet son relativamente baratos de diseñar, desarrollar y mantener, lo que asegura un bajo costo de tenencia.

Normalmente se reutilizan los componentes de las redes de datos existentes, con ciertas mejoras a la infraestructura general.

- ✓ **Uso del cliente universal.-** El navegador web, es la única interface necesaria, por lo que se lo conoce también como cliente universal. Este provee una interface común, intuitiva y estandarizada de muy fácil uso; por lo que los costos de entrenamiento son menores, tan solo se trata de apuntar en los temas de interés y hacer click en ellos para revisarlos.

- ✓ **Acceso total.-** Los servicios de una Intranet, son accesibles vía TCP/IP para cualquier navegador autorizado en la red que corra sobre un computador de cualquier plataforma o cualquier dispositivo inalámbrico de nueva generación, sin importar su ubicación geográfica. La red posee la inteligencia suficiente para garantizar el acceso oportuno a la información.

- ✓ **Independencia de plataforma.-** Los servicios de una Intranet, pueden correr en muchas plataformas. Los autores desarrollan una aplicación una vez, para que corran dondequiera. De esta manera se evita el gasto de migrar las aplicaciones cuando se

actualicen o cambien las diferentes plataformas que se utilicen en la organización.

- ✓ **Independencia de la base de datos.-** Los servicios de una Intranet, pueden interactuar con cualquier base de datos, sin necesidad de clientes especializados, utilizando desde consultas dinámicas hasta transacciones complejas.

- ✓ **Escalabilidad.-** Los servicios de una Intranet, son totalmente escalables acorde con la funcionalidad demandada por la organización. Las aplicaciones pueden escalar desde las diferentes redes de área local hasta las redes de área extendida, e incluso Internet, sin necesidad de reescribir ningún código.

- ✓ **Robustez.-** Los servicios de una Intranet, se construyen sobre una tecnología robusta y probada en el Internet. Actualmente se cuenta con herramientas de desarrollo, servidores y herramientas de administración seguras, confiables y probadas.

- ✓ **Ambiente enriquecido.-** Los servicios de una Intranet, ofrecen una amplia variedad de medios de información, como texto, gráficos, sonido y video.

3.3.5 Criterios de Selección de Servicios de una Intranet [11]

A continuación, se listan algunos de los criterios que son considerados, para la selección de servicios en una Intranet, para una organización:

- ✓ **Retorno de la Inversión.-** Normalmente existe un Retorno de la Inversión (ROI) muy elevado y de corto plazo. Este es un aspecto muy relevante actualmente en la Armada.
- ✓ **Presupuesto.-** Se debe considerar los costos de inversión iniciales y los costos de mantenimiento, proyectándolos al ciclo de vida del sistema. En conjunto son normalmente inferiores a otras alternativas. El proyecto tiene un presupuesto plurianual y considera tanto inversión en equipamiento, como gastos de administración y manutención. Conforme a la doctrina de planificación presupuestaria de la Armada según su plan director, es un proyecto integral plurianual.
- ✓ **Fortalecer las necesidades de los procesos de gestión.-** Proveer valor agregado a procesos claves de gestión. La aplicación adecuada de la tecnología puede lograr reducir considerablemente los tiempos y costos innecesarios en los procesos, aerodinamizando la gestión institucional. Otro ejemplo de aplicación puede ser el acceso permanente a las

fuentes de información que permita la colaboración de equipos de trabajo dispersos geográficamente, tal cual es la realidad de la Armada.

- ✓ **Anticipación en los requerimientos de recursos.**- Se debe mejorar la infraestructura tecnológica ya existente en algunos repartos de la Armada. En la medida que cambia la cultura tecnológica de los usuarios, aumenta la demanda de mayor disponibilidad y la dependencia organizacional del sistema.
- ✓ **Valor promocional.**- Considerar pilotos como el implementado en éste trabajo en el Instituto Oceanográfico de la Armada, que demuestren las capacidades y bondades a los Directivos y usuarios.
- ✓ **Valor educacional.-** Considerar procesos de aprendizaje durante el desarrollo, implementación, administración; requerimientos de entrenamiento y requerimientos de infraestructura adecuada para lograr desarrollar una cultura informática en los usuarios para facilitar el proceso de cambio.
- ✓ **Alcance de la audiencia.-** Habilidad necesaria para alcanzar el mayor número de usuarios del segmento previsto como comunidad de usuarios para cada uno de los diferentes servicios ofrecidos, contando con al menos un servicio (mensajería electrónica o mensajería instantánea) de gran

difusión a todo nivel (Oficiales, Tripulantes y Empleados Civiles).

- ✓ **Grado de complejidad.**- Considerado especialmente por el nivel de dificultad para el desarrollo de aplicaciones orientadas al web, entrenamiento de los desarrolladores, entrenamiento de los usuarios y mantenimiento.
- ✓ **Reusabilidad.-** Habilidad para reciclar componentes de programas en otras aplicaciones a nivel Institucional.

Las características de una aplicación piloto deben ser las siguientes:

- ✓ Simple, fácil y rápida de desarrollar e implantar.
- ✓ Un retorno de inversión obvio y rápido, con una tasa dramáticamente alta.
- ✓ Una herramienta absolutamente demostrativa que venda la Intranet al Comando y a los nuevos usuarios.
- ✓ Mejoras demostrables inmediatamente en los procesos más familiares.

3.3.6 Tipos de Servicios para una Intranet

Existen dos tipos básicos de servicios dentro del concepto de una Intranet: los servicios de usuarios, que suministran recursos y aplicaciones al usuario final; y los servicios de red, que permiten interconectar y ejecutar el entorno de red organizacional [11].

Los servicios de usuarios disponibles son los siguientes:

- ✓ Publicación y administración de la información.
- ✓ Comunicación y colaboración.
- ✓ Navegación por las fuentes de información.
- ✓ Acceso a aplicaciones.

Los servicios de red de una Intranet son los siguientes:

- ✓ Directorios de usuarios y recursos.
- ✓ Replicación de información.
- ✓ Mecanismos de seguridad.
- ✓ Administración de los servicios.

3.3.6.1 Publicación y administración

Incluyen la creación, publicación y administración de documentos HTML/XML en línea, con sus gráficos, audios

y videos asociados en los diferentes sitios web. Estos documentos una vez publicados, están inmediatamente disponibles a través de la red TCP/IP para cualquier usuario, de cualquier plataforma, con una navegador web, y los suficientes derechos de acceso. El ejemplo más común para esta aplicación, es la publicación de la información formal de la organización, como: políticas y manuales de procedimientos, órdenes generales, directivas generales permanentes y temporales, leyes y reglamentos, planes de proyectos, artículos de prensa, anuncios oficiales, horarios y descripción de cursos, investigaciones y material didáctico.

Para facilitar la navegación y la consulta de la información a los usuarios, sin que se demande un conocimiento exacto de la ubicación física o lógica de la información, es muy conveniente considerar el uso de sistemas de catalogación y máquinas de búsqueda, así como agentes descubridores de contenido.

3.3.6.2 Comunicación y colaboración

Este tipo de aplicación, habilita el uso de comunicaciones privadas, colaborativas y grupos de discusión públicos o

limitados, a los usuarios de la Intranet. Algunos ejemplos pueden constituir: el uso del correo electrónico (SMTP, POP, MIME y IMAP4) y grupos de discusión (NNTP). Para este tipo de aplicaciones resulta útil también incluir algún tipo de servicio de directorio, con información personal de los usuarios del sistema, así como sus claves personales públicas, de modo que se facilite la validación de los derechos de acceso de los usuarios.

3.3.6.3 Navegación por las fuentes de información

Es un servicio que se provee a través de los protocolos en los que se basa el World Wide Web, HTTP para la transmisión de la información desde los servidores hacia los clientes, y HTML/XML el lenguaje que estandariza o describe el contenido de las páginas web. El navegador web interpreta las etiquetas utilizadas en HTML, para de acuerdo a ello mostrar el contenido debidamente.

3.3.6.4 Acceso a las aplicaciones basadas en red

La principal aplicación de estos servicios, es la integración de bases de datos y sistemas de información. Son programas normalmente desarrollados en Java, JavaScript, C#, o algún tipo de CGI (Common Gateway Interface)

como PHP, que utilizan scripts o APIs, como JDBC, para interactuar con la base de datos, o a través de un controlador nativo proporcionado por el fabricante de la base de datos. El uso más frecuente de este servicio, puede ser para transacciones comerciales en línea, desarrolladas para apoyo a la logística institucional; consulta de existencias de suministros y repuestos; ingreso de reportes de uso de maquinaria en las unidades de abordo; aplicaciones de recursos humanos para la Dirección General del Personal; servicios de información oceanográfica e hidrográfica.

3.3.6.5 Aplicaciones administrativas

Las aplicaciones administrativas ayudan a mantener juntos los servicios que corren en el ambiente general de la red. Estos servicios son: directorios, información de derechos de acceso, replicación y administración.

Las aplicaciones de directorios, proveen un sitio seguro y centralizado de información de los usuarios y recursos de la red, derechos de uso de aplicaciones específicas, control de accesos, claves públicas, certificados digitales y configuración de servidores. De esta manera, se mantiene

un perfil para cada usuario, en el que consta la información de contacto de éstos, así como también sus derechos de acceso a los diferentes servicios. Este servicio se combina con mecanismos de control de acceso, encriptación, claves de autenticación, Firewalls ó corta fuegos y protocolos seguros, para impedir accesos no autorizados a la información y servicios disponibles en la red.

Las aplicaciones de replicación, maximizan la eficiencia, utilización y desempeño de la red, distribuyendo estratégicamente los datos a través de la intranet, reconciliando los cambios en las diferentes copias cuando sea necesario, o el tráfico en la red lo permita. Un ejemplo de lo que debe estar distribuido son: contenido del web, grupos de discusión, directorios y casilleros de mensajería.

Con el objetivo de facilitar la navegación de los usuarios a través de las fuentes de información, se cuenta también con el servicio de catalogación, el mismo que crea una indexación de los documentos HTML/XML disponibles, búsqueda de estos documentos y su exploración.

Otras aplicaciones administrativas dan a los administradores del sistema las herramientas para

administrar los servidores, aplicaciones, servicios y otros recursos desde cualquier parte del Intranet, a través de un navegador web, utilizando para ello protocolos estándares de administración como SNMP.

3.4 Requerimientos Básicos de Seguridad y Disponibilidad de la Información

El plan de modernización de las comunicaciones de las Fuerzas Armadas contempló la implantación de un sistema nacional de comunicación, basado en una red estratégica de enlaces microondas que unirá las dependencias de las diferentes Fuerzas y será la estructura tecnológica que de soporte a la transferencia de información digital tanto operativa como administrativa en la Institución. Pero antes debe prepararse concienzudamente un plan informático dentro del cual se defina cuáles serán los nuevos sistemas de información a desarrollarse y que harán uso de esta infraestructura, y cuáles serán los esquemas de seguridad a implantarse para cubrir los requerimientos que exigen la doctrina militar: manejar diferentes grados de seguridad de la información.

La Armada tiene una estructura organizacional bien definida, en donde la Dirección de Inteligencia tiene la responsabilidad específica de

realizar estudios, evaluaciones y recomendaciones de normas de seguridad para los Repartos [14]. Ésta Dirección es la llamada a emitir nuevas disposiciones en cuanto a políticas, estándares, procesos y procedimientos de seguridad a ser aplicados en sistemas de misión crítica en un ambiente de Intranet, cuya importancia convierten a estos sistemas en activos que deben ser protegidos.

El tema de la seguridad de redes es muy amplio por sí solo y un análisis aplicado al caso a la Armada escapa al alcance de éste trabajo y sería motivo de otro trabajo de investigación. Por ello nuestro objetivo en la presente sección es aportar con guías básicas y prácticas a ser utilizadas para a futuro definir las Políticas de Seguridad Informática de la institución, donde se establezca la forma como se controlará el uso y responsabilidades en la red, el diseño del modelo de seguridad y los planes de contingencia o planes de acción cuando se detecte violaciones a las políticas.

En esta sección se mencionará cuales son los aspectos generales de seguridad de la información, los requerimientos básicos de seguridad en la red que deben ser cubiertos, los análisis técnicos que conducen a definir el modelo seguridad a implantar y una descripción general de las herramientas de seguridad actualmente disponibles para implementar los servicios de seguridad conforme a las políticas establecidas.

3.4.1 Aspectos generales de la seguridad de la información.

La necesidad de seguridad de la información es mayor ahora que antes y ello demanda que los ***"profesionales de la información se conviertan también en profesionales en la protección de la información"***. Pero concretamente, ¿Qué es la seguridad en una red?; podemos decir que ***"Es el conjunto de medios para proteger la información, no importa donde ésta resida o viaje en la red"*** [15].

Debido a la difusión de las tecnologías de la información, la mayoría de las organizaciones actuales están expuestas a una serie de riesgos derivados de una inadecuada protección de la información en sus sistemas de información automatizados. Las causas más comunes que le dan una tendencia creciente a ésta vulnerabilidad son: Primero, la gran expansión del empleo de computadoras personales que ha magnificado el problema de la implantación de seguridad en sistemas de información, debido especialmente a la carencia de controles de seguridad básicos en éste tipo de sistemas; En segundo lugar la evolución de las organizaciones hacia entornos con acceso global y múltiple, con un aumento de la conectividad entre distintas organizaciones, lo que plantea retos importantes en la gestión de la seguridad.

Los riesgos comúnmente asociados con la incorrecta protección de la información son:

- Revelación a personas no autorizadas.
- Inexactitud en los datos.
- Inaccesibilidad de la información cuando se necesita.

La seguridad de la información por tanto se basa en tres aspectos fundamentales que debe cubrir un sistema de información automatizado seguro [16]: **Confidencialidad, Integridad y Disponibilidad (Figura 3.2).** Preservar éstas tres características de la información constituye el objetivo principal de la seguridad de la información.

FIGURA 3.2. ASPECTOS FUNDAMENTALES DE UN SISTEMA DE INFORMACIÓN SEGURO

Existen además otros aspectos de seguridad que pueden considerarse estar incluidos en los tres aspectos fundamentales

mencionados, pero que es importante considerarlos: Autenticidad, Imposibilidad de rechazo (no repudio), Consistencia, Aislamiento y Auditoría

Para tener una apreciación global de lo que representa la seguridad de la información, tenemos que considerar los aspectos que ésta engloba, los elementos a proteger, los tipos de amenazas que contra ellos se presentan y el origen de tales amenazas; tal como se trata de sintetizar en una visión global de la seguridad de la información, como se muestra en la Figura 3.3 [17]:

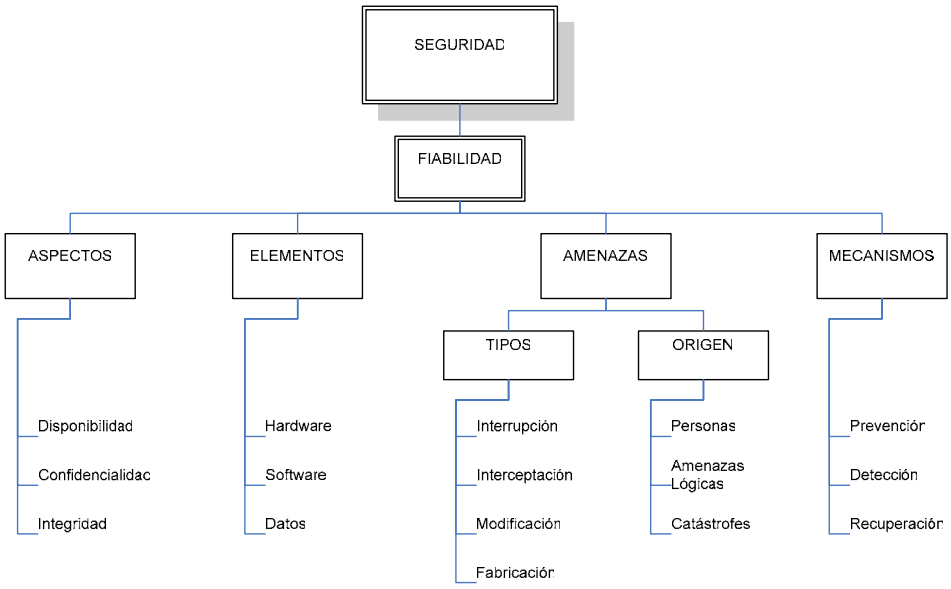


FIGURA 3.3. VISIÓN GLOBAL DE LA SEGURIDAD DE LA INFORMACIÓN EN UN AMBIENTE INFORMÁTICO

En general, se requiere que la información esté donde uno quiere cuando uno lo quiera. Que ésta sea confiable y precisa. Se quiere que esté lejos de personas no autorizadas y que estemos seguros de que no ha sido alterada.

A continuación daremos una definición de los aspectos fundamentales de seguridad [18]:

Confidencialidad.

Se entiende por confidencialidad el aspecto de seguridad, o condición de un sistema informático, que asegura que la información en él contenida, no esté disponible o no pueda ser descubierta por personas, entidades o procesos no autorizados para ello. A veces es denominada secretismo o privacidad. En áreas gubernamentales, especialmente en las relacionadas con la seguridad interna y externa, como es el caso de la Armada, éste es un aspecto primordial sobre los otros. Algunos de los mecanismos para salvaguardar la confidencialidad de los datos son: técnicas de control de acceso a los sistemas, y cifrado de la información confidencial, tanto almacenada como en las comunicaciones.

Integridad.

Se entiende por integridad el aspecto de seguridad que garantiza que los datos pueden ser modificados, incluyendo su creación y borrado, sólo por personas autorizadas de hacerlo. A la integridad se añaden otros conceptos análogos como: precisión (*accuracy*) y autenticidad (*autenticity*). El concepto de integridad implica que el sistema no puede modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Evita que los datos sean falseados, garantiza que los datos que fueron recibidos o recuperados, son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. El problema de la integridad no solo se refiere a modificaciones intencionadas, sino también a cambios accidentales. En el ámbito de las redes la integridad tiene un complemento que es la autenticidad, que tiene que ver con la provisión de medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos. Algunos de los mecanismos para salvaguardar la integridad, están relacionados con la criptografía que presenta varios métodos para mantener y asegurar la autenticidad de los mensajes y la precisión de los datos recibidos; éstos algoritmos criptográficos añaden códigos o firmas a los mensajes en el origen, para que en el

destino sean recalculados y comparados. Esto no solo asegura la integridad de los datos, sino la autenticidad de la misma y el no repudio.

Disponibilidad.

Se entiende por disponibilidad, el grado en que un dato está en el lugar, momento y forma, según como ha sido previamente acordado, cuando es requerido por un usuario autorizado. Tiene que ver con capacidad de acceder a un sistema de información en un tiempo de espera considerado aceptable, según acuerdos preestablecidos.

Disponibilidad quiere decir que el sistema, es decir tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo. Una de las amenazas y ataques más comunes contra la disponibilidad, es el ataque de “negación de servicio” (*Denial of Service*). Esto significa que los usuarios no pueden obtener los servicios esperados del sistema, porque:

- El computador puede haber sido estropeado, o se produjo una caída del sistema operativo; o,

- No hay suficiente memoria (recursos) para ejecutar los servicios (programas); o,

- Los discos, cintas o impresoras no están disponibles, o están llenos; o,

- No se pueden acceder a las bases de datos.

El libro Orange Book es uno de los documentos más influyentes que existen y donde se detallan los estándares y prácticas comúnmente aceptadas en las organizaciones como las bases para la elaboración de las propias políticas de seguridad [16].

Así mismo, la norma internacional ISO 17799, es un estándar detallado de la administración de seguridad de la información aprobado en Diciembre del 2000, basado totalmente en la norma británica BS 7799. El ISO 17799 es una colección de códigos de práctica, que ayudan a la implantación de una seguridad de información de seguridad total. Incluye las siguientes partes [19]:

- Descripción de la seguridad de la información, porqué es necesaria la seguridad de la información, como evaluar los requerimientos de seguridad, y como evaluar los riesgos y asignar controles de seguridad.

- En la Sección 1 y 2, se describe el alcance del estándar, y la definición de términos.

- La sección 3 está dedicada a la Política de Seguridad.

- La sección 4 describe la organización necesaria para administrar la seguridad.

- La sección 5 cubre la clasificación de bienes y activos, y su control.

- La sección 6 cubre los aspectos del personal.

- La sección 7 cubre la seguridad física y ambiental.

- La sección 8 se encarga de la administración de las operaciones informáticas relacionadas con la información, y las comunicaciones.

- La sección 9 tiene que ver con el control de acceso a los sistemas.

- La sección 10, cubre los aspectos de desarrollo y manutención de sistemas.

- La sección 11, los aspectos de planificación de la continuidad del negocio.

- La sección 12, cubre los aspectos de conformidad de la norma, considerando regulaciones, leyes y reglamentos.

Cómo podemos ver, la cobertura del enfoque integral de la administración de la seguridad de la información, está debidamente regulada y cubierta por éste estándar internacional.

3.4.2 Política de Seguridad Informática

La política de seguridad informática de una organización es un conjunto de reglas y procedimientos que indican como la organización responde a las amenazas contra su información, y como se reducen las debilidades en la operación de los sistemas que administran dicha información. La política dará las pautas necesarias para adoptar las medidas de seguridad que permitan proteger los recursos de la red contra pérdidas y daños.

La política de seguridad establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización. No se trata simplemente de una descripción técnica de mecanismos de seguridad, ni de una

expresión legal que involucre sanciones. Es más bien una descripción de lo que deseamos proteger y el por qué de ello.

Elementos de una política de seguridad informática

La política debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la organización para lograr una visión conjunta de lo que se considera importante.

La política debe considerar entre otros, los siguientes elementos:

- Alcance de la política, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito institucional.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cubre el alcance de la política.

- Definición de violaciones y de las consecuencias de la falta de cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que tienen acceso.

Las políticas deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

Por otra parte, la política debe especificar la autoridad que debe hacer que las cosas ocurran, el rango de los correctivos y sus actuaciones que permitan dar indicaciones sobre la clase de sanciones que se puedan imponer. Finalmente, las políticas, como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: incremento, disminución o rotación del personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios entre otros.

Guías para establecer una política de seguridad informática

Para desarrollar la política de seguridad en una organización es necesario considerar los siguientes pasos [15]:

a) **Determinar la importancia y el riesgo de los recursos con que dispone la organización.-** Como se requiere orientar los esfuerzos a proteger los puntos más sensibles de la red, se vuelve imprescindible hacer un análisis técnico que nos permita identificar cuáles son los recursos con mayor riesgo. Las preguntas que debe contestarse aquí son:

- ¿Qué es lo que se necesita proteger?
- ¿De qué o quienes se necesita protegerlos?

Se debe determinar lo siguiente:

- Identificación de los recursos
- Identificación de amenazas
- Cálculo del riesgo

b) **Determinar la relación entre los usuarios y los recursos.-** Aquí se identifica a los usuarios que puedan acceder a los recursos y que están autorizados hacer con ellos.

Las preguntas que deben ser contestadas aquí son:

- ¿A quién es permitido el uso de recursos?
- ¿Cuál es el uso apropiado de los recursos?
- ¿Quién está autorizado a otorgar accesos y aprobar usos?

c) **Diseñar el modelo de seguridad.-** Que en base a la información obtenida anteriormente nos permita diseñar las

estrategias de seguridad para brindar protección a los puntos más sensibles de la red.

En el gráfico de la Figura 3.2 se pueden visualizar todos los elementos que intervienen para el estudio de una política de seguridad. Se comienza realizando una evaluación del **factor humano** que interviene – teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad, de los **mecanismos** con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, el **medio ambiente** en que opera el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las **amenazas posibles**.

Una vez evaluado todo lo anterior, se origina un programa de seguridad, que establece los pasos a dar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino.

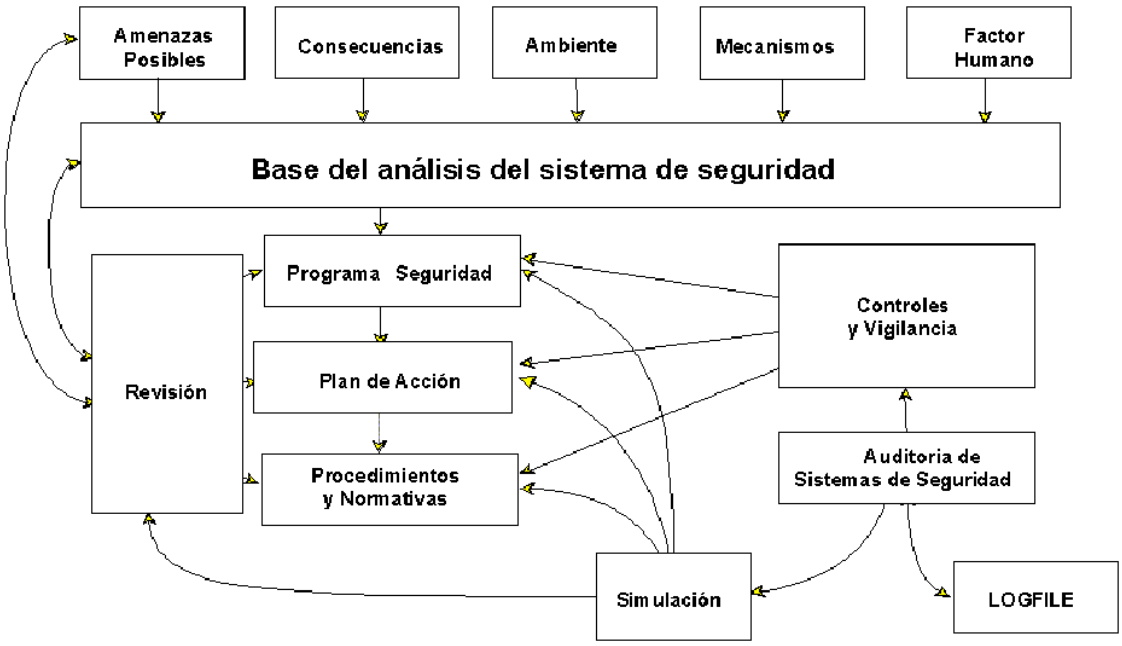


FIGURA 3.4. DIAGRAMA PARA ANÁLISIS DE UN SISTEMA DE SEGURIDAD

Con el propósito de asegurar el cumplimiento de todo lo anterior, se **realizan los controles y la vigilancia** que aseguren el fiel cumplimiento de los tres puntos antepuestos. Para asegurar un marco efectivo, se realizan auditorías a los controles y a los archivos de registro o logs, que se generen en los procesos implementados (de nada vale tener archivos de registro si nunca se los analizan o se los analizan cuando ya ha ocurrido un problema).

Con el objeto de confirmar el buen funcionamiento de lo creado, se procede a simular eventos que atenten contra la seguridad del

sistema. Como el proceso de seguridad es un proceso dinámico, es necesario realizar revisiones al programa de seguridad, al plan de acción y a los procedimientos y normas. Estas revisiones, tendrán efecto sobre los puntos tratados en el primer párrafo y, de esta manera, el proceso se vuelve a repetir.

Es claro que el establecimiento de políticas de seguridad es un proceso dinámico sobre el que hay que actuar permanentemente, de manera tal que no quede desactualizado; que cuando se descubran debilidades, éstas sean subsanadas y, finalmente, que su práctica por los integrantes de la organización no caiga en desuso.

3.4.3 Modelo de Seguridad [15]

Las políticas de seguridad informática necesitan de una serie de medidas de diferente índole para su implementación, en las que se combinan aspectos organizacionales, lógicos y físicos, que apuntan a prevenir, detectar y corregir ciertas falencias o mal usos de los sistemas de información:

a) **Medidas de Seguridad Organizacionales.-** Se refieren al personal y la administración de los sistemas. Se incluyen aspectos como responsabilidades, administración y procedimientos de seguridad.

b) **Medidas de Seguridad Físicas.-** Tienen que ver con la protección externa de los sistemas. Proteger los sistemas de amenazas externas como por ejemplo accesos físicos a salas de cómputo y equipos de comunicaciones, protección contra incendios, robos, inundaciones, etc.

c) **Medidas de Seguridad Lógicas.-** Se refieren a las amenazas internas en los sistemas. Incluyen las medidas para asegurar la integridad, confidencialidad, disponibilidad y registro transaccional de los datos o información digital. Aquí se contemplan técnicas como autenticación, control de acceso, firmas digitales, auditorías del sistema y uso de criptografía.

3.4.4 Servicios de Seguridad

Para hacer frente a las amenazas a la seguridad se definen los servicios de seguridad, cuya función es proteger a los sistemas tanto de procesamiento como de transferencia de datos. Estos servicios se implementan con uno o varios mecanismos o herramientas de seguridad. Se podrían clasificar los servicios de seguridad en:

a) **Confidencialidad.-** Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las

piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

b) **Autenticación.-** Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Garantiza que quien dice ser "X" es realmente "X". Es decir, se deben implementar mecanismos para verificar quién está enviando la información.

c) **Integridad.-** Requiere que la información sólo pueda ser modificada por las entidades autorizadas. Se asegura que los datos recibidos no han sido modificados de ninguna manera. Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar elementos menos obvios como respaldos, documentación, registros del sistema, tránsito en la red, etc. Esto comprende cualquier tipo de modificaciones:

- Causadas por errores de hardware y/o software.
- Causadas de forma intencional.
- Causadas de forma accidental.

Cuando se trabaja con una red, se debe comprobar que los datos no fueron modificados durante su transferencia.

d) **No Repudio.-** Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que, en efecto, el mensaje fue enviado y viceversa.

e) **Control de acceso.-** Requiere que el acceso a los recursos sea controlado y limitado por el sistema destino mediante uso de contraseñas o llaves.

f) **Disponibilidad.-** Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten. De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella. Por tanto, se deben proteger los servicios de cómputo de manera que no se degraden o dejen de estar disponibles a los usuarios de forma no autorizada. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

g) **Auditoría.-** Consiste en contar con los mecanismos para poder determinar qué es lo que sucede en el sistema, qué es lo que

hace cada uno de los usuarios, y los tiempos y fechas de dichas acciones.

En cuanto a los dos últimos puntos resulta de extrema importancia, cuando se trata de los derechos de los usuarios, diferenciar entre “espiar” y “monitorear” a los mismos. La ética es algo que todo buen administrador debe conocer y poseer.

Finalmente, todos estos servicios de seguridad deben ser tomados en cuenta en el momento de elaborar las políticas y procedimientos de una organización para evitar pasar por alto cuestiones importantes como las que señalan dichos servicios. De esta manera, es posible sentar de forma concreta y clara los derechos y límites de usuarios y administradores. Sin embargo antes de realizar cualquier acción para lograr garantizar estos servicios, es necesario asegurarnos de que los usuarios conozcan sus derechos y obligaciones (es decir, las políticas), de tal forma que no se sientan agredidos por los procedimientos organizacionales.

3.4.5 Herramientas de Seguridad Disponibles [15], [18]

En esta sección se mencionan varias de las tecnologías de seguridad lógicas disponibles para implementar los servicios de seguridad.

3.4.5.1 Herramientas para Confidencialidad

Estas herramientas se basan en la aplicación única o combinada de los siguientes esquemas:

- **Encriptación con claves privadas.-** Utiliza algoritmo de clave simétrica en la que la misma clave sirve para encriptar y desencriptar los mensajes.
- **Encriptación con claves públicas.-** Utiliza algoritmo de clave asimétrica en la que la llave pública encripta el mensaje, y la privada se utiliza para desencriptarlo como se describe en la Figura 3.3.

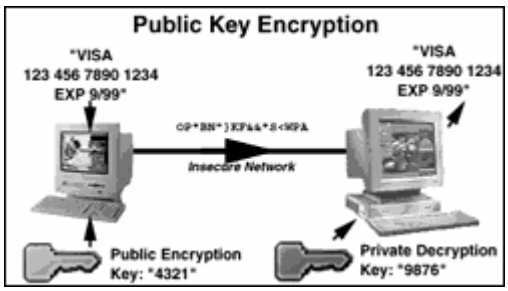


FIGURA 3.5. ENCRIPTACIÓN CON CLAVES ASIMÉTRICAS

a) Pretty Good Privacy (PGP)

Es un programa de seguridad desarrollado para soportar la codificación de clave pública, las firmas digitales y la compresión de datos. Constituye una poderosa familia de

productos criptográficos que permiten el intercambio de mensajes seguros y asegurar archivos, discos y conexiones de red con privacidad y fuerte autenticación.

b) Servidores de Web Seguros

Ofrece los servicios de confidencialidad, encriptando todo el tráfico entre los browsers clientes de la Intranet y el servidor web. Esto se logra utilizando el protocolo SSL (Secure Sockets Layer), lo que evita que un tercero pueda interceptar y descifrar los paquetes de datos que fluyen entre el browser y el servidor web. SSL se basa en una combinación de los esquemas de clave pública y privada.

c) Virtual Private Networks (VPN)

Tradicionalmente para una organización proveer conectividad directa entre diferentes edificios principales y sucursales, se requería alquilar o implementar una línea de datos costosa. Ahora una solución más económica es proveer a ambas oficinas de conectividad a Internet para que estas puedan comunicarse. El peligro en hacer esto es que no hay privacidad en este canal, y es difícil proveer a la otra oficina del acceso a recursos internos sin protegerlos de intrusos en Internet.

Las VPN proporcionan la capacidad de comunicar las dos oficinas entre sí de tal manera que pareciera que están directamente conectadas sobre una línea dedicada privada. La sesión entre ellos, aunque sea por Internet, es privada (debido a que el enlace es encriptado), y el enlace les permite compartir recursos internos en forma segura.

3.4.5.2 Herramientas de Autentificación

a) Claves de una sola vida

Han existido muchos incidentes que involucran programas denominados Caballos de Troya y programas tipo sniffers que capturan los passwords ingresados por teclado, de modo que los atacantes pueden utilizarlos para subsecuentes accesos a las cuentas en servidores. Esto es posible debido a que las claves son utilizadas una y otra vez y pasan por la red en texto claro.

Varias técnicas de autenticación han sido desarrolladas para resolver estos problemas. Entre estas técnicas están las tecnologías challenge-response que proveen claves ha ser utilizadas una sola vez.

b) Kerberos

Kerberos es un sistema de seguridad que provee autenticación en redes distribuidas físicamente inseguras,

basado en el modelo de distribución de claves. Kerberos utiliza una base de datos de claves simétricas almacenada en un Centro de Distribución de Claves (KDC) conocido como el servidor Kerberos. A un usuario o servicio se le concede “tickets” electrónicos después de conectarse y negociar con el KDC. Estos tickets son usados para autenticación entre usuarios y/o servicios. Todos los tickets llevan una marca de tiempo que limita el periodo de tiempo durante el cual el ticket es válido. Se requiere una sincronización entre servidor y clientes para este sistema.

El lado práctico de Kerberos es su integración con la capa de aplicación. Las aplicaciones típicas como FTP, Telnet, POP y NFS se han integrado con el sistema Kerberos.

3.4.5.3 Herramientas para No-Repudio

Firmas Digitales

Una firma digital es una técnica que le asegura al receptor de un archivo de Internet/Intranet que éste realmente proviene de la persona que el archivo indica.

Si se comprende la forma en que se realiza la codificación de llave pública también comprenderá la forma en que trabajan las firmas digitales. En la codificación de llave pública el emisor codifica un documento utilizando una

llave pública y el receptor lo decodifica utilizando una llave privada. Con la firma digital ocurre lo contrario. El emisor utiliza una llave privada para codificar una firma y el receptor decodifica la firma empleando una llave pública. Debido a que el emisor es la única persona que puede codificar su firma, solo él puede autentificar los mensajes [17].

Básicamente, lo que se requiere es un sistema en donde uno puede enviar un mensaje firmado a otro de tal manera que [17]:

1.- El destinatario pueda verificar la identidad del originador.

2.- El originador no pueda más tarde desconocer el contenido del mensaje.

3.- El destinatario no pueda fabricarse un mensaje a sí mismo.

3.4.5.4 Seguridad de Red a través de Firewalls

Los firewalls o cortafuegos son mecanismos del modelo de seguridad de red, que tienen como objetivo proteger un sistema de red de computadoras de ataques provenientes

de Internet u otra red. Cumple con los siguientes objetivos [15]:

- Restringir el ingreso por un sólo punto de control.
- Prevenir que intrusos tomen control de otros mecanismos de protección con el fin de arruinar todo el sistema defensivo.
- Restringir la salida por un punto único de control.

Un firewall para Internet se coloca por lo regular en un punto entre Internet y la red de computadoras que se desea proteger, como se observa en la Figura 3.6. Todo el tráfico dirigido a la red interna y proveniente de Internet tiene que atravesar el firewall, y éste tiene la oportunidad de dejar pasar sólo el tráfico aceptable y rechazar lo que las políticas de seguridad establezcan como no confiable.

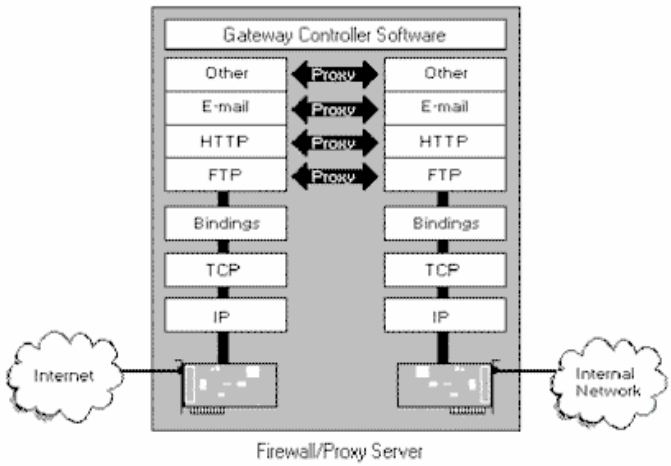


FIGURA 3.6. REPRESENTACIÓN DE UN FIREWALL

Con una política de seguridad precisa, y una correcta implementación y configuración del firewall, se puede alcanzar un altísimo nivel de seguridad en el perímetro externo de la Intranet.

3.5 Análisis Funcional de la Armada como Organización

La Armada, como parte integrante de las Fuerzas Armadas, es una Institución Nacional, permanente y regular, cuya función y naturaleza está definida en la Constitución de la República.

Para tal efecto, tiene establecido su Plan Estratégico Institucional, como principal herramienta de la cual se derivan el Plan de Fortalecimiento del Poder Naval, el Plan de Fortalecimiento Institucional y su Plan Director.

En el Plan Estratégico Institucional, están definidos los elementos estratégicos que citamos a continuación [20]:

Visión de la Armada

“Una Armada con un Poder Naval disuasivo, altamente entrenada y lista para la victoria. Involucrada totalmente con el desarrollo y proyección de los intereses marítimos y con el apoyo a las comunidades más necesitadas; constituida por hombres de elevada calidad profesional y moral, y que basa su institucionalidad en el cumplimiento de valores y principios fundamentales.”

Misión de la Armada

“Estructurar, alistar y mantener un Poder Marítimo, que contribuya a garantizar la seguridad y el desarrollo de la nación, a fin de apoyar a la consecución y mantenimiento de los Objetivos Nacionales; de acuerdo a la planificación para tiempos de paz, conflicto y guerra.”

El sistema de planificación tiene tres niveles; ver la Tabla IV:

TABLA IV

SISTEMA DE PLANIFICACIÓN INSTITUCIONAL DE LA ARMADA

Nivel	Denominación	Información que genera	Responsable
I	Planificación Institucional	• Visión de futuro de la Institución. • Misión de la Armada. • Objetivos Estratégicos Institucionales. • Políticas Institucionales. • Directrices que tiendan a la consecución de los Objetivos. • Determinación de medios.	Comandante General. Estado Mayor.
II	Planificación Sectorial	• Visión. • Misión. • Objetivos Sectoriales. • Políticas Sectoriales. • Acciones Estratégicas a corto, mediano y largo plazo.	Jefes Sectoriales
III	Planificación del Reparto Naval	• Visión. • Misión. • Objetivos del Reparto. • Políticas del Reparto. • Proyectos.	Comandantes y Directores de Reparto

Objetivos Estratégicos Institucionales

1. Desarrollar una Armada moderna, eficiente, disuasiva, capaz de enfrentar nuevas tareas y prioridades.

2. Formar Personal Naval capacitado, disciplinado, con altos valores morales y satisfechos de ser miembros de la Armada.
3. Mantener presencia Naval en todo el territorio nacional.
4. Reducir la dependencia del presupuesto general del Estado.
5. Establecer una Autoridad Marítima acorde con las exigencias internacionales y con amplia interrelación con sus usuarios.
6. Constituir una Institución líder en el Pacífico Sudeste en investigación y estudios científicos.
7. Contribuir al desarrollo del país y proyectar los intereses marítimos y fluviales hacia las cuencas del Pacífico, Amazonas y Región Antártica.
8. Lograr hasta el 2023 el fortalecimiento mínimo indispensable de la Fuerza Naval, que le permita recuperar y mantener su capacidad disuasiva suficiente ante las potenciales amenazas; y constituir un aporte para la seguridad y el desarrollo institucional.

Políticas Institucionales del Mando

De las Políticas Institucionales del Mando, resaltamos aquellas con las cuales éste proyecto debe buscar alineamiento y armonía:

1. **Modernizar la Armada** adaptándole a nuevas tareas y prioridades.
2. Implantar un **desarrollo sustentado de la educación formal e informal** en todo nivel.

…

4. **Reducir al máximo la dependencia tecnológica del exterior**.

…

9. **Manejar el Recurso Humano** de manera global, **planificando y coordinando acciones** en los diversos campos: administración del personal, bienestar, vivienda, educación y salud.

…

11. **Impulsar la modernización** dentro del campo de acción de la autoridad marítima, **automatizando procesos, generando eficiencia, mejorando en su totalidad el servicio al usuario**.
12. **Alcanzar el máximo de eficiencia en toda gestión**, utilizando los **principios de economía de escala y tercerización de servicios**.
13. Impulsar la participación activa de la Armada en la **investigación y estudio científico del mar y del ambiente marino-costero.**
14. **Contribuir al desarrollo marítimo, investigación científica del medio ambiente marino-costero** y brindar seguridad al tráfico marítimo, con el mantenimiento permanente de las áreas marítimas, puertos marítimos, sus canales y ayudas a la navegación.

Organización de la Armada [21]

Una vez promulgado el Plan Estratégico Institucional, con el propósito de poderlo llevar a cabo, la Armada modifico su organización reestructurándola por sectores. Actualmente la Armada está organizada en seis sectores: Administrativo, Operativo, Personal, Material, Marina Mercante, e Intereses Marítimos. Dentro de estos sectores se aglutinan

los diferentes Repartos Navales. La estructura de la Armada y su Organización por Sectores se muestra en la Figura 3.7.

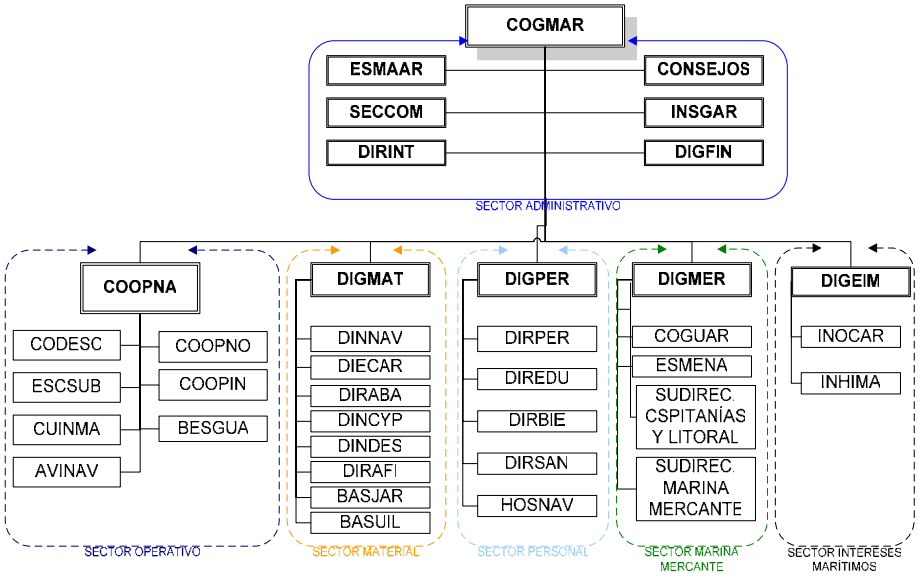


FIGURA 3.7. ORGANIZACIÓN DE LA ARMADA POR SECTORES

Como podemos apreciar, el Sector Administrativo es el ente coordinador que vincula al resto de Sectores para que la Institución funcione armoniosamente.

El Sector Administrativo tiene como principal Objetivo Estratégico Sectorial, “El propender a la consecución de los Objetivos Estratégicos Institucionales”, por tanto al ser la Dirección de Desarrollo Administrativo e Informático parte de éste sector, tiene que elaborar una planificación secuencial o en serie, una vez promulgado el Plan Estratégico Institucional, para proponer herramientas que faciliten a

todos los sectores la consecución de sus objetivos y un desarrollo adecuado.

Uno de los retos organizacionales de la Dirección de Desarrollo Administrativo e Informático, será tener éxito con la propuesta de organización informática de la Armada, la misma que trata de ser transversal a todos los sectores, eliminando las barreras interorganizacionales, de modo se pueda explotar lo siguiente:

1. **Agrupar requerimientos y experiencia.-** Tanto los requerimientos de usuarios, como la experiencia de los desarrolladores de los Repartos Navales en un mismo Sector, tendrán mucho en común, por lo que deberán ser formalizados, consolidados y aprobados para ser aprobados por los organismos competentes. El propósito es ofrecer soluciones informáticas útiles con capacidad de uso a nivel Institucional.
2. **Capacidad de integración.-** Al definir requerimientos y flujos de información dentro de cada Sector, se podrá implementar Sistemas de Información Informáticos con arquitecturas de información a nivel institucional que soporten la integración entre sectores.
3. **Intercambio de conocimiento e información.-** La interacción entre los Centros de Tecnología de Información de cada Sector, facilita y habilita el intercambio de conocimientos y experiencias,

lo que ayuda a romper el esquema actual de “Islas de Automatización”.

4. **Generación de nueva información.-** Al implantar Sistemas de Información Informáticos en cada sector, bajo una Arquitectura de Información Institucional, se habilitara el intercambio de información entre sectores, gatillando una producción de nueva información a disposición de los diferentes niveles de decisión para funciones de Mando, Control y Asesoramiento.
5. **Definición de Procesos, Estándares y Metodologías que promuevan la reutilización.-** El Desarrollo de Sistemas de Información Informáticos deberá basarse en Procesos, Estándares y Metodologías diseminadas y controladas por la Dirección de Desarrollo Administrativo e Informático para los Centros de Tecnología de Información. Esto promueve la reutilización de recursos.

Propuesta de la Nueva Organización Informática en la Armada

Para tener éxito en el desarrollo de Sistemas de Información Informáticos en la Armada debido a sus diversos campos de acción, demanda una estructura funcional y orgánica adecuada para la Gestión Informática a Nivel Institucional.

La Organización propuesta incluye un Consejo de Informática de la Armada; la redefinición y reubicación geográfica de la Dirección de Desarrollo Administrativo e Informático, dándole un rol eminentemente técnico; mantener el Centro de Tecnología de Información de Nivel 1 de Quito; mantener el Comité Técnico Informático de la Armada, los Centros de Tecnología de Información de Nivel 2 y 3; el establecimiento de los Foros Informáticos y las Fuerzas de Tarea Específicas.

Consejo de Informática de la Armada

Organismo de asesoramiento del Estado Mayor en asuntos informáticos, que busca el alineamiento de los Sistemas de Información Informáticos con el Plan Estratégico Institucional, emitiendo las Políticas Institucionales para la gestión de la información. El Consejo se conformará por un representante de cada Sector de la Armada, a través de quienes se plantearán los requerimientos sectoriales, y estará presidido por el Subjefe del Estado Mayor. El Consejo priorizará los proyectos a ser desarrollados por la Dirección de Desarrollo Administrativo e Informático.

Dirección de Informática

En el Nivel Técnico – Administrativo, tenemos la Dirección de Informática quien será el responsable de emitir las disposiciones correspondientes que provengan de las Políticas dictadas por el Consejo de Informática de la Armada, y controlará su cumplimiento. La

Dirección de Informática será la responsable técnicamente de la infraestructura tecnológica centralizada y de la Red de Información Institucional. Para tal efecto tiene en Guayaquil a su cargo los siguientes Departamentos: Desarrollo de Sistemas de Información, Redes de Información, Operaciones y Producción, Seguridad Lógica, y, Cultura Informática.

Comité Técnico Informático de la Armada

Organismo de Apoyo y Asesoramiento técnico de la Dirección de Informática, conformado por los Jefes de los Centros de Tecnología de Información de Nivel 1 y 2 de cada Sector, y presidido por el Director de Informática. Su función es analizar las posibilidades de empleo de diferentes tecnologías para la resolución de problemas planteados a la Dirección de Informática.

Centros de Tecnología de Información

Son órganos operativos encargados de las principales tareas informáticas, a través de los cuales se desarrolla y opera las distintas soluciones puestas en producción. Los Centros de Tecnología de Información están clasificados en 3 niveles:

- En el nivel 1 está el Centro de Tecnología de Información de Quito.

- En el nivel 2 tenemos los ubicados dentro de los otros cinco sectores de la Armada y en los repartos que tienen un desarrollo informático importante.
- En el nivel 3 está todo reparto donde exista una Red de Datos Local.

La Dirección de Informática a través de sus Departamentos Técnicos y del Centro de Tecnología de Información de Nivel 1, es responsable de:

- La centralización del desarrollo y la adquisición del software a nivel institucional.
- La consolidación del ambiente de procesamiento.
- La ingeniería y administración de la Red de Información de la Armada.
- La administración de la seguridad lógica.
- El desarrollo de la cultura informática.

Los Centros de Tecnología de Información de nivel 2, son responsables de:

- La administración de los recursos de procesamiento locales que son específicos a su reparto.
- La administración de recursos informáticos locales a nivel de usuario.

- El establecimiento formal de los requerimientos a ser enviados para desarrollo, mantenimiento o mejoramiento de sistemas de información existentes o demandados.
- Soporte informático a usuarios.

Los Centros de Tecnología de Información de nivel 3, son responsables de:

- La administración de los recursos informáticos locales a nivel de usuario.
- Soporte informático a usuarios.

Foros Informáticos

Los Foros Informáticos son grupos de discusión especializados en determinados tópicos o tecnologías, conformados por el Comité Técnico Informático de la Armada. Se desempeñan en el sentido transversal y su función es estudiar, investigar, analizar, probar y proponer mejoras aplicativas dentro de su tópico especializado. Ejemplo de foros informáticos son: Tecnologías Open Source aplicables a la Institución, Plataforma de desarrollo Java 2 Enterprise Edition, Plataforma Microsoft .Net, etc.

Fuerzas de Tarea

Para el análisis de problemas o alternativas puntuales técnicas y especializadas que se puedan presentar, el Comité Técnico Informático puede sugerir la conformación de un equipo de trabajo temporal

dedicado a tiempo completo o parcial hasta alcanzar los resultados deseados a manera de “Fuerza de Tarea”. Los resultados son propuestos al Comité Técnico Informático de la Armada.

En la Figura 3.8, se resume la propuesta de Organización de la Informática en la Armada:

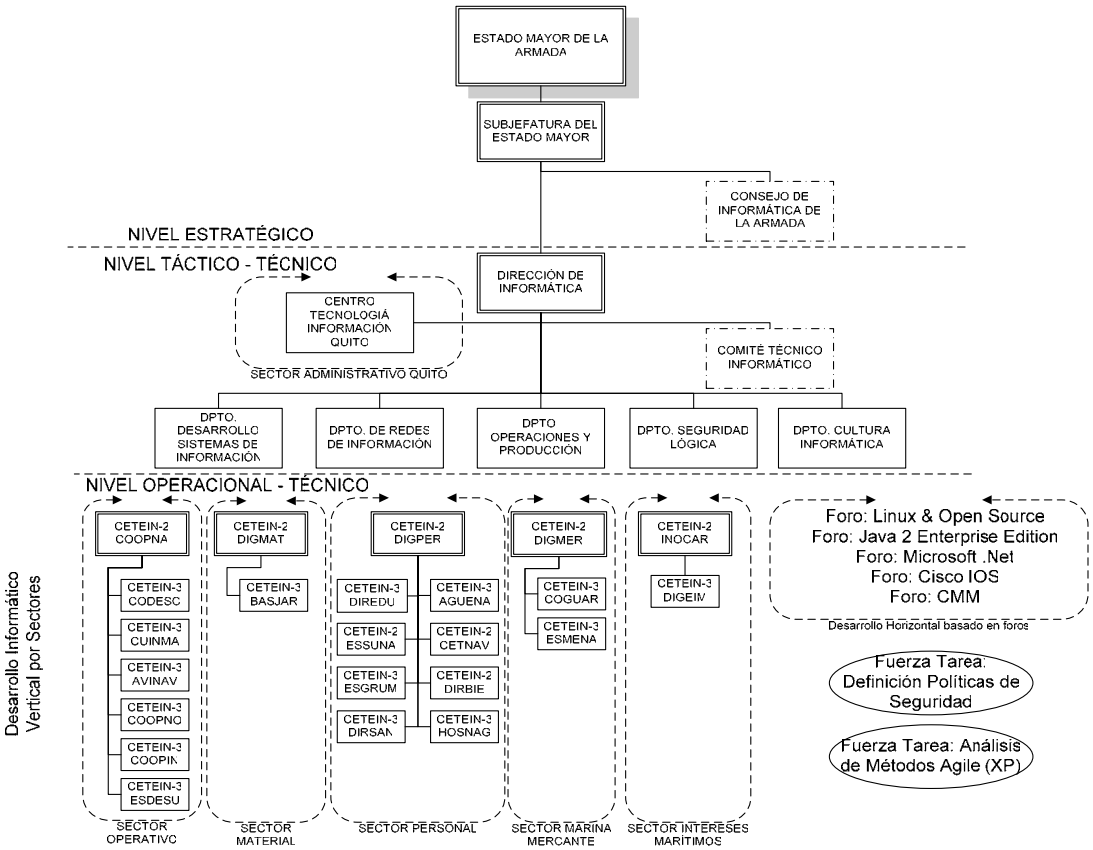


FIGURA 3.8. PROPUESTA DE LA ORGANIZACIÓN INFORMÁTICA EN LA ARMADA

3.6 Definición de Interacciones entre los Sectores de la Armada y sus Repartos Subordinados

En un análisis de las tareas definidas para los Sectores de la Armada, se han determinado aquellas cuyo desempeño podría ser mejorado y asistido con el soporte de sistemas de información basados en el Intranet.

El Comandante General de Marina comanda al Sector Operativo, a través del Comando de Operaciones Navales, y administra los Sectores de Apoyo y Desarrollo, a través de los Jefes de Sector; tal como se lo describe en la Figura 3.9; por tanto se debe tener una gran capacidad de comunicación y coordinación a éste nivel.

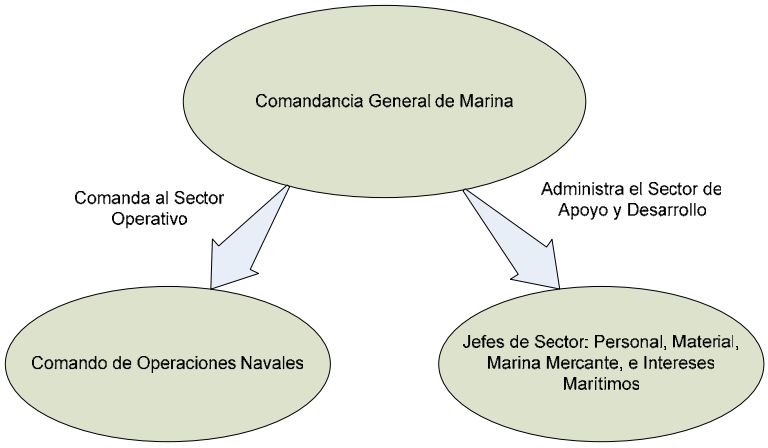


FIGURA 3.9. ACCIONES GENERALES DE LA COMANDANCIA GENERAL DE MARINA

Son tareas del Comandante General de Marina emitir políticas, directrices y directivas, que orienten la acción de la Fuerza Naval en los diversos campos de su actividad; por tanto es necesario que éstas sean ampliamente difundidas, ver Figura 3.10.

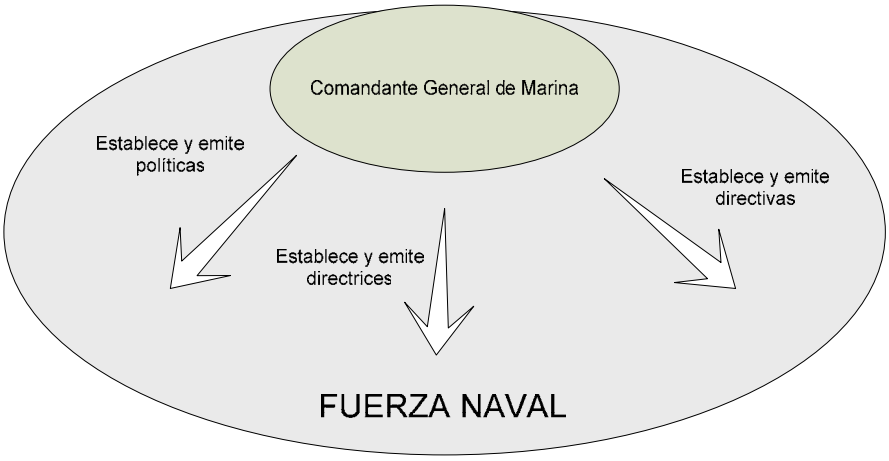


FIGURA 3.10. TAREAS PRINCIPALES DEL COMANDANTE GENERAL DE MARINA

La Dirección de Inteligencia Naval, se encarga de recopilar la información necesaria para producir inteligencia; prepara y ejecuta operaciones especiales de contrainteligencia y guerra sicológica; y, estudia y recomienda normas de seguridad para los repartos y unidades de la Armada, así como para sus miembros; por tanto requiere de un medio para la obtención de información de alta penetración y gran capacidad de difusión; su interacción es con toda la Fuerza Naval, de acuerdo a lo que se muestra en la Figura 3.11.

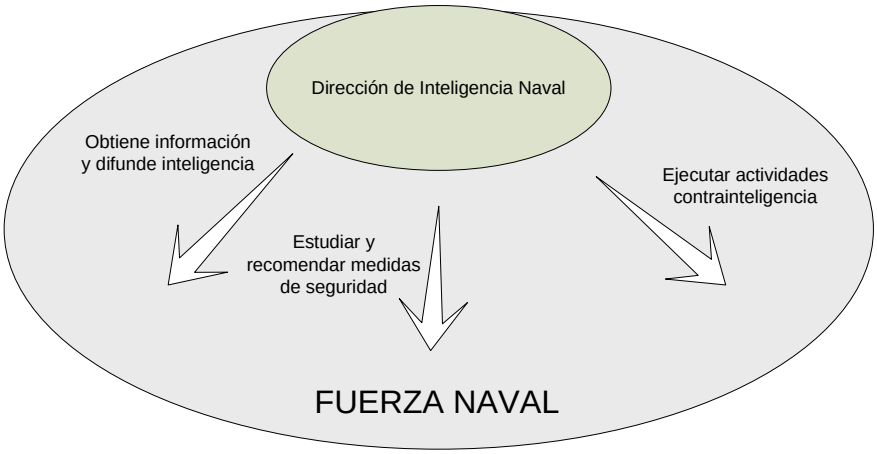


FIGURA 3.11. ACCIONES GENERALES DE LA DIRECCION DE INTELIGENCIA NAVAL

Los Órganos de asesoramiento y consejo, tienen establecidas sus funciones en sus reglamentos respectivos cada uno con un propósito definido, los mismos que deben ser conocidos tanto por los miembros del Consejo, como por todos los miembros de la Fuerza Naval que acudan o sean regulados por dichos Consejos. La forma de difundir los reglamentos vigentes con las últimas modificaciones debe ser de alta penetración, así como también se debe garantizar un fácil acceso a los mismos. El Comando General debe tener una gran capacidad de comunicación y coordinación con sus Órganos de Consejo y Asesoramiento, y éstos a su vez una gran capacidad de difusión de las resoluciones aprobadas, a los distintos miembros de la Fuerza Naval interesados y autorizados a conocerlas. Ver Figura 3.12.

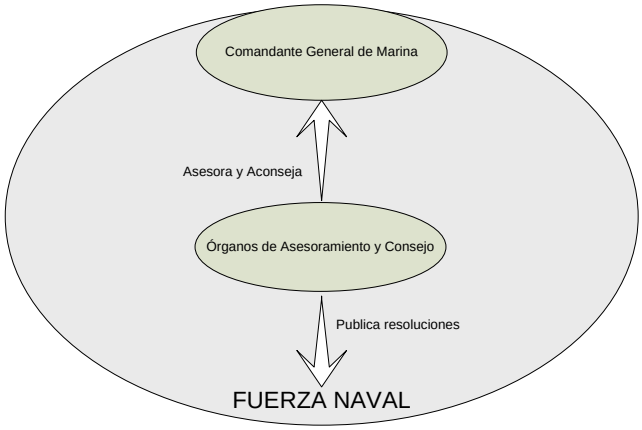


FIGURA 3.12. ACCIONES GENERALES DE LOS ORGANOS DE ASESORAMIENTO Y CONSEJO

El Estado Mayor de la Armada es el Órgano de Planificación cuyas funciones principales se indican en la Figura 3.13.

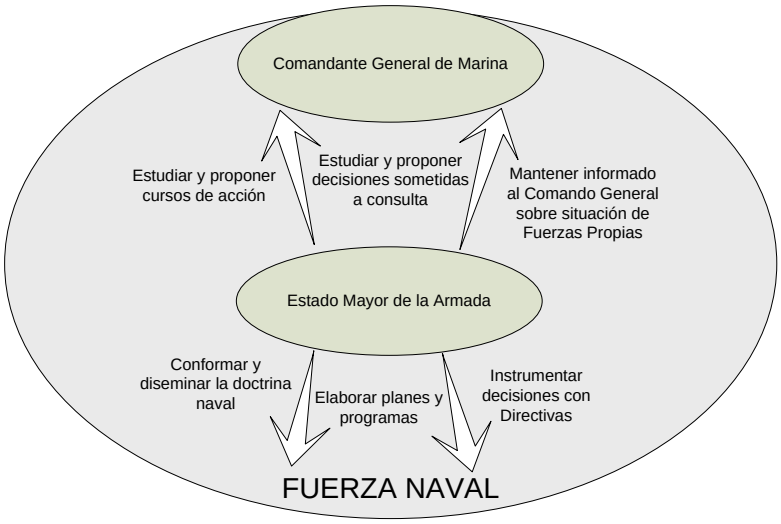


FIGURA 3.13. TAREAS PRINCIPALES DEL ESTADO MAYOR DE LA ARMADA

La Inspectoría General de la Armada es el órgano de control y cuyas funciones principales se indican en la Figura 3.14.

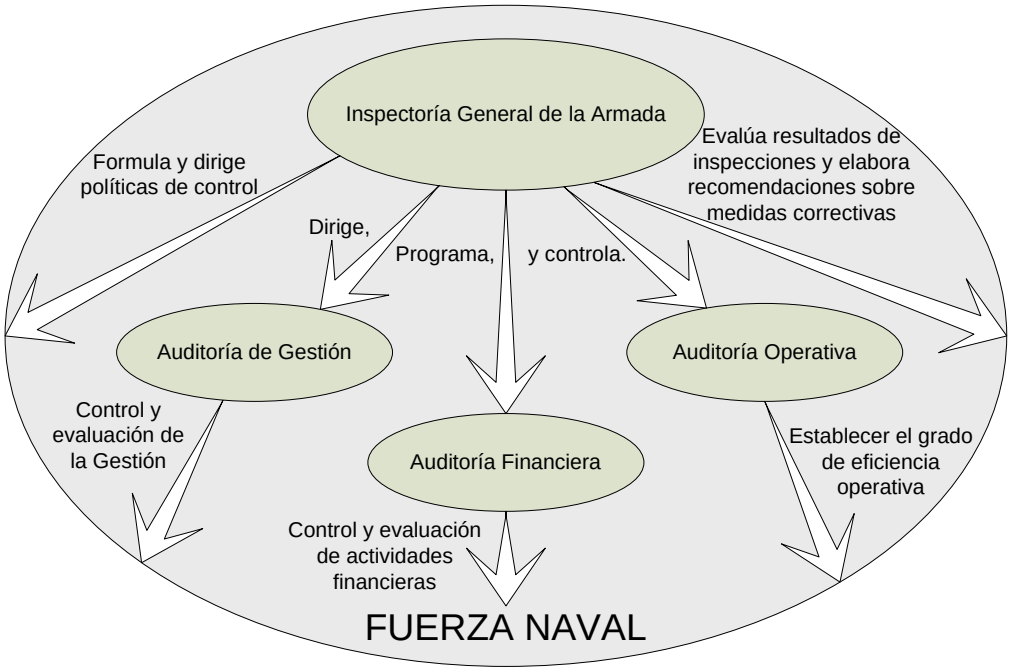


FIGURA 3.14. TAREAS PRINCIPALES DE LA INSPECTORIA GENERAL DE LA ARMADA

El Comando de Operaciones Navales es el responsable de la conducción de la Fuerza Operativa en las operaciones militares, tal como se muestra en la Figura 3.15.

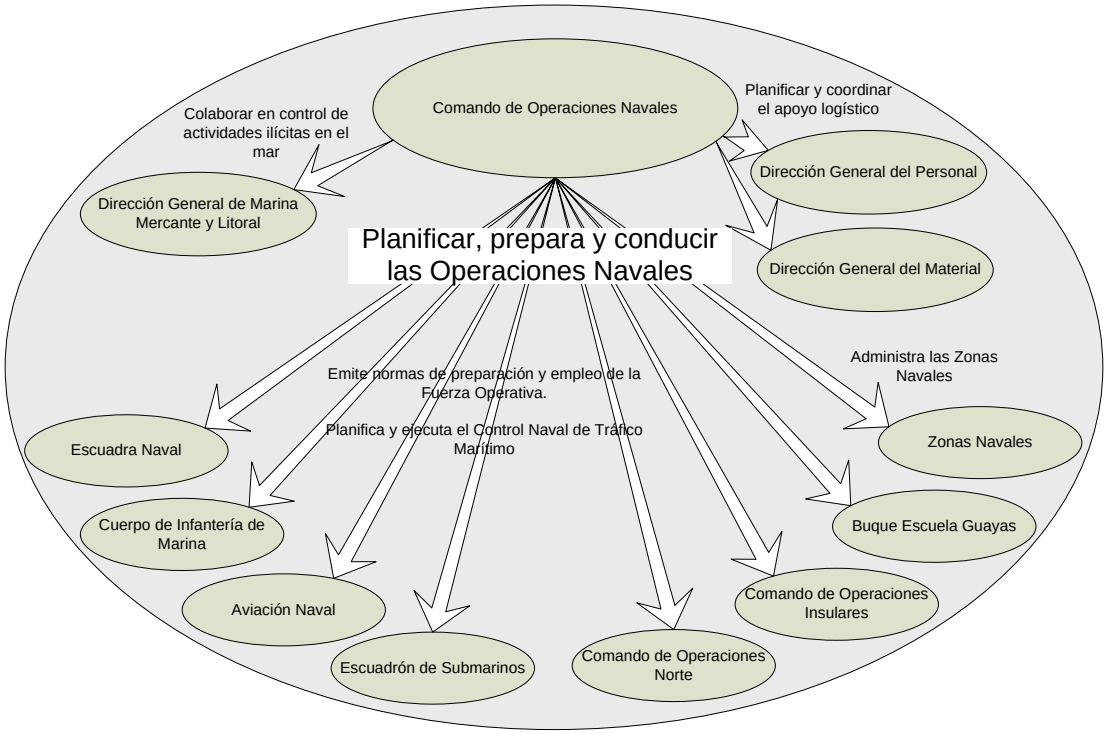


FIGURA 3.15. TAREAS PRINCIPALES DEL COMANDO DE OPERACIONES NAVALES

La Secretaría del Comando General de la Armada es la responsable de realizar la proyección de la imagen institucional, tanto en el ámbito nacional como internacional, administrando además las actividades del Comandante General, tal como se muestra en la Figura 3.16.

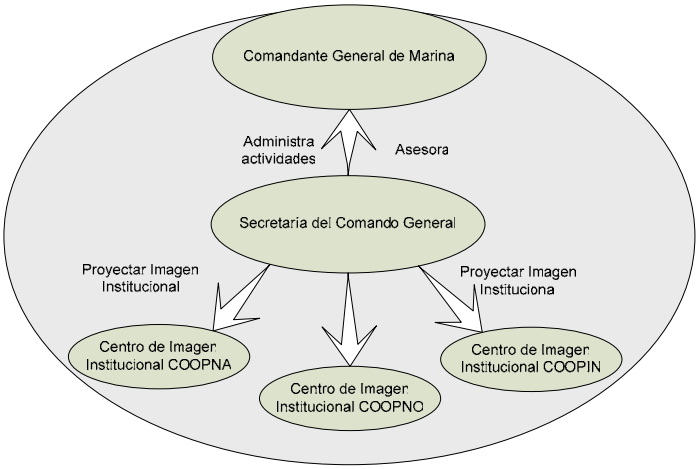


FIGURA 3.16. TAREAS PRINCIPALES DE LA SECRETARIA DEL COMANDO GENERAL

La Dirección General del Personal es la responsable de la administración de los Recursos Humanos de la Armada y sus tareas principales se muestran en la Figura 3.17.

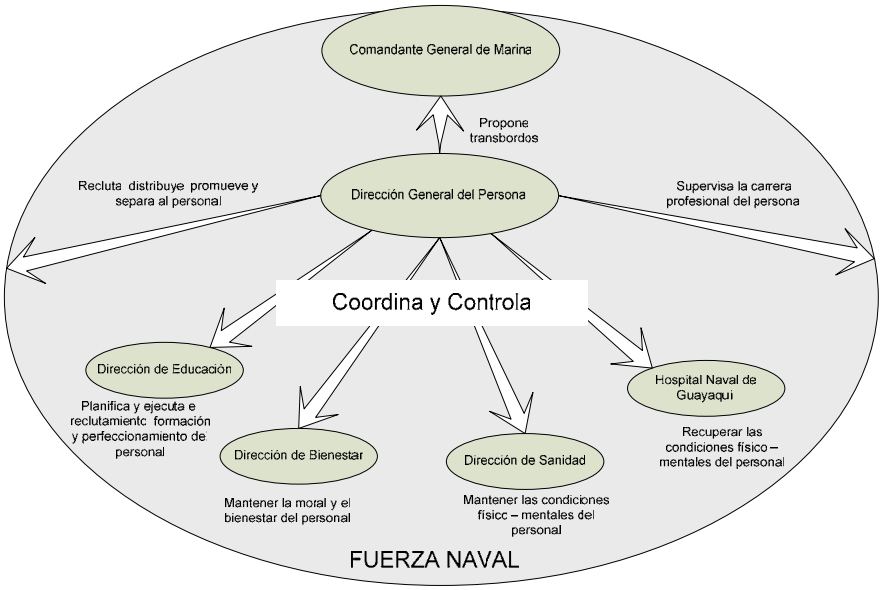


FIGURA 3.17. TAREAS PRINCIPALES DE LA DIRECCION GENERAL DEL PERSONAL

La Dirección de Educación de la Armada es la encargada de formar, especializar y perfeccionar profesionalmente a los miembros de la institución, tal como se muestra en la Figura 3.18.

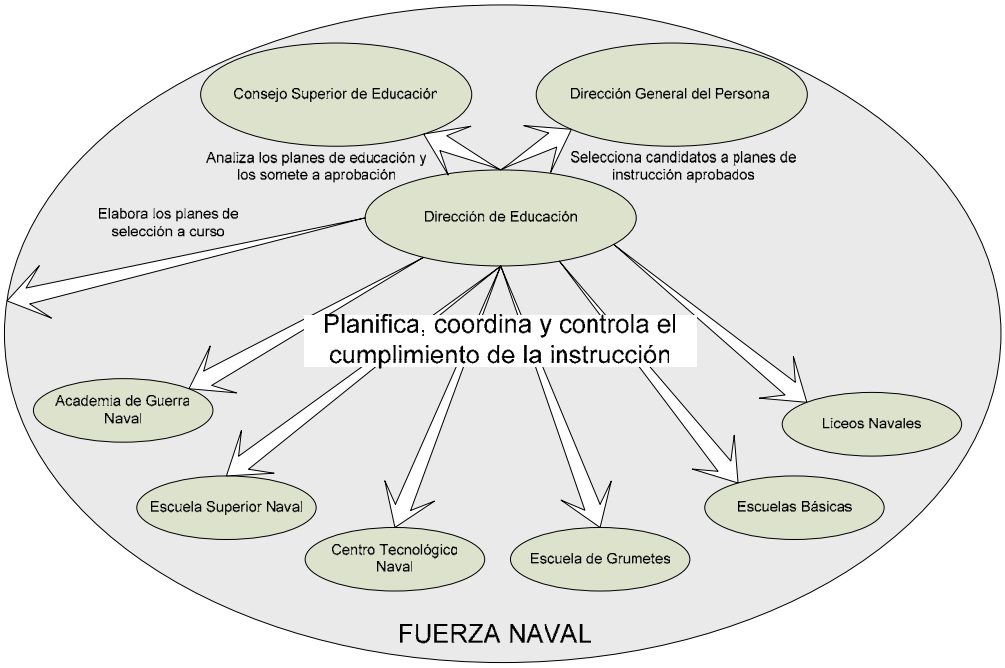


FIGURA 3.18. TAREAS PRINCIPALES DE LA DIRECCION DE EDUCACION

La Dirección General de Finanzas se encarga de administrar los recursos económicos y el patrimonio de la Armada, y sus tareas principales se muestran en la Figura 3.19.

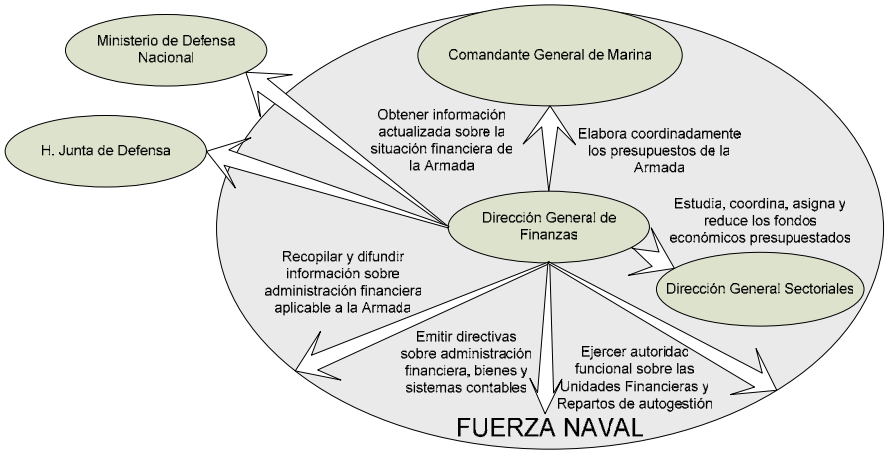


FIGURA 3.19. TAREAS PRINCIPALES DE LA DIRECCION GENERAL DE FINANZAS

La Dirección General del Material, como responsable de planificar, organizar y ejecutar la logística de producción, así como administrar los recursos materiales y proporcionar el apoyo logístico a los repartos navales, tal como se muestra en la Figura 3.20.

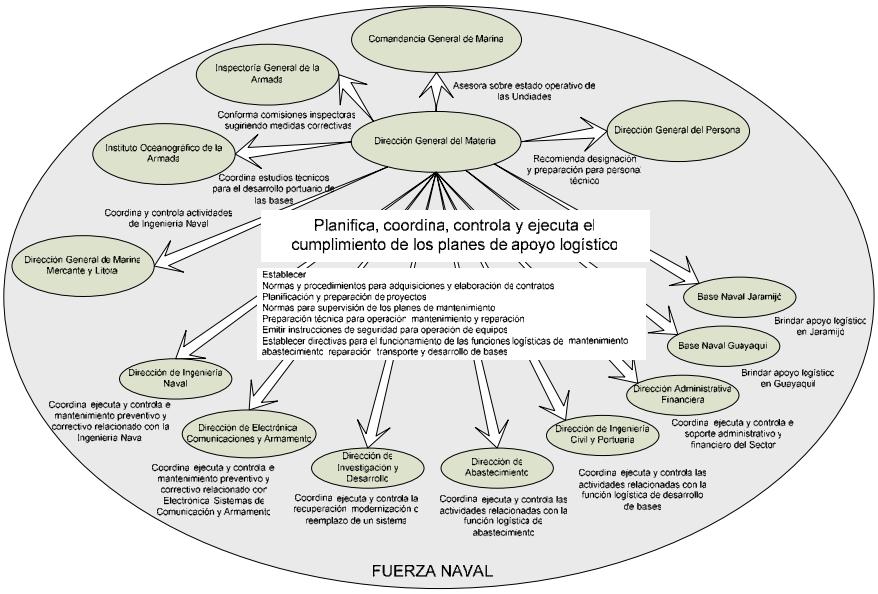


FIGURA 3.20. TAREAS PRINCIPALES DE LA DIRECCION GENERAL DEL MATERIAL

La Dirección General de Intereses Marítimos, es la responsable de planificar, organizar, dirigir y controlar la participación de la Armada en el fortalecimiento del poder marítimo nacional, tal como se muestra en la Figura 3.21.

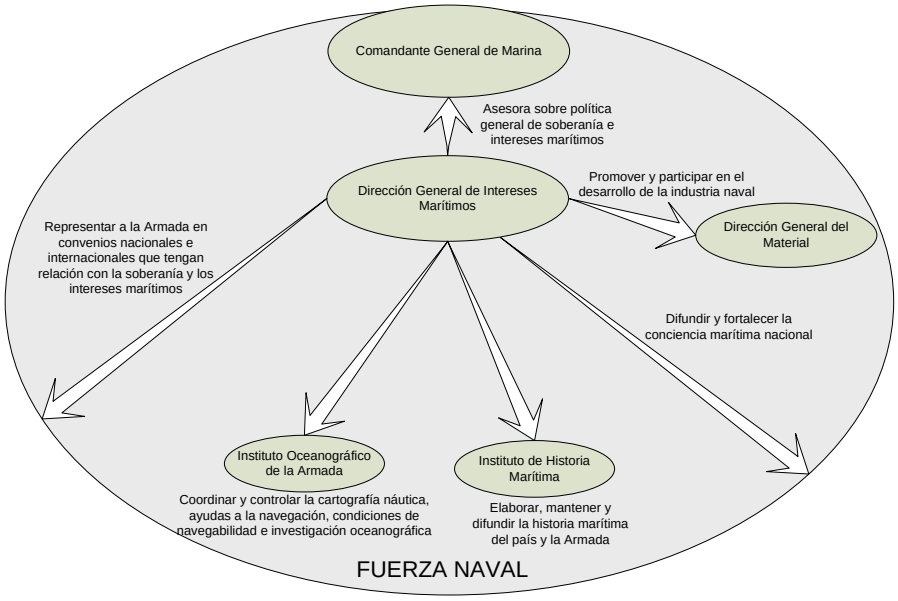


FIGURA 3.21. TAREAS PRINCIPALES DE LA DIRECCION GENERAL DE INTERESES MARITIMOS

La Dirección General de la Marina Mercante y del Litoral, como Autoridad Marítima es responsable de administrar las actividades relacionadas con la Marina Mercante Nacional, el transporte por agua y su infraestructura portuaria, así como de ejercer el control de las actividades ilícitas y garantizar la vida en el mar, tal como se muestra en la Figura 3.22.

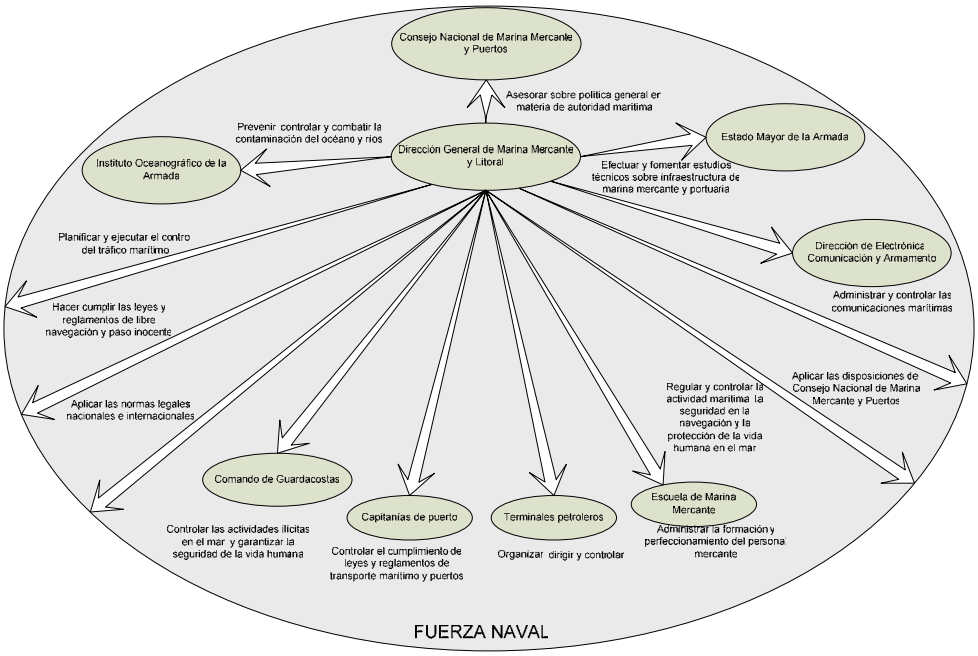


FIGURA 3.22. TAREAS PRINCIPALES DE LA DIRECCION GENERAL DE MARINA MERCANTE Y DEL LITORAL

3.7 Escenarios Aplicables para: Sistemas de Información, Repositorios de Información, Mensajería, Publicación, Grupos de Discusión y Herramientas Colaborativas; a manera de servicios corporativos basados en el Intranet Naval

3.7.1 Sistemas de Información Propuestos

Sistema de Control de Gestión

Para llevar a cabo el Plan Estratégico el modelo de gestión más adecuado para la Armada es el Cuadro de Mando Integral

(Balanced Score Card), el cual provee a la Dirección los elementos que permitan tomar mejores decisiones, en base a un monitoreo de los Indicadores de Gestión. Estos indicadores son formulados sobre las cuatro dimensiones del modelo de CMI: Financiera, Clientes (Internos y externos a la institución), Procesos Internos, y, Formación y Crecimiento. Éste modelo permite medir el desempeño individual y colectivo, así como lograr un mayor comprometimiento y comprensión de la Estrategia Formulada.

La automatización del modelo de gestión de CMI a través de un Sistema de Información para el Control de la Gestión en la Armada, es un proyecto estratégico que busca transformar la evaluación de la gestión.

En las Figuras 3.23 y 3.24 se muestra el empleo del Cuadro de Mando Integral como un Sistema de Gestión Estratégica [22]:

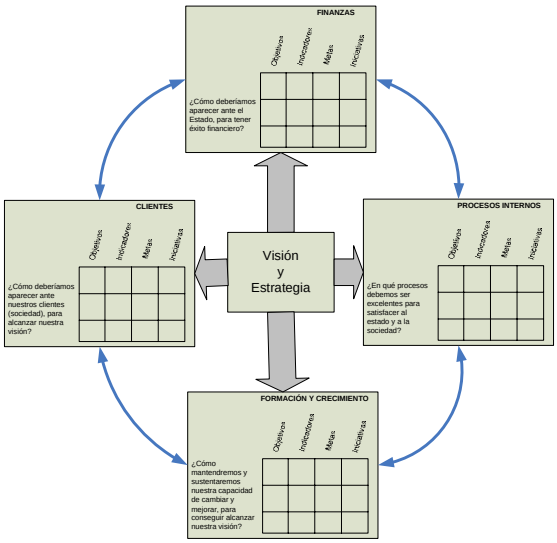


FIGURA 3.23. EL CUADRO DE MANDO INTEGRAL COMO ESTRUCTURA PARA TRANSORMAR UNA ESTRATEGIA EN TÉRMINOS OPERATIVOS

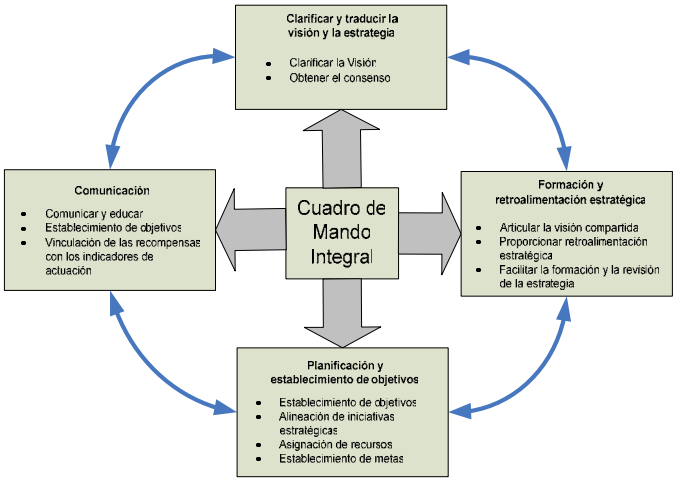


FIGURA 3.24. EL CUADRO DE MANDO INTEGRAL COMO UN MARCO ESTRATÉGICO PARA LA ACCIÓN

Este proyecto está alineado estratégicamente con el siguiente Objetivo Específico del Estado Mayor de la Armada:

- Alcanzar los Objetivos Estratégicos Institucionales.

Sistema de Información Comunicacional

Las Comunicaciones Administrativas en la Armada siguen dependiendo de una estructura basada en papel, refinada por modelos de gestión burocráticos, jerarquizados y piramidales, que ya no es eficiente ni eficaz.

El proceso comunicacional (desde que se emite la idea a comunicar, hasta que la recibe el destinatario) utiliza demasiados recursos humanos y materiales, insumos y el tiempo que consume no es compatible con la era en que vivimos. La seguridad también deja mucho que desear. Así mismo las actividades que se requieren para almacenar, recuperar y eliminar la información del archivo son muy costosas. El proceso es burocrático ya que sigue la estructura orgánica de la Armada.

Los requerimientos de alto nivel establecidos para éste sistema son:

- Sistema de mensajería electrónica unificada estructurada, seguro con firma digital y capacidad de automatización de flujos de trabajo; para reemplazar los Oficios, Cartas, Memos y Radiogramas. El sistema estará integrado a la telefonía interna y por tanto al voice mail.

- Portal Colaborativo con directorios y archivos clasificados en: privados, compartidos (por grupo de trabajo) y públicos; con capacidad de búsquedas por palabras claves en base a la indexación automática del portal, haciendo uso intensivo de tecnología de administración de contenidos.

- Directorio institucional que provea información de contacto e identidad de los diferentes miembros de la institución, así como de los recursos para administración de identidades. Incluye además calendario y agenda compartida de usuarios.

- Un modelo de seguridad que integre los perfiles de usuarios con niveles de acceso, autenticación y autorización de modo que se provea un modelo de seguridad superior al establecido en la normativa actual en torno al papel.

- Herramientas colaborativas para reuniones virtuales: análisis, depuración y elaboración compartida de documentos en tiempo real; exploración compartida del web; pizarra electrónica compartida; mensajería instantánea integrada con audio.

El producto que cumple con los requerimientos establecidos es el Oracle Collaboration Suite, cuyo modelo funcional se muestra en la Figura 3.25 (21):

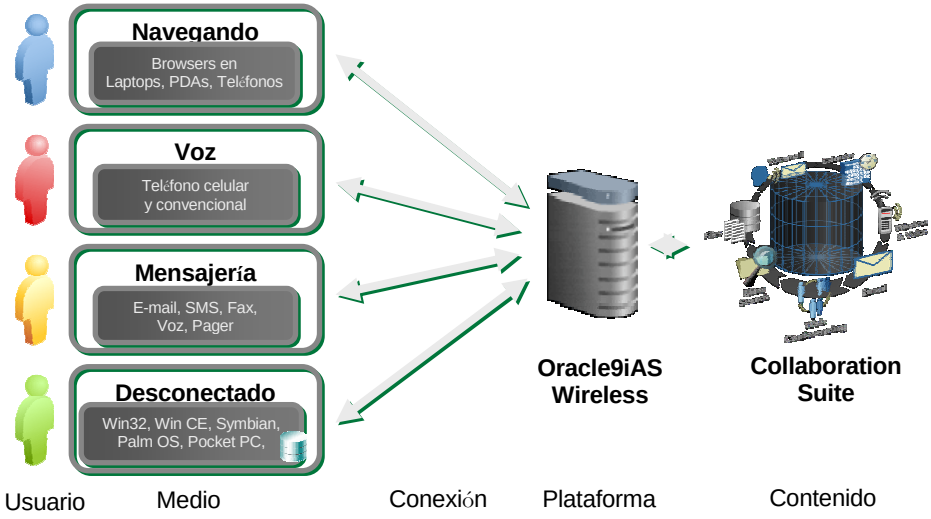


FIGURA 3.25. MODELO FUNCIONAL DE ORACLE COLLABORATION SUITE [23]

Este proyecto está alineado estratégicamente con el siguiente Objetivo Específico del Estado Mayor de la Armada:

- Alcanzar los Objetivos Estratégicos Institucionales.

Modernización del Sistema Integrado Financiero

La Armada mantiene una doctrina para el manejo de sus recursos económicos tanto en la planificación como en la ejecución presupuestaria, llamada “Plan Director”.

El sistema actual que apoya la gestión del Plan Director no facilita una gestión integral de la información. Además hay nuevas regulaciones que centralizan la gestión de compras totalmente en la Dirección de Abastecimientos de la Armada, lo que tiene un impacto funcional, siendo necesario adecuar el Sistema a ésta nueva realidad.

La propuesta es que el Departamento de Contabilidad y Presupuesto de la Dirección General de Finanzas, sea responsable de la consolidación diaria y mensual de todos los procesos operativos financieros y contables de las nuevas unidades financieras a nivel nacional; cuyo número será reducido drásticamente manteniéndose una unidad financiera principal en Guayaquil y otra en Quito con suficientes capacidades para el pago de obligaciones de la Armada con sus proveedores. Debido a la centralización de las adquisiciones no se requerirán más unidades financieras. Los repartos mantendrán únicamente

pequeñas pagadurías para manejo de gastos corrientes que cubran manejos de fondos rotativos y caja chica.

La aplicación de tecnología de Business Intelligense basada en Data Minning permitirá establecer en conjunto con el Sistema de Control de Gestión, la mejor forma de asignar y reasignar los recursos económicos en la Armada.

Además de buscar el máximo nivel de eficiencia y eficacia en el manejo de los Recursos Económicos, se logrará que ésta gestión sea más transparente, lo que a su vez trae beneficios para la Inspectoría General de la Armada como ente de Control.

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General de Finanzas de la Armada:

- Optimizar los procesos financieros dirigidos a los Sectores de la Armada.

- Alcanzar la excelencia en la administración financiera.

- Optimizar el sistema integrado de contabilidad, presupuesto y activos fijos.

- Invertir los Recursos Financieros disponibles mejorando su rendimiento y calidad.

Portal Informativo Institucional

A la estrategia de proyección de la imagen institucional se integrará un Portal Informativo Oficial de la Institución. El contenido de éste sitio estará a cargo de un Consejo Editorial Multisectorial dirigido por la Secretaría del Comando General de Marina.

A continuación se muestra un modelo esquemático del Portal de la Armada en la Figura 3.26:

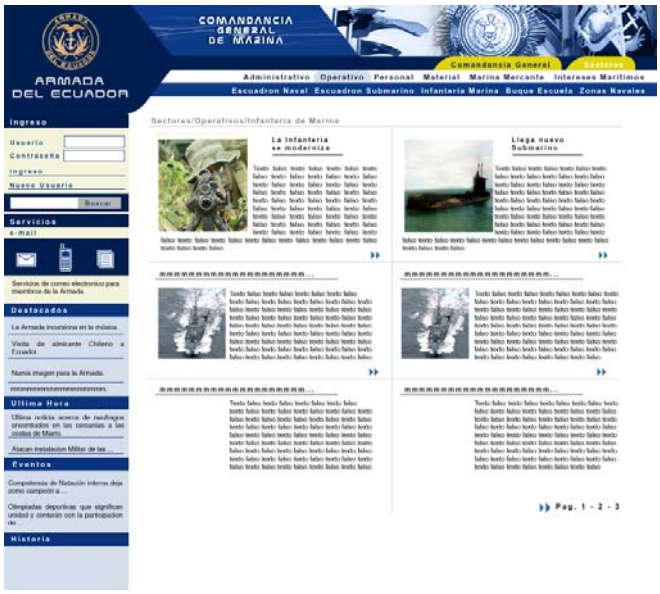


FIGURA 3.26. MODELO ESQUEMÁTICO DEL PORTAL DE LA ARMADA

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Secretaría del Comando General de la Armada:

- Difundir los valores éticos y morales en que se sustenta la Institución para mantener la credibilidad y confianza institucional.

- Mantener informada a la ciudadanía de las actividades desarrolladas en la Armada.

- Mejorar y difundir la imagen institucional a través de los repartos que brindan atención al público.

Sistema de Gestión del Conocimiento

Entendiendo que la creación del conocimiento organizacional es la base de un sistema de innovación, la Armada ha determinado la necesidad de estructurar, generar, emplear y mantener una base de conocimiento institucional, como principal herramienta de apoyo a la Doctrina Naval. Basado en la tecnología de Gestión de Contenidos, implementado en un Portal que permite a los miembros de la Institución tener acceso a toda la normativa de la Institución, así como también a la Directivas Generales y Específicas tanto vigentes como históricas. De igual manera es el

medio electrónico a través del cual se publica la Orden General mensual del Comandante General de Marina.

Este sistema permite mejorar la eficiencia y eficacia del Personal, de modo que todos tengan un registro consistente y actualizado de toda la normativa aplicable para todos los aspectos profesionales de la Vida Naval.

El propósito principal del proyecto es crear un repositorio de archivos en diferentes formatos (Word, Excel, Powerpoint, html, pdf, etc), indexados en base a palabras claves; de modo que se evite el retrabajo y se reutilice contenido.

En la Figura 3.27 se muestra el ciclo de gestión del conocimiento, en el que se implementa la base de conocimientos con tecnología de gestión de contenidos:

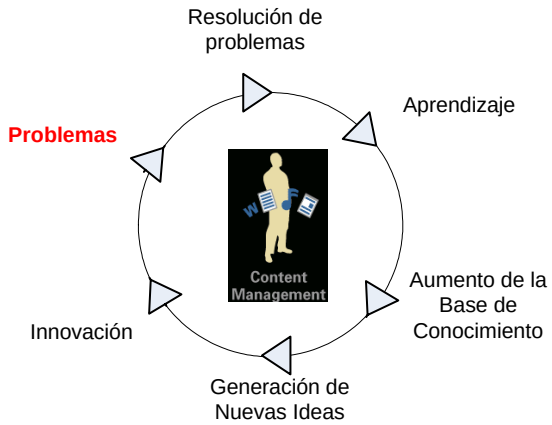


FIGURA 3.27. CICLO DE GESTIÓN DEL CONOCIMIENTO

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Inspectoría General de la Armada:

- Establecer un ente encargado de la sistematización de conceptos, valores, métodos, procesos, normas y principios; que permita capitalizar los activos intelectuales.
- Codificar y difundir la normativa legal vigente.
- Implementar el archivo general y biblioteca de consulta.
- Proyectar una sólida imagen de eficiencia, justicia y equidad.

Sistema de Información Logístico Naval

La logística militar depende vitalmente de la existencia, operatividad y disponibilidad de los equipos, y es necesario utilizar en la mejor forma posible los recursos financieros asignados por el Estado.

El Sistema de Información Logístico Naval está compuesto por diferentes subsistemas conformados en gran parte bajo el paradigma de un gran portal.

Este Sistema de Información gestionan todo el Ciclo Logístico de las Funciones Logísticas relacionadas con el Material: Mantenimiento y Reparación, Abastecimiento, Desarrollo de Bases, y Transporte.

Subsistema de Mantenimiento.- Cubre el mantenimiento preventivo, predictivo y correctivo asistido por computador, en sus diferentes fases de reparación, recuperación y modernización. Incluye el manejo de la información completa de los diferentes componentes de cada uno de los equipos, que conforman cada sistema en todas las Unidades Navales. Además gestiona la asignación de tareas al recurso humano técnico a cargo de las diferentes direcciones; asistiendo además a éste personal con las guías de instrucción para cada tipo de mantenimiento planificado a llevar a cabo. Está integrado con los sistemas de control de inventario de repuestos y con el sistema financiero. Automatiza completamente los flujos de proceso de las Direcciones Técnicas de Ingeniería Naval, y, Electrónica, Comunicaciones y Armamento, para los mantenimientos de reparación y recuperación; y a la Dirección de Investigación y Desarrollo para el mantenimiento de modernización. Los flujos de proceso automatizados son considerados de extremos a extremo, es decir desde que el cliente interno (las Unidades Navales) requieren anticipadamente un

mantenimiento o reparación abriendo la respectiva Solicitud de Trabajo, o a partir de la generación automática de tal Solicitud a través del instrumentaje predictivo; hasta la entrega del trabajo y cierre del proceso. El componente tiene una interface web que conforma el portal que mantiene informado del estado actual de las órdenes de trabajo en proceso a las Unidades Navales, así como también a los diferentes niveles de Mando. Con la aplicación de tecnología de Business Intelligense se provee análisis multidimensional que permita determinar sistemas, equipos y componentes con altas tasas de falla.

En la Figura 3.28, se muestra lo que representa el mantenimiento asistido por computador que se pretende implementar con éste subsistema:

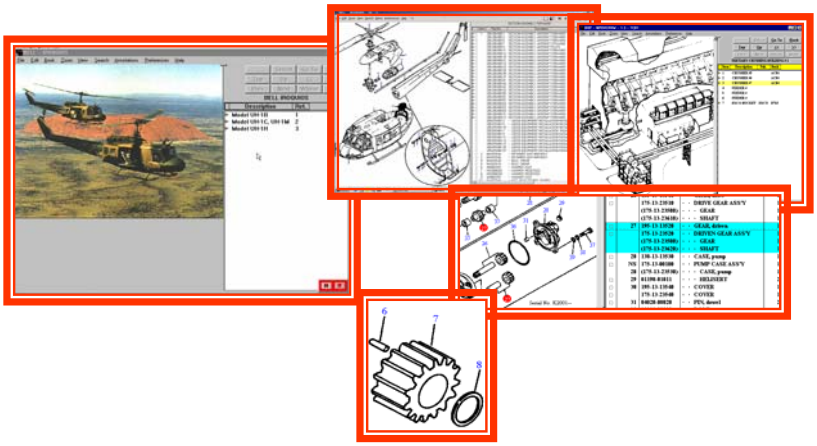


FIGURA 3.28. MANTENIMIENTO ASISTIDO POR COMPUTADOR

Subsistema de Control de Proyectos de Desarrollo de Obra Civil.- Cubre todo el manejo de Proyectos de Desarrollo de Obra Civil a cargo de Dirección de Ingeniería Civil y Portuaria de la Armada. Básicamente integra la tecnología de automatización de procesos de trabajo “Workflow” con sistemas transaccionales integrados al Sistema Financiero de la Armada. Es un sistema distribuido totalmente basado en web que permite operar los procesos desde las obras mismas a los Inspectores Técnicos en Obra. Mantiene un control de los avances de los contratistas y proveen acceso a los Organismos de Control e Inspección permanentemente. Provee un Portal de Construcciones, que mantiene informadas a las empresas privadas y públicas sobre los proyectos que la Armada está llevando a cabo o ha planificado ejecutar, de manera que la licitación y adjudicación de contratos se mantenga totalmente transparente para la sociedad ecuatoriana.

Subsistema de Abastecimiento.- Implementado a través de una solución híbrida de e-procurement y e-marketplace, ofrece a través de un portal toda la funcionalidad relacionada con la función logística de abastecimiento. Parte por la determinación de las necesidades, para lo cual se analiza el comportamiento del consumo de los distintos repartos navales de equipos, materiales, insumos y repuestos. Esta información es obtenida de los pedidos

atendidos a través de una tienda electrónica provista por el portal a través del Intranet. Con éste esquema se busca reducir la necesidad de que los repartos navales mantengan bodegas de suministros, materiales y repuestos locales, sino hasta un nivel óptimo determinado (buffer de primer nivel), así se evitaría un efecto latigazo que ocasione un descenso en el stock de las bodegas centrales ocasionando una reposición debido solamente a la acumulación ineficiente de inventarios en “bodegas satélites” en los diferentes repartos. Una vez determinada la necesidad, se pasa a la fase de obtención, para lo cual se elaboran los diferentes requerimientos los mismos que son publicados como parte del proceso renovado de adquisiciones en el portal. Los proveedores registrados y debidamente calificados tendrán acceso a los procesos, haciendo sus ofertas en línea, las que una vez calificadas como técnicamente habilitadas, pasan a un periodo de subasta inversa en línea por un periodo corto de tiempo, donde se garantiza la confidencialidad de los concursantes entre sí y para los encargados de la adquisición. Adjudicada la adquisición se prosigue con la evaluación del rendimiento del proveedor. Todo el manejo de los inventarios está integrado al Sistema Financiero. El portal implementa pagos electrónicos a sus proveedores a través de Transferencia Electrónica de Fondos. El portal estará integrado

con el Subsistema de Transporte vinculándose con la fase de distribución, para lo cual se implementarán modelos de optimización de rutas, horarios y flotas, de modo que se asignen los medios más adecuados para la distribución. En concreto, el proceso actual toma aproximadamente 22 horas laborables, con el proyecto planteado se pretende reducir el tiempo a 4 horas laborables. El subsistema de abastecimiento también incluye la modalidad de adquisición bajo contratación pública y licitación en el portal.

En la Figura 3.29 se muestra el modelo conceptual del subsistema de abastecimiento:

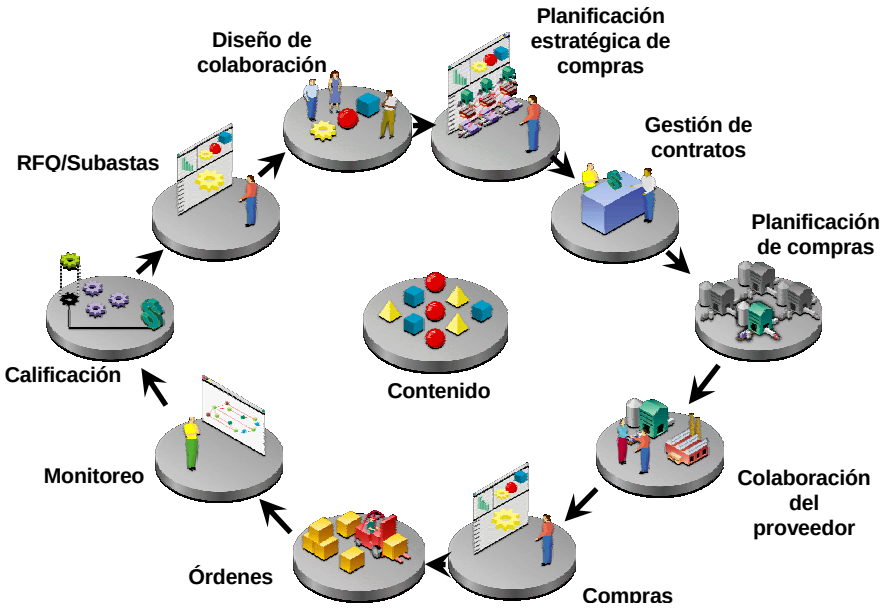


FIGURA 3.29. MODELO CONCEPTUAL DEL SUBSISTEMA DE ABASTECIMIENTO

Subsistema de Transporte.- Este subsistema basado en el paradigma de portal, permite atender los diferentes requerimientos de la Armada de medios de transporte vehicular: automóviles, camionetas, buses y camiones. Básicamente es un sistema de gestión de flotas que está integrado al Sistema de Mantenimiento y al de Recursos Humanos para la asignación de tareas. Controla además el control de consumo de combustibles.

Subsistema de Gestión del Apoyo Logístico Inmediato.- Es un componente que se emplea durante las Operaciones Navales, cuando se activan los Grupos de Apoyo Logístico de la Armada. Estos son grupos móviles que tienen como misión soportar el esfuerzo logístico de la Fuerza. Básicamente es un sistema del tipo Help Desk, pero orientado a reportar y aperturar tickets de solicitudes de trabajo inmediatas, que son enrutadas de manera inteligente a los distintos GAL, mejorando la eficiencia y recolectando las métricas de desempeño, que permitan mejorar la asignación de medios de tales grupos.

Subsistema de Control de Cargas Líquidas.- Es un sistema que integrado a sensores automáticos de medida de flujo y capacidad, determinan el consumo real, las existencias reales y los saldos en

los grandes repositorios de abastecimiento y de las Unidades Navales de: Combustibles, Aceites y Agua Dulce.

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General del Material:

- Constituirse en una Organización moderna, ágil y eficiente. Considerando:
    - Monitorear y medir la consecución de los Objetivos definidos en el Planeamiento Estratégico Institucional.
    - Mejoramiento continuo de los procesos.
    - Optimización del Sistema de Información basado en los procesos logísticos.
    - Optimización de los procesos de contratación pública.
    - Ejecución eficiente de la función básica con los recursos económicos asignados para tal efecto.
- Alcanzar la máxima eficiencia posible del material. Considerando:

- Implementar el mantenimiento planificado en las Unidades Navales y en los medios terrestres de transporte.
- Definición de modelos que permitan determinar la obsolescencia técnica y logística de los Sistemas y Equipos.
- Elaborar los planes de desarrollo de la frontera Norte.
- Ejecutar los planes de mantenimiento de las instalaciones terrestres.
- Optimizar la adquisición y control de vehículos terrestres de la Armada.

- Optimizar el empleo de los recursos asignados al Sector del Material. Considerando:
  - Optimizar el proceso de adquisiciones locales.
  - Optimizar los procesos de importaciones.
  - Optimizar el control de inventarios.

- Optimizar la determinación de necesidades.

- Planificar y controlar la adquisición de combustibles y lubricantes.

- Fortalecimiento de la Dirección General del Material. Considerando:

  - La modernización de los procesos de gestión de las Dirección Técnicas y los talleres.

  - Impulsar la investigación científica y técnica para disminuir la dependencia tecnológica externa y propender al desarrollo tecnológico institucional y nacional.

  - Desarrollar y fortalecer el apoyo logístico móvil y fijo para la Fuerza Operativa Naval y Guardacostas.

Sistema de Información de Gestión de Sanidad y Hospitalaria

Proyecto de automatización de la gestión técnica hospitalaria del Hospital Naval de Guayaquil, conformado por los siguientes componentes:

Admisión de pacientes.- Integrado con facturación, Caja, Cobranzas y Seguro Social de Fuerzas Armadas. Permite estandarizar e integrar los procesos de admisión de pacientes en las áreas de: emergencia, ambulatorio, hospitalización y servicios. Este módulo deberá permitir:

- Mantener un manejo único de historia administrativa por paciente.
- Búsqueda de historias por diferentes campos.
- Consultas de pacientes por estado de admisión.
- Elaboración de presupuestos referenciales de atención.
- Administración de habitaciones.
- Manejo de ingresos, preingresos y traslados de pacientes entre áreas y habitaciones.
- Registro de información personal y laboral de pacientes.
- Relaciones de diagnósticos con tratamientos.
- Definición de afiliaciones para determinación de precios y descuentos en servicios.

- Manejo histórico de la información por admisión de pacientes.

- Estadísticas de presupuestos emitidos y admisiones realizadas.

Servicio de Intervenciones.- Múltiples opciones de control y administración de áreas de quirófanos, sala de partos, sala de emergencias, sala de hospitalización. Contiene un agente generador de estadísticas en base a los registros en quirófano del tipo de intervenciones realizadas, lo que brinda entre otras cosas:

- Relaciones de equipos utilizados en intervenciones y tratamientos.

- Desglose de medicamentos y material médico.

- Clasificación de productos consumidos por tipo de servicio.

- Enlace directo con inventario y facturación.

Órdenes de servicio.- Permite controlar la realización de exámenes de rayos X, laboratorio, banco de sangre, o cualquier otro servicio administrable a través de órdenes de trabajo.

Administración de paquetes.- Permite establecer las diferentes opciones de cargos por cobertura del Seguro Social de Fuerzas Armadas, facturando el costo que corresponda si es Militar en Servicio Activo, Familiar Dependiente o Particular.

Reservación de quirófanos.- Planificación del uso de las salas de quirófano proveyendo una visión clara del cronograma de uso de los quirófanos.

Facturación.- Permite facturar desde cualquier área los valores correspondientes por los diferentes motivos de los servicios prestados. Entre otros puntos hace lo siguiente:

- Manejo de estado de pre-alta, reingreso y anulación de alta.
- Carga automática de servicios fijos.
- Reportes de servicios no facturados.
- Reportes para asientos contables.
- Listado de facturación por sitio, item de servicio, cuenta.
- Listado de notas de crédito en un periodo.
- Aplicación de coberturas y anticipos a facturas.

- Anulación de facturas.
- Cálculo automático de descuentos por nivel de prestación del seguro.
- Impresión de estados de cuenta de pacientes.
- Cargas automáticas por servicios adicionales.

Historia Clínica.- Manejo de un número único de historia clínica del paciente, totalmente digitalizada.

Farmacia.- Proceso de facturación al paciente, venta a terceros, incorporación de equipos de impresión y lectores de código de barra, manejo de inventarios.

Control de citas.- Por especialidad médica, agenda de disponibilidad de médicos por día, programación de consultas ambulatorias.

Honorarios Médicos.- Control y generación de los honorarios del cuerpo médico y proveedores de servicios.

Contabilidad y Finanzas.- Manejo integral de la Gestión de los Recursos Financieros.

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General del Personal:

- Optimizar el uso de las Unidades de Salud que registran bajos índices de ocupación y contribuir el crónico déficit fiscal del sector de la salud.

- Proveer medicamentos genéricos a precios bajos y en amplio stock a toda la Población Naval.

- Mejorar la calidad de la atención médica en los centros hospitalarios de la Armada.

Sistema de Información de Carrera Naval

Este sistema permite gestionar los diferentes servicios de bienestar, educación, desarrollo profesional y carrera profesional, a través de un portal de Recursos Humanos que basado en la tecnología eCRM permita mejorar el desempeño profesional, disminuir la tasa de deserción, y mejorar el reclutamiento del Personal Naval. A través de éste portal, el personal naval tiene acceso a sus registros personales de su carrera, los que se encuentran registrados en el Sistema Transaccional de Personal, y en la Libreta de Vida Naval ya digitalizada; así como también se tiene acceso a las mejores posibilidades de desarrollo profesional

que sean acordes a su perfil y situación personal. El portal implementa además recursos de asesoría legal y consulta sobre regulaciones impuestas a la carrera naval. A través del portal, el personal puede tener acceso a los servicios de bienestar como son: Comisariato Naval a través de una tienda electrónica, cooperativas a través de Home Banking, Vivienda Fiscal, Convenios Educativos, Comerciales, Culturales y Deportivos.

En la Figura 3.30 [24] se muestra un diagrama esquemático de la solución propuesta, es decir la habilitación del acceso vía navegador web, con personalización a los datos del sistema integrado de personal de la Armada:

FIGURA 3.30. DIAGRAMA ESQUEMÁTICO DEL PARADIGMA PORTAL [24]

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General del Personal de la Armada:

- Optimizar las tareas que cumple la Dirección General del Personal como una gran Dirección responsable del manejo integral del personal.

- Optimizar el empleo del Recurso Humano, ubicando el personal de Oficiales y Tripulantes en las plazas orgánicas conforme a su especialización, perfeccionamiento y experiencia.

- Modernizar la gestión del bienestar y crear la infraestructura necesaria para ser proveedora de servicios de calidad.

Modernización del Sistema de Educación Virtual

Mejoramiento de la primera versión del Sistema de Educación Virtual utilizado actualmente para los cursos por correspondencia (a distancia) de la Academia de Guerra Naval, para lo cual es necesario implantar un sistema de Gestión del Aprendizaje, para desarrollar los cursos obligatorios, opcionales y tutoriales. El sistema permitirá planificar los cursos, crear y mantener los contenidos y llevar a cabo las evaluaciones.

El Sistema de Educación Virtual permitirá llevar a cabo cursos de especialización tipo diplomado, orientado a la Oficialidad para desarrollar competencias en gestión administrativa y Alta Dirección.

Permitirá además llevar a cabo cursos de especialización técnicos, orientados a la Oficialidad y Tripulantes para desarrollar competencias en áreas técnicas del material, intereses marítimos y administración de recursos humanos.

En la Figura 3.31 se muestra la página principal del sistema de educación a distancia de la Academia de Guerra Naval:

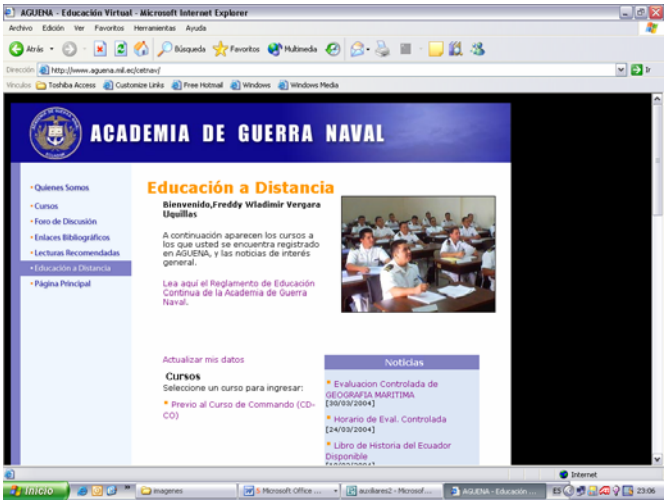


FIGURA 3.31. SITIO WEB DEL SISTEMA DE EDUCACIÓN A DISTANCIA DE LA ACADEMIA DE GUERRA NAVAL

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General del Personal de la Armada:

- Capacitar a los Mandos Medios para que conduzcan proyectos de reingeniería de procesos y mejoramiento continuo en sus repartos.

- Acoplar el proceso educativo a la Carrera Naval y necesidades institucionales, perfeccionando el modelo del sistema educativo.

- Alcanzar la excelencia de la educación en los Centros Educativos.

- Crear una educación complementaria en las áreas del material, intereses marítimos y recursos humanos.

- Propender a la creación de la Universidad Marítima.

Sistema de Información de Gestión de la Autoridad Marítima

Es un Sistema de Información que implementa a través de un Portal en Internet la ventanilla virtual de la Autoridad Marítima, mejorando la eficacia de los procesos de gestión que tienen mayor impacto con los clientes externos de la Dirección General de

Marina Mercante: Gente de Mar, Agencias Navieras, Operadores Portuarios, Personal de Marina Mercante, etc.

El Portal además permitirá integrar todas las fuentes de datos actualmente dispersas en las distintas capitanías del litoral, con lo cual se mejorará considerablemente la eficacia del ejercicio de la Autoridad Marítima.

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General de Marina Mercante y del Litoral:

- Estructurar la Dirección General de Marina Mercante para alcanzar una mayor eficiencia y agilidad en el ejercicio de sus funciones.
- Desarrollar y fortalecer las capitanías de puerto.
- Impulsar el desarrollo de la Marina Mercante Nacional.
- Apoyar el desarrollo portuario nacional.
- Optimizar las administraciones de las Superintendencias de los Terminales Petroleros.

Portal de Información Ecuador Marítimo

Sistema de Información Comunicacional que busca proyectar y desarrollar los Intereses Marítimos en el Ecuador.

A través de éste portal se informan todos los convenios y acuerdos internacionales suscritos por el Gobierno del Ecuador, así como los proyectos de convenios y acuerdos con su respectivo análisis como parte del asesoramiento que da la Armada del Ecuador en los temas marítimos al gobierno central.

El portal pretende además proyectar el desarrollo de los Intereses Marítimos a partir de la Investigación Científica a cargo del Instituto Oceanográfico de la Armada, en donde la comunidad científica internacional podrá interactuar con los Sistemas de Información disponibles en el web, para el análisis de información y datos océano-atmosféricos recolectados, analizados e interpretados por los técnicos del Instituto en las áreas de nuestra jurisdicción.

El portal proyecta también los logros del Instituto Antártico Ecuatoriano, donde se encuentran disponibles las distintas expediciones que ha llevado a cabo el Instituto Oceanográfico en el Buque Oceanográfico Orión al Continente Blanco, así como los

diferentes estudios y experimentos llevados a cabo en la Estación Científica “Pedro Vicente Maldonado”.

Otra faceta del desarrollo de los Intereses Marítimos, son los museos navales, los mismos que tendrán su versión virtual en el portal.

La Armada además de estudiar el océano y la atmósfera, fiel a los orígenes de la navegación más antigua, sigue mirando al firmamento, por lo cual el portal tendrá una versión del Planetario en el Internet.

Otra de las actividades que lleva a cabo el Instituto Oceanográfico de la Armada, es la administración de las ayudas a la navegación como parte de las acciones para garantizar la seguridad de la navegación en las aguas de nuestro mar territorial. El Instituto Oceanográfico de la Armada es el organismo técnico responsable a nivel nacional de la creación de las cartas náuticas y del mantenimiento de las ayudas a la navegación. En el Portal estarán disponibles las cartas electrónicas que actualmente se están desarrollando en el Instituto para su comercialización.

En las Figuras 3.32 y 3.33, se presentan los sitios web de la Dirección General de Intereses Marítimos, y del Instituto Oceanográfico de la Armada:

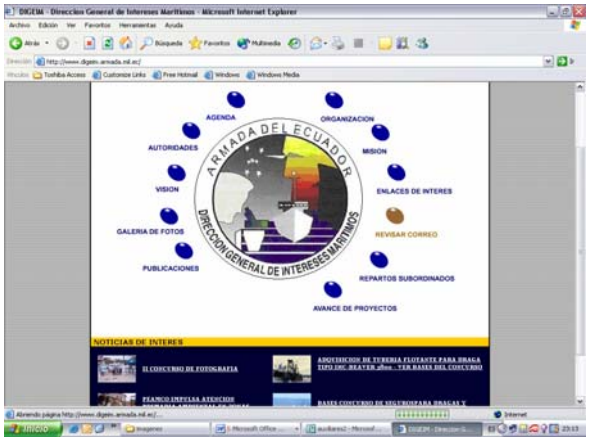


FIGURA 3.32. SITIO WEB DE LA DIRECCIÓN GENERAL DE INTERESES MARÍTIMOS

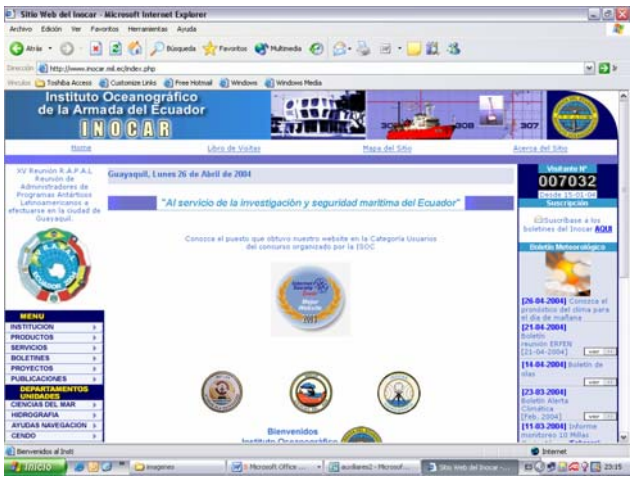


FIGURA 3.33. SITIO WEB DEL INSTITUTO OCEANOGRÁFICO

Este proyecto está alineado estratégicamente con los siguientes Objetivos Específicos de la Dirección General de Intereses Marítimos:

- Modernizar y mejorar los procesos de la Dirección General de Intereses Marítimos de la Armada, generando eficiencia dentro de la Armada y el país.

- Promover la adhesión del Ecuador a la Convención del Mar y demás acuerdos internacionales de interés para el país.

- Contribuir a la planificación del desarrollo de la navegación fluvial amazónica y costera.

- Concienciar al Personal Naval y sectores de la comunidad marítima que desarrolla actividades en el mar, sobre la necesidad de proteger y preservar el medio marino – costero.

- Hacer de los ecuatorianos un pueblo con una definida y clara conciencia marítima, que le permita desarrollar una cultura en el mar y sus recursos en propio beneficio.

- Garantizar la seguridad para la navegación en el mar, ríos y demás vías navegables.

- Contribuir a las comunidades costeras, Personal Naval y estudiantes de educación básica mediante la educación en los beneficios del manejo sustentable de los ecosistema marino – costeros para elevar la calidad de vida de la población ecuatoriana.

- Optimizar la investigación marítima en apoyo a las Operaciones Navales y el desarrollo del país.

- Contribuir al conocimiento y aprovechamiento sustentable de los recursos del mar y a la protección de la zona marino – costera.

- Incrementar el conocimiento del océano, especialmente en los procesos relacionados a la interacción océano – atmósfera y al equilibrio de los ecosistemas marino – costeros, para contribuir al desarrollo de las comunidades costeras, continentales e insulares.

- Alcanzar niveles óptimos de interacción con entidades científicas, educacionales, de financiamiento nacional e internacional, que coadyuven al desarrollo de la investigación marítima en el Instituto Oceanográfico de la Armada.

- Desarrollar actividades de investigación de Historia Marítima que permitan escribir, difundir y proyectar nuestra Historia Institucional y del Mar Ecuatoriano a la comunidad nacional e internacional.

- Mantener el archivo de documentación histórica en forma eficiente a fin de que su consulta y búsqueda de datos históricos contribuyan a escribir la Historia Marítima del Ecuador.

3.7.2 Repositorios de Información

Leyes y reglamentos.

La Armada, tiene regulada su actividad a través de leyes y reglamentos, los mismos que deben ser ampliamente difundidos y conocidos por todos sus miembros de modo que se pueda ejercer el Comando, y se cumpla con la administración de justicia. Para ello es necesario contar con un sitio web que permita el acceso a todas las leyes y reglamentos internos, a través de cualquier navegador web, con acceso a la red TCP/IP.

De este modo, todos los miembros de la fuerza, tendrán acceso a las normas vigentes, puesto que estas serán fácilmente actualizadas, sin ser necesario contar con un mecanismo manual

de registro de cambios y correcciones para controlar las reformas y actualizaciones, como se lo lleva actualmente en los medios basados en papel. El personal naval, podrá tener acceso a la información que regula y reglamenta sus actividades, la que siempre deberá estar actualizada en un repositorio común, en forma consistente disminuyendo notablemente los esfuerzos de impresión, distribución y actualización de copias, pero esencialmente dando la facilidad de contar con acceso a las leyes y reglamentos actualizadas y vigentes, lo que permitirá mejorar las actividades reglamentarias.

Manual de Organización de la Armada.

El Manual de Organización de la Armada, describe funcionalmente a la institución, indicando su definición, misión, objetivos y tareas.

Adicionalmente, define la estructura orgánica de la Armada, indicando los órganos que la conforman, y sus guías funcionales.

Es muy importante, que todos los miembros de la institución, tengan acceso a esta información, de modo que se entienda plenamente la forma en que la Armada está organizada, y por

tanto se conozca todas las responsabilidades que tiene cada reparto dentro de la organización.

De igual manera, cada reparto tiene su propio manual de organización, en el que se define el reparto, su misión, objetivos y tareas; su estructura organizacional y las guías funcionales para cada plaza dentro del reparto. Si esta información está publicada en línea, desde el manual de organización de la Armada, se puede tener vínculos directos a estos manuales de los repartos, de modo que se pueda revisar a todas las responsabilidades de los miembros de la institución en sus diferentes plazas orgánicas.

Manuales de Procesos

Los Manuales de Procesos son aprobados por el Estado Mayor de la Armada, a través de la Dirección de Desarrollo Administrativo e Informático. En ellos se plasma y estandariza la forma de conducir las diferentes actividades, encadenadas en una cadena de valor definida.

En estos manuales se describen incluso los procedimientos establecidos para las diferentes actividades para todos los procesos que conforman los macroprocesos principales de la Armada.

Directivas Generales Permanentes

Las Directivas Generales Permanentes, son disposiciones emanadas por el Comandante General de Marina con un alcance institucional, o por un Director General, con un alcance funcional en el área en que su Dirección actúa, como por ejemplo: Normas para el manejo adecuado de la información calificada, emanadas por la Dirección de Inteligencia Naval, o normas para la operación de maquinaria de propulsión principal en las unidades navales, emanadas por la Dirección de Ingeniería Naval.

3.7.3 Publicación

La publicación de la información es aplicable a la transmisión de información concurrente, la que tiene como propósito con cierta frecuencia establecida, comunicar disposiciones temporales a la Fuerza Naval. El costo de difundir esta información en medios impresos en papel se puede reducir drásticamente además de garantizar el acceso a la información relevante en demanda.

Orden General

La Orden General es publicada tres veces en cada mes, con el propósito de informar las diferentes movilizaciones del personal naval, sus condiciones de ascenso, condecoraciones, sanciones, y

diferentes situaciones que regulan la condición profesional del personal naval, el bienestar naval y boletines informativos del Instituto de Seguridad Social de las Fuerzas Armadas.

Directivas Generales Temporales

Las Directivas Generales Temporales, son disposiciones emanadas por el Comandante General de Marina con un alcance institucional, o por un Director General, con un alcance funcional en el área en que su Dirección actúa, con un carácter temporal, en la que se dan disposiciones para llevar a cabo una función encomendada a la Fuerza Naval, como por ejemplo: Elecciones populares.

CAPÍTULO 4

4. DISEÑO DE LA INTRANET DE LA FUERZA NAVAL

Normalmente un buen diseño de una aplicación contempla tres funciones principales bien definidas: el interfaz de usuario, la lógica del negocio y la base de datos. Por tanto, el desarrollador debería decidir las plataformas en que éstas funciones se ejecutarán. En el Intranet, la interfaz de usuario está definida como un estándar en el navegador web como cliente universal, y las aplicaciones deben propender a ser independientes de plataforma. Esto permite al equipo de desarrollo concentrarse en la usabilidad, la lógica y el contenido necesario que debe proveerse para la aplicación.

Las aplicaciones tradicionales con un enfoque de sistema transaccional requieren una estructuración de la información para ser almacenada en una base de datos. Si bien es cierto que el desarrollo de las tecnologías

analíticas de las bases de datos como: inteligencia de negocios, almacenes de datos y minería de datos, permiten tener múltiples aplicaciones orientadas a los niveles gerenciales, ejecutivos y soporte a toma de decisiones; no son el enfoque más adecuado para representar debidamente las ideas, el aprendizaje organizacional o la base de conocimientos. Estas ideas y el conocimiento plasmado en un documento fruto de una actividad eminentemente humana, no siempre pueden representarse con cantidades discretas, números y atributos generalizados, que es lo que las bases de datos manejan muy bien. Si bien es cierto, hoy en día el papel de tecnologías como XML ha permitido contar a las bases de datos con esquemas autodescriptibles muy útiles para crear metadata de manera mucho más flexible, lo que permite basar la gestión de contenidos documentales en una base de datos, no son sino una adaptación del mundo de la estructuración al mundo de lo “no estructurado”. La alternativa en una Intranet son los sistemas de administración de información, los mismos que sin sacrificar las ideas y el conocimiento plasmado en un documento, permiten tener la misma versatilidad al momento de buscar información en un ambiente web. Por ejemplo, quien duda de la capacidad de recuperar documentos relevantes a un criterio de búsqueda determinado del sitio www.google.com. Aún cuando el desarrollo de aplicaciones para una Intranet, están en su

infancia, no hay que dejar de lado que nacen desde la perspectiva de administración del conocimiento y no desde la perspectiva de la lógica estructurada.

Pero la principal característica que hacen que una Intranet sea tan atractiva, no es la cantidad de información disponible en forma ágil, sino el hecho de poder hacer de cualquier usuario un publicador de información en el medio electrónico sin necesidad de pasar por un formulario del tipo "llene los espacios en blanco"; si esto no se consigue, no es posible habilitar una verdadera capacidad de innovación. Hoy en día tenemos la tendencia de habilitar a los trabajadores para que sean “trabajadores del conocimiento”; de hecho existe una marcada tendencia en Fuerzas Armadas a la necesidad de gestionar el conocimiento. Michael Howard, asesor del Comando Conjunto de las Fuerzas Armadas de Estados Unidos de Norteamérica, sugiere que: “La guerra ya no es solo una profesión exigente en lo físico, sino además en lo intelectual. Es esta última capacidad la que debe ser cultivada, desarrollada y sostenida por los Militares.” [25]

¿Cómo podemos tener una organización que aprende, si basamos nuestros procesos en una estructura rígida? Si conocemos la estructura de un problema y de la información, ¿Cómo podemos aprender algo nuevo? El aprendizaje es un proceso de descubrir estructuras, si tan solo

administramos el conocimiento en un repositorio que encaja en una estructura ya entendida, ¿Cómo podemos aprender en forma radical nuevas cosas?

4.1 Reglas para Guiar el Pensamiento del Diseñador de una Aplicación de Intranet

Al diseñar una aplicación para una Intranet, es necesario tener en consideración las siguientes reglas [4]:

1. Piense más allá del enfoque tradicional de desarrollo de aplicaciones, piense siempre en la funcionalidad deseada.

Las aplicaciones de una intranet son modulares, por lo que necesitamos pensar en funciones completas. No es necesario construir todas las piezas de una sola vez. Con un enfoque iterativo e incremental, es posible enriquecer de manera continua las prestancias de un Intranet. Mantenga el enfoque en los objetivos que se desean alcanzar, el resultado final y formas alternativas de llegar ahí.

2. Desarrolle procesos en términos de clases funcionales y en el cómo están relacionadas ellas entre sí.

Las aplicaciones de propósito general, deben empezar a ser construidas en funciones lógicas más simplificadas. Debemos mirar como las clases funcionales pueden ser compartidas en dominios especializados. La mayoría de aplicaciones pueden ser definidas en términos de cuatro clases funcionales:

a) Funciones de control (clientes, recursos, inventarios).

b) Funciones de configuración (información de: productos, soluciones, beneficios e instrumentos financieros).

c) Información:

- Publicación (halar información).
- Notificación (empujando información).

d) Intercambio:

- Negociación (ideas).
- Colaboración (ideas).
- Transacciones (dinero).

Las clases de funciones de este tipo, nos facilitan la reutilización de contenido y de las herramientas, en un mayor rango de dominios.

3. Para cada función identificada, verificar si el proceso soportado es estructurado, semi - estructurado o no estructurado.

Para cada clase funcional, pregunte que es lo que espera del usuario: comportamiento estándar y repetitivo, o pensamiento e innovación. Se debe reconocer que para cada uno de los usuarios, se pueden requerir diferentes procesos para lograr que alcance los resultados deseados. Sin embargo, para cada clase funcional específica, en un proceso específico, el grado de estructuración debe ser plenamente identificado. Al determinar el nivel de estructuración, se puede identificar qué herramienta o enfoque utilizar al implementar la clase funcional, por ejemplo: las transacciones monetarias, cronogramas, control y perfiles de usuarios, son mejor implementadas con tecnología de bases de datos transaccionales. Cuando los procesos son menos estructurados, como la colaboración de otros usuarios, la innovación, creación y negociación, la tecnología basada en paso de mensajes es más apropiada.

4. Mirar cada interacción con los usuarios en términos apropiados de halar y empujar.

Para identificar características de empujar y halar información en las aplicaciones de una Intranet, puede ser útil la siguiente guía:

- ✓ Empuje lo que se necesita conocer al instante, y tiene un tiempo de vida útil corto, como por ejemplo: Noticias y pedidos instantáneos, Comunicación personal.

- ✓ Hale lo que será referenciado en el futuro: Cualquier cosa que pueda ser impresa para una gran cantidad de personas, Comunicación concurrente. (Reuniones, conferencias, etc)

- ✓ Si la definición no es tan obvia, considere inicialmente el enfoque de empuje de información, pero con control del usuario. Ejemplo: uso de agentes personales, distribución de contenidos bajo suscripción.

5. Soporte al aprendizaje de individuos y organizaciones.

Las aplicaciones de una Intranet deben diseñarse con características de adaptación y aprendizaje en mente. Se pueden utilizar bases de conocimiento para ayudar al aprendizaje individual, recuperando la forma en que otros han aprendido y la han publicado para que esté disponible para la organización.

El aprendizaje organizacional, puede darse en forma de grupos de discusión o sitios de conversación, puede existir también sitios web con preguntas frecuentes, bases de datos documentales, etc.

4.1.1 Normas de Diseño de Aplicaciones

Una Intranet, es como el silicón del software. La tecnología de estado sólido que revolucionó la industria electrónica, desplazando las consideraciones de diseño de circuitos básicos a un mayor nivel de abstracción, de modo que se pueda pensar en la solución de un problema desde el punto de vista de funciones a ser desempeñadas, y no de cables y componentes básicos. De igual manera, los estándares de comunicaciones de Internet aplicados a una Intranet; junto con los estándares de contenido del web, proveen al usuario una transparencia de la ubicación y la especificación del contenido respectivamente, permitiendo un nivel de abstracción en el diseño de aplicaciones, que permite ver las soluciones como funciones y no como pedazos de código de software. Este concepto, es el mismo que sigue el paradigma orientado a objetos. Ahora la Intranet permite una verdadera universalidad para la reutilización de componentes y objetos, constituyéndose en una fuerte razón e incentivo para migrar en el

desarrollo de aplicaciones del enfoque estructurado, al paradigma orientado a objetos. Los repositorios de clases, pueden ser utilizados a lo largo y ancho de la Intranet si se implementan con el lenguaje universal del web: Java, lo que permitiría aumentar la eficiencia en el uso de recursos a nivel institucional.

Tal como se muestra en la figura No. 4.1, la infraestructura de las aplicaciones en un ambiente de Intranet, se puede dividir en cuatro módulos funcionales: contenido estándar, herramientas de creación de contenido, agentes descubridores y administradores de ambientes.

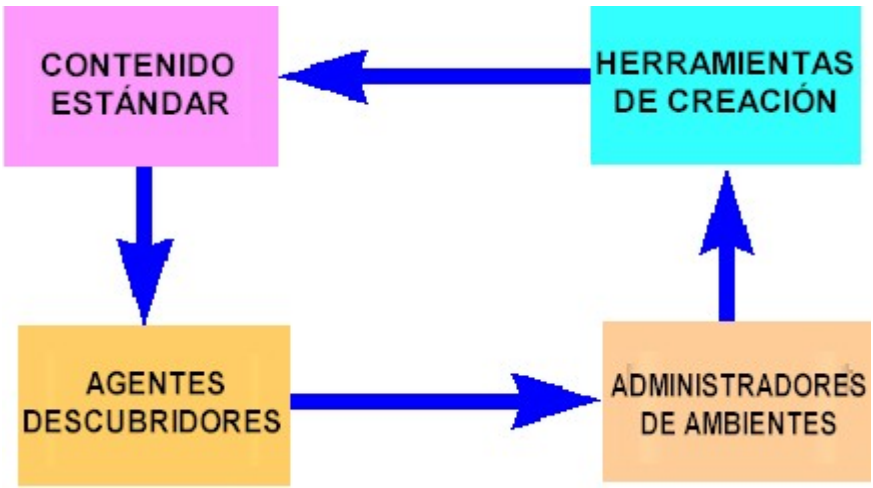


FIGURA 4.1. CUADROS FUNCIONALES DE LA INFRAESTRUCTURA DE UNA APLICACIÓN PARA UNA INTRANET

Las aplicaciones de una Intranet, no son pedazos monolíticos de código de software; son ambientes distribuidos de software que proveen una infraestructura funcional específica, donde ésta sea requerida, permitiendo la personalización de aplicaciones basada en las necesidades y demandas de los usuarios.

1. Contenido estándar.

Lo que ha permitido que el Internet funcione, es la estandarización del contenido y no de las herramientas utilizadas para crear ese contenido. No hay que pasar el tiempo estandarizando en la organización el tipo de navegador o servidor web a utilizar, ni tampoco las herramientas de desarrollo. Hay que entender lo que es importante y diferente en una Intranet. Durante el desarrollo una de las metas más sagradas es la independencia del contenido de algún tipo de estándar propio de un fabricante. El contenido del web no puede ni debe desarrollarse sin estándares públicos, ni independencia de fabricantes.

Si bien es cierto, el web se basa en el modelo cliente-servidor clásico, no se tiene los mismos costos ocultos como: administración de versiones, distribución de actualizaciones y

administración distribuida de aplicaciones. La única aplicación que se requiere instalar en la estación cliente, es el navegador web, lo que se hace una sola vez ya que las aplicaciones se encuentran íntegramente en los servidores corporativos; las mismas que son transmitidas a las estaciones clientes en demanda. Tampoco se está hablando de un servidor único de propósito general, la funcionalidad puede estar distribuida en servidores menos complejos y más especializados, lo que facilita la confianza y administración de los centros de datos y procesamiento. Además el uso de varios servidores especializados, ayuda a distribuir el tráfico en la red eliminando los cuellos de botella. Lo importante es que los servidores provean contenido estándar, y no la marca del servidor.

Es importante recalcar que la estandarización de contenido, no se refiere únicamente al texto y gráficos utilizados; sino también a la lógica que implementa los métodos y procesos. El estándar de facto en este caso, es el uso del lenguaje de programación Java; sin embargo, hay otras opciones que van logrando despuntar y de alguna manera complementarse, como XML, y la propuesto por

Microsoft en la arquitectura .Net con C#. La lógica puede ser procesada en el servidor, en el navegador web, o en ambos.

2. Herramientas de creación de contenido

La insistencia en la estandarización de contenido en una Intranet debe ser constante y permanente, para no sacrificar una de las ventajas que la Intranet puede proveer. Tiempo atrás el formato propietario de una determinada herramienta, como un procesador de palabras de un fabricante específico, obligaba a imponer a esa herramienta en particular como un estándar en la organización para que se pueda permitir a los usuarios compartir información. Aún cuando ahora los diferentes procesadores de palabras cuentan con convertidores de un formato a otro, no hay nada como utilizar un estándar universal como el formato del web: HTML ó XML.

Dentro de este ambiente de editores capaces de trabajar con el formato HTML, se debe insistir en el estándar universal y no en formatos soportados particularmente por determinados navegadores web, por lo que resulta no apropiado desde el punto

de vista conceptual de una Intranet, utilizar el eslogan de: "este sitio se ve mejor con .... "

Es importante revisar el paquete que se va a utilizar en la creación del contenido, puesto que podría haber algún tipo de candado propietario que tan solo a determinados editores de ese paquete se les permita hacer cambios en el contenido que hemos creado. La insistencia, es un apego pleno a los estándares de contenido web.

Los editores que se utilicen, deben ser capaces de crear el contenido en formato HTML, así como leer y editar otros archivos HTML no creados con ese editor, y volverlo a guardar sin ningún inconveniente. El uso de ciertos editores, como Microsoft Word, permitirán implementar políticas de migración de la información en formatos propietarios a formato HTML, incluso sin alterar mayormente los hábitos de los usuarios.

Si se cuenta con herramientas de software de administración de bases de datos, se puede también optar por contenido creado en demanda o contenido dinámico. El inconveniente del uso de estos grandes repositorios es que sus capacidades de búsqueda,

catalogación e indexación, se limitan solamente a repositorios de éste tipo, donde no es posible utilizar agentes descubridores basados en robots o arañas, que utilizan los estándares de contenido y los vínculos para: catalogar, indexar y descubrir nueva información, sino más bien las herramientas propias de la base de datos.

3. Agentes descubridores

El uso de esta funcionalidad no es nuevo, puesto que los esquemas de base de datos y sistemas de administración de documentos, que normalmente son altamente estructurados, proveen algún mecanismo para descubrir información en demanda.

La principal diferencia entre este enfoque tradicional, y el de las modernas máquinas de búsqueda que tiene el web, es la necesidad de trabajar excesivamente en la información para estructurarla de modo que funcionen debidamente. Esa necesidad de estructuración, en la medida que la cantidad de información disponible aumenta, demanda un enfoque altamente técnico, muy

dependiente de una infraestructura compleja de un departamento de sistemas de información.

La ventaja de los agentes descubridores, basados en arañas, es la explotación de la estandarización de los vínculos, y la transparencia de la ubicación de la información en un ambiente web. Estos agentes catalogan e indexan el contenido utilizando mecanismos de sistemas de administración de bases de datos en el nuevo ambiente distribuido en varios servidores, creando múltiples repositorios de información a lo largo y ancho de la Intranet corporativa.

Otro uso de éste tipos de agentes puede ser el de mapeo de los sitios web, lo que permitirá generar tablas de contenido de sitios, así como también descubrir y verificar enlaces rotos.

Uno de los usos más orientados a los usuarios, son los agentes que monitorean el cambio de contenido de páginas específicas, notificándolo al usuario.

El potencial de los agentes descubridores de contenido es el poder de habilitar al usuario con el control del flujo y acceso a la información que para él es relevante.

4. Administradores de ambientes

En esta categoría encontramos los administradores de sitios, o los ambientes de desarrollo de sitios web. Normalmente, su funcionalidad está orientada a proveer una vista integrada del contenido de un sitio web, así como desarrollar y administrar de manera más eficiente a estos.

El problema de estas herramientas, es que normalmente están muy atadas en forma propietaria a otras herramientas específicas del mismo proveedor. Sin embargo, los administradores de ambiente, integran las otras tres partes funcionales de una aplicación de Intranet, por lo tanto son muy necesarios.

Al pensar en un administrador de ambiente, es necesario considerar que si la aplicación es de alto nivel, deberá contar con un contenido base que mostrar, un método para descubrir información relevante, y herramientas para actualizar y añadir contenido. Si el proceso es altamente estructurado y bien entendido, entonces el administrador de ambiente es especializado y luce como una aplicación basada en transacciones, normalmente se basan en un sistema de administración de base de datos que genera en forma dinámica el

contenido. Si el proceso es solo parcialmente estructurado, entonces el administrador de ambiente, luce más como un marco de trabajo o una herramienta de propósito más general, como herramientas de publicación, catalogación y búsqueda, para un Servidor Web específico. Si el proceso es no estructurado, el administrador de ambiente es más como una herramienta de desarrollo de sitios, por ejemplo: Microsoft FrontPage ó Macromedia Dreamweaver.

Estas cuatro áreas funcionales que deben ser consideradas por una aplicación de Intranet, son las que en conjunto permiten la administración y manipulación de la base de conocimientos, la misma que deberá estar disponible para satisfacer los diversos requerimientos y cumplir con las expectativas de los usuarios.

4.2 Diseño de la Arquitectura Lógica

La forma de esquematizar el contenido en el Intranet, la infraestructura lógica que permitirá administrar, mantener y producir información, define la arquitectura lógica de la Intranet.

4.2.1 Conceptos Preliminares

Antes de discutir la arquitectura de un Intranet, es necesario revisar algunos conceptos:

Intranets

Ampliando el concepto de Intranet presentado en el capítulo 2, un Intranet es una infraestructura de comunicaciones. Está basada en los estándares globales de comunicación del Internet y en cuanto al contenido en los estándares globales del World Wide Web. Así las herramientas utilizadas para el Internet, son las mismas que las utilizadas en el Intranet.

Dos tipos de páginas

Existen dos tipos básicos de páginas: las páginas de contenido y las páginas de búsqueda. Las páginas de contenido contienen información con algún valor para los usuarios y forman la estructura del contenido del Intranet. Las páginas de búsqueda proveen un contexto para ayudar a los usuarios a encontrar las páginas de contenido apropiadas para sus necesidades actuales de información, y forman la estructura de navegación del Intranet.

Las páginas de contenido pueden tomar muchas formas; pueden ser páginas estáticas, o pueden ser páginas dinámicas donde el contenido se genera "sobre la marcha" desde una base de datos o repositorio de información. Las páginas de contenido pertenecen generalmente a un individuo. Con el tiempo se espera que la forma y el sentido de éstas páginas cambien en la medida que se gane experiencia en áreas de documentos no lineales (vinculados), en multimedios, contenido modular y en la integración con la utilización adecuada de applets (java applets).

Las páginas de búsqueda vienen en más de una forma también, pero siempre tienen la misma función: ayudar a los usuarios a encontrar información relevante. Hay páginas que sirven a una audiencia específica o función. Una página de búsqueda de vínculos contiene vínculos a otras páginas, puede contener una breve descripción del contenido al cual están apuntando para ayudar a los usuarios a evaluar las posibilidades. Las páginas de búsqueda orientadas a la búsqueda, como www.google.com, no se restringen a los alcances específicos de los usuarios, sino que son más bien generales, pero no proveen el mismo nivel de contexto para ayudar a los usuarios a formular sus consultas

apropiadamente. Hoy en día es muy común encontrar una combinación de estas dos estructuras. Las páginas de búsqueda retornan sus resultados como páginas de vínculos con las primeras líneas del contexto y ponderaciones de acuerdo a las coincidencias con los criterios de la búsqueda. Así mismo pueden proveer una nueva búsqueda refinada, dentro del espacio limitado ahora por los resultados de la primera consulta.

En el diseño de la arquitectura lógica de la información, vamos a encontrar sitios centrales de información (sitios web) y sub-sitios de información. Si bien es cierto es necesario estandarizar el contenido, los estilos y ciertas guías para el diseño de las páginas web que conformen estos sitios, a veces es necesario observar la flexibilidad necesaria que permita a los grupos o departamentos incluir sus propios estilos para incentivar la creatividad evitando un ambiente tenso y forzado de producción de información. Estos son los subsitios, grupos de páginas web dentro de un sitio central que tienen un estilo común y generalmente comparten una misma metáfora como mecanismo de navegación. En las páginas principales de estos subsitios es necesario proveer una información general de registro la misma que debe incluir:

- ✓ Información de contacto del grupo o departamento.
- ✓ Una breve descripción del contenido del subsitio.
- ✓ Palabras claves indicativas de tópicos puntuales o funciones que hagan de vínculos, como por ejemplo: Noticias, Servicios, Productos, etc.
- ✓ Una definición de la audiencia pretendida.
- ✓ Un enlace al mapa del subsitio.

Este registro permite a los visitantes explorar y navegar flexiblemente en el subsitio.

Existen unas páginas de búsqueda que son el corazón de esta arquitectura lógica, las guías con valor agregado. El valor agregado se genera al proveer una estructura de acceso al contenido de los sitios web que sintetiza la visualización de la información superando las barreras genéricas impuestas en toda la estructura general. Estas se pueden crear desde el punto de vista de una audiencia específica, un tópico específico o con una tarea en mente como por ejemplo un tutorial. Un ejemplo de estas páginas son: un tour para visitar el sitio para los nuevos usuarios,

una guía para buscar dentro del sitio, una guía para seleccionar un técnico o proveedor.

Todas estas guías pueden incluir narrativas acerca del contenido que se encuentra en el sitio, o de los pasos necesarios para llevar a cabo una tarea, de modo que sirva para educar a los usuarios nuevos.

El uso de estas guías con valor agregado, reduce la lucha interna entre los proveedores de contenido de los sitios por ganar una posición privilegiada en la página principal del sitio, rediseñando su función a un punto de partida para escoger sea una guía de este tipo, o algún destino específico dependiendo si el usuario visita por primera vez el sitio o ya tiene una idea clara de que es lo que necesita y por tanto donde lo puede encontrar. De esta manera la página principal puede ser el sitio elegante con una identidad visual que proyecta la imagen de la organización, departamento o grupo y dirige a los usuarios en forma adecuada a las áreas con contenido.

Un uso especial que tienen las páginas de búsqueda es para asistir a la administración del contenido web. Hay algunas

instancias para estas páginas administrativas, una de ellas es el "Mapa del Sitio"; un conjunto de páginas vinculadas con todo el contenido formal del sitio. Hay otras para la administración de proyectos, administración funcional y soporte de ciclos de revisión.

La figura No. 4-2 muestra los elementos que conforman parte de la arquitectura lógica de la información, los que permiten a la organización administrar formalmente el conocimiento disponible en el ambiente distribuido de la Intranet.

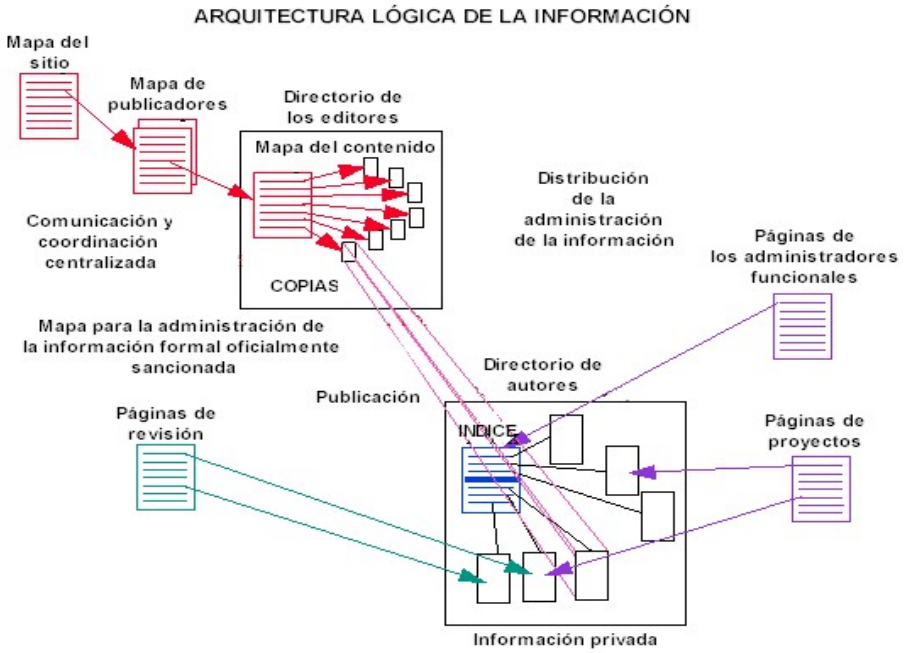


FIGURA 4.2. ARQUITECTURA LÓGICA DE LA INFORMACIÓN

4.2.2 El Mapa del Sitio

Un conjunto estructurado de páginas de búsqueda, puede ser muy útil para la administración del ciclo de vida de la publicación de contenido. Este conjunto conforma el Mapa del sitio. Su primera audiencia son los administradores de la información; pero muchos usuarios lo encuentran muy útil para encontrar información que las otras páginas no permiten visualizar en forma intuitiva.

El mapa del sitio está constituido solo de vínculos a manera de “tabla de contenido”. Cada página pertenece a un comité de la organización encargado de la creación y calidad del contenido bajo su responsabilidad. El mapa del sitio no tiene que estar basado en la estructura de la organización en sí; puede ser un mapa lógico donde el nivel superior es la misión de la organización, el siguiente nivel los lineamientos principales necesarios para cumplir la misión, hasta llegar a los niveles operativos donde está la información.

Tal como se muestra en la figura No. 4-3, el mapa del sitio comienza con una página superior perteneciente al Director General de la organización (delegada generalmente la

responsabilidad al Administrador del Web). Esta página contiene vínculos a los mapas de cada una de las líneas de actividades principales llevadas a cabo por la organización, Sectores en el caso de la Armada, en este nivel son administradas por los publicadores de cada suborganización.

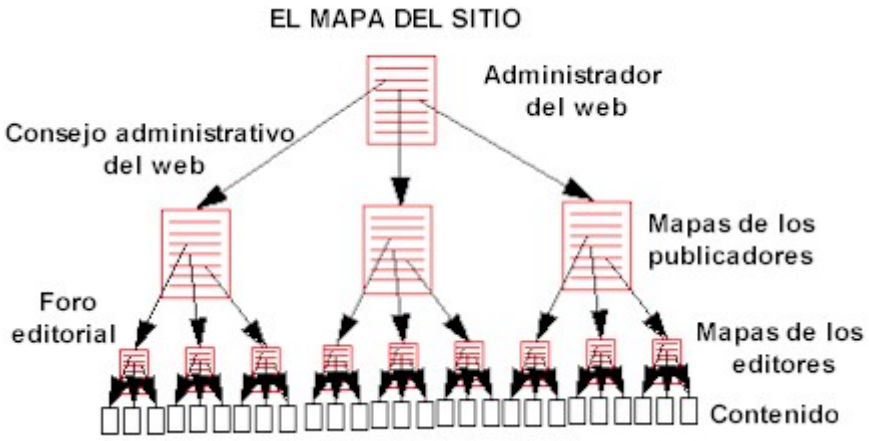


FIGURA 4.3. EL MAPA DE SITIO

Las páginas de los publicadores, tienen así mismo vínculos a las páginas de los editores; las páginas de los editores pueden tener una estructura adicional de páginas que le ayude en la administración y mantenimiento de modo que pueda organizar el contenido a su cargo. Finalmente estas páginas apuntan a las páginas de contenido formal de la organización.

Este modelo se puede aplicar en macro a nivel de las Fuerzas Armadas (o cualquier institución gubernamental). La página del Administrador del Web en el Comando Conjunto apunta a las de los administradores de cada una de las Fuerzas: Terrestre, Naval y Aérea, e incluso a cualquier otra de instituciones que tengan relación con actividades de seguridad nacional como: Policía Nacional, Defensa Civil, Comisión de Tránsito del Guayas, Cancillería, etc. A su vez éstas páginas apuntarán a las distintas agencias, en el caso de la Armada los Sectores; y de éstas a las Direcciones y demás Repartos Navales. Éstas si son muy grandes, pueden tener su propio Administrador y Consejo del web. La ventaja de este modelo de arquitectura lógica, es la flexibilidad. Se puede generar desde arriba hacia abajo, o desde abajo hacia arriba, incluyendo ambos a la vez. Si muchas agencias desarrollan su Intranet independientemente, con este tipo de estructura de Mapa de sitio, se puede enlazar todo al momento que toda la organización termine la implementación de su Intranet. Nada deberá cambiar en los Mapas existentes. Esta flexibilidad es el resultado de la toma de decisiones distribuidas con una comunicación y coordinación centralizada.

El Mapa de sitio provee una foto instantánea del contenido formal de una organización. Los administradores pueden empezar a recorrer todos los vínculos de todo el contenido a su cargo para verificar, administrar y soportar todo lo que ellos son responsables. Es de suponer que la primera vez que se implementa el Mapa del sitio, y los administradores funcionales se involucren, les causará sorpresa ver la cantidad y calidad de información de la que son responsables. La razón es que nunca antes tenían la posibilidad de explorar con tanta facilidad, ni ver tantas vistas múltiples y contextuales de lo que ellos poseen a su cargo cuando la información está en papel o en formatos electrónicos rígidos y estructurados. El Intranet les da a los administradores funcionales ésta capacidad, permitiéndoles apreciar el potencial de un Intranet no solo para acceder a la información, sino para mejorar su calidad.

Un mapa de sitio tiene muchas características interesantes. Una vez que se lo crea los autores y publicadores pueden publicar su información y el contenido se mantiene actualizado en una estructura lógica. Las categorías de contenido o el nivel de funciones de los editores no se afecta aún si se lleva a cabo una

reorganización de funciones en la organización, ya que no está basado en la estructura orgánica de la Institución, sino en las funciones que permiten cumplir su misión. Si ocurre un cambio en el refinamiento de la misión o aumentan los objetivos, el mapa se ajusta rápidamente por los administradores del contenido, lo que significa solo añadir o suprimir unos cuantos vínculos. El contenido no tiene que ser movido de un lado a otro, puesto que en el Intranet el usuario nunca está consiente de la ubicación física de los archivos que tienen la información. Es un mundo virtual en el que la información viene al usuario justo cuando él la necesita. Con esto logramos tener una forma de mantener todo el contenido formal de la organización sin necesidad de forzar la publicación de información a través de una autoridad central que pronto se volvería en un cuello de botella.

4.2.3 El Mapa Sombra

El mapa de sitio provee una forma de administración para el contenido formal, sin embargo, la administración también necesita ver y controlar el trabajo en progreso, es decir el contenido formal que todavía no se ha culminado. Para este propósito se crea el mapa sombra, el mismo que funciona exactamente igual que el

mapa del sitio, pero no es promocionado a los usuarios y por tanto no es accesible abiertamente por que está protegido con claves de acceso. Puede enlazarse este mapa con las páginas de búsqueda de las administraciones involucradas con el desarrollo del contenido mientras éste se crea.

El mapa de sombra llega hasta los niveles de los autores. El autor contiene una página de índice que contiene dos secciones: trabajo propuesto y trabajo terminado. Cuando el primer borrador del trabajo propuesto se termina, el autor lo coloca en su directorio web y lo enlaza desde su página índice. En la medida que se hagan las revisiones, es su responsabilidad indexar la última versión para que ésta sea referenciada. Cuando termina el proceso de revisión, el autor mueve los archivos revisados a la sección de trabajo terminado, y actualiza los vínculos de su índice a lo que será la dirección permanente de la información desarrollada, elimina cualquier mecanismo de control de acceso temporal que haya sido utilizado, así la página entra en producción.

Está metodología de trabajo es muy importante utilizarla en los grupos de desarrollo de proyectos. Los autores que quieran poner

a consideración su trabajo para que sea revisado, pueden utilizar un mapa similar notificando al administrador del proyecto y al resto del grupo para que su desarrollo sea revisado, aprobado y puesto en producción.

Existe otra aplicación útil a este mecanismo, son las matrices organizacionales las que pueden ser creadas por los administradores funcionales. Consisten de vínculos a las páginas índice de cada funcionario que debe reportar al administrador funcional. Así se crea una forma rápida de trabajar, reportando tanto el trabajo terminado como los progresos de lo pendiente. Una vez que se crea la infraestructura y la cultura, este método requiere un esfuerzo mínimo manteniendo los reportes actualizados, y, una comunicación y coordinación permanente.

Finalmente, las páginas de revisión se pueden crear cuando el contenido está listo para una revisión final. Cada página de este tipo consiste de una serie de vínculos al contenido que está en la cola de revisión final. Cuando un editor pone su trabajo formalmente en su sección de terminado, éste se vincula automáticamente a las páginas de revisión. Los encargados del proceso de revisión, acceden estas páginas y se encargan de

revisar, y, aprobar o rechazar el contenido en una manera ágil y rápida siguiendo los vínculos. Se provee un mecanismo de comentarios por parte del autor para considerar las sugerencias. La tecnología de Intranet podría incluso proporcionar grupos de discusión para este proceso.

4.2.4 Búsqueda General

La búsqueda es la principal forma que permite a los usuarios encontrar la información en el Intranet. Un agente de búsqueda tiene algunas funciones: provee a los usuarios información en el contexto de un proceso específico, provee una infraestructura eficiente y consistente. Puede verificar duplicación de información y poner en contacto a los autores para coordinar esfuerzos, y ayudar a considerar que información debe ser considerada formal.

En las organizaciones se generan páginas de agentes informales. Un autor tan solo la crea con vínculos a cierta información que para sus propósitos es relevante. Estas páginas pueden ser valiosas para determinar nuevos requerimientos.

Otro tipo común de página de búsqueda que se encuentra en la Intranet son las páginas de revisión. Tienen vínculos apuntando a

las páginas que los creadores han sometido al proceso de revisión por parte de los editores y publicadores.

4.2.5 El Directorio de Búsqueda

El directorio de búsqueda de la organización, a veces conocido como "páginas amarillas", organiza el contenido por tópicos, y ayudan a los usuarios a encontrar lo que necesitan. Generalmente es administrado por el Administrador del Web o el Webmaster principal. A veces incluye las páginas informales. Se debe buscar un mecanismo de control de estas páginas informales, puede ser algún mecanismo de suscripción vía formulario o e-mail al Administrador del Web, el mismo que puede autorizar la publicación por un periodo determinado. Lo importante es controlar que este directorio no se convierta en un repositorio de vínculos a páginas abandonadas, cuyo autor no actualiza ni revisa el contenido.

4.2.6 El Índice de la Organización

Este índice provee a los usuarios otra forma de encontrar información. Normalmente es generado por una máquina de búsqueda. Manteniendo el modelo de toma de decisiones

distribuidas, la máquina de búsqueda no debe buscar en páginas publicadas en sistemas específicos o administrados por algún software en especial. La máquina de búsqueda y el generador de índice deben basarse en agentes descubridores (Web Crawlers o Spiders) que frecuentemente exploran el Intranet y catalogan su contenido. Esto es consistente con la coordinación versus el modelo de control, y protege a la organización del uso de tecnología con candados propietarios.

La figura No. 4-4, muestra la estructura final de la arquitectura lógica de la información en una Intranet. Estos son los elementos finales que junto con el marco de trabajo, conforman la infraestructura organizacional y administrativa necesaria para garantizar que una Intranet cumpla con la funcionalidad de ser una base de conocimientos organizacionales o corporativos distribuida. Estos son los procesos y la gente, que junto con la infraestructura tecnológica, constituyen una Intranet funcional.

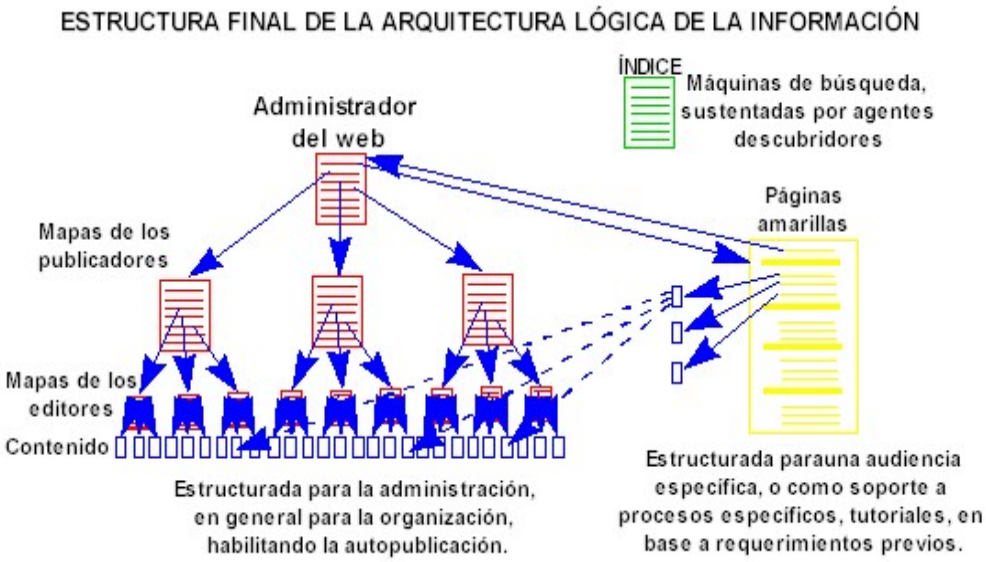


FIGURA 4.4. ESTRUCTURA FINAL DE LA ARQUITECTURA LÓGICA DE LA INFORMACIÓN

4.3 Desarrollo de Aplicaciones Centradas en el Web

La mayoría de aplicaciones de software, pueden caracterizarse por tener tres elementos distintos: Un elemento de interfaz de usuario, que interactúa con él mostrándole información y respondiendo a los eventos generados por él; un elemento de procesamiento de la información o lógica de negocio, que efectúa operaciones sobre los datos de la aplicación basado en los procesos ejecutados por el usuario; y el elemento de almacenamiento de datos que recupera, almacena y

administra los datos generados y utilizados por los otros dos elementos. [26].

Como ya se explicó anteriormente, existe actualmente una necesidad de descentralizar la toma de decisiones y enfocar los procesos de negocios y operaciones en un ambiente de comunicación y coordinación centralizada; por lo que las áreas de desarrollo de sistemas deben enfocarse ahora en el desarrollo de un nuevo tipo de aplicación conocido como: aplicaciones centradas en la red [27]. Una aplicación centrada en red utiliza tecnología independiente de plataforma y los estándares abiertos del Internet, para correr en cualquier plataforma de hardware y software que soporten estos estándares, evitando así el acoplamiento a un tipo de hardware y sistema operativo específico. Adicionalmente, se enmarcan en el esquema de desarrollo de aplicaciones distribuidas, las que permiten entre otras cosas, hacer un uso más eficiente de los recursos de hardware disponibles.

La ventaja de desarrollar aplicaciones centradas en red, es que permiten mantener un ambiente abierto de servicios provistos a través de la Intranet institucional; lo que permite a los departamentos de

sistemas, desarrollar, implementar y administrar un sinnúmero de aplicaciones que [27] :

- ✓ Se crean una sola vez y corren en cualquier sistema;
- ✓ Son fáciles de desarrollar;
- ✓ Son escalables desde las redes de área local hasta el Internet;
- ✓ Están basadas en estándares abiertos para garantizar la compatibilidad y la interoperatividad;
- ✓ Permiten una integración con la tecnología actual basada en bases de datos;
- ✓ Son colecciones de componentes basados en tecnología orientada a objetos, altamente reutilizables.

El rango de soluciones puede abarcar desde aplicaciones centradas en información como repositorios de conocimiento corporativo, hasta aplicaciones centradas en líneas de negocios, como: comercio electrónico, automatización de procesos y administración de inventarios.

4.3.1 Evolución hacia la Arquitectura Centrada en el Web

En la década de los años 80, las aplicaciones eran independientes y monolíticas; es decir los tres elementos básicos de la aplicación: interfaz de usuario, la lógica de negocio, y, los datos, estaban mezclados en un solo código. Se diseñaban para correr en un equipo de escritorio o en un servidor, pero su interacción con otras aplicaciones era nula, eran soluciones estáticas e inflexibles. Dentro de las ventajas que tuvo este modelo tenemos la facilidad y rapidez de desarrollo; sin embargo sus desventajas fueron la difícil identificación de donde hacer los cambios, los problemas de rendimiento al no ser escalables, y su difícil reutilización. En la Figura 4-5 se muestra un diagrama conceptual de estas aplicaciones [28]:

FIGURA 4.5. APLICACIONES MONOLÍTICAS DE LOS AÑOS 80

Luego en los años 90 emerge el modelo de arquitectura de software cliente-servidor clásico, en base al cual se diseñaron aplicaciones que enlazaban inteligentemente a clientes y servidores para proveer en conjunto una solución más completa. Las ventajas que proveía éste modelo es que los datos estaban almacenados en un solo servidor, lo que evita la duplicidad y facilita la escalabilidad en actualizaciones de hardware de dicho servidor. Sin embargo entre las desventajas tenemos que es muy difícil de instalar y por tanto costoso de actualizar; la parte cliente tiende a ser monolítica y muy dependiente de la estructura de los datos, la lógica del lado del cliente normalmente incluía demasiadas reglas del negocio por lo que su administración y mantenimiento tenía un costo adicional oculto normalmente no contemplado (cliente gordo); el flujo de información entre el cliente y el servidor era transmitido usualmente utilizando un protocolo propietario. Además consume demasiado ancho de banda de la red porque viajan demasiados datos al cliente lo que no la hace viable para instalaciones grandes con algunos cientos de usuarios geográficamente dispersos; el modelo era demasiado rígido, con un alto costo de tenencia. En la Figura 4-6 se muestra un diagrama conceptual de estas aplicaciones [28].

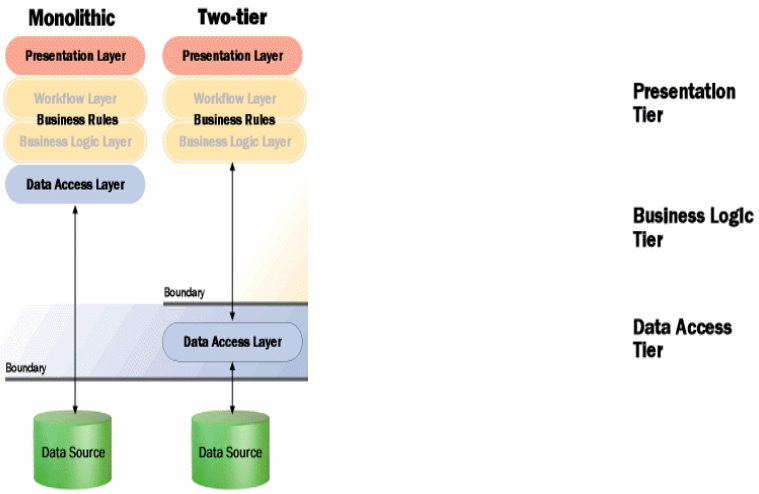


FIGURA 4.6. APLICACIONES CLIENTE – SERVIDOR CLÁSICO DE INICIOS DE LOS AÑOS 90

A mediados de los años 90, en la medida en que el comportamiento organizacional se ve altamente influido por procesos de mejoramiento continuo, reingeniería de procesos y trabajo cooperativo, surgió la necesidad de contar con un ambiente más flexible y abierto que pueda satisfacer estas nuevas demandas en soluciones informáticas. Las nuevas aplicaciones deben ser capaces de correr en una variedad de diferente tipo de hardware y sistemas operativos, contar con un medio de distribución ágil que facilite la administración de soluciones en una infraestructura altamente descentralizada, que cubra

supercomputadores, servidores departamentales, equipos de escritorio y equipos portátiles, así como también equipos de la próxima generación, como las computadoras de red o dispositivos móviles de mano (Ejemplo: Teléfonos celulares, PDAs, Pocket PCs). La necesidad de integración e interoperatividad demanda además un apego a los estándares abiertos y públicos. Estas nuevas aplicaciones deberán [27]:

- ✓ Ser independientes de plataforma para permitir ser creadas una vez y correr en cualquier sistema, sean máquinas clientes o máquinas servidores, en lugar de requerir una recompilación del código dependiendo de la plataforma destino en la que será utilizada.
- ✓ Correr en clientes y servidores sin necesidad de recompilar, lo que permitirá una partición universal de la aplicación.
- ✓ Tener un bajo costo de implementación y tenencia, facilitando el desarrollo de habilidades ya determinadas.
- ✓ Utilizar estándares abiertos que sean lo suficientemente flexibles para integrarse con otras aplicaciones desarrolladas al momento o por desarrollarse en el futuro.

- ✓ Utilizar la inversión existente en infraestructura de computadores de escritorio, servidores, supercomputadores, bases de datos y redes.
- ✓ Ser escalables de ser necesario desde las redes de área local hasta el Internet.
- ✓ Ser desarrolladas y administradas centralizadamente desde los servidores, evitando el gasto de las actualizaciones estáticas de nuevas versiones, en los computadores de escritorio y móviles individuales.
- ✓ Soportar la reutilización de componentes, aumentando la habilidad de desarrollar nuevas aplicaciones en forma rápida a partir de los servicios actuales.

A finales de los noventa, entrando el nuevo siglo, fenómenos organizacionales como la globalización que ocasionan niveles de competitividad en escalas mucho mayores a las acostumbradas, ocasionan un sinnúmero de cambios que a la larga generan una reacción de la tecnología para poder responder de la manera más eficiente posible, puesto que a su vez la economía es actualmente muy dependiente de la tecnología de información. En la Tabla V presentamos una comparación de las estructuras organizacionales

y las características preponderantes del entorno empresarial, a fines de los 80 y fines de los 90 [28]:

TABLA V

COMPARACIÓN DE ESTRUCTURAS Y ENTORNOS

Finales de los 80	Finales de los 90
Mercados estables	Mercados competitivos
Metas internas	Metas orientadas a los clientes
Estructura organizacional fija	Estructura organizacional flexible
Implementación de software por aplicación funcional	Ingeniería de negocio orientada por procesos
Estructura funcional	Estructura orientada por procesos

Pero, ¿Cuáles son los cambios en un mundo distribuido?

TABLA VI

CAMBIOS EN UN MUNDO DISTRIBUIDO

ANTES	HOY
# Usuarios = # Empleados	Usuarios = Clientes, Proveedores, Socios, Empleados (Internet, Extranet, Intranet)
Conexiones con líneas dedicadas	Conexiones ocasionales en demanda
Datos alfanuméricos	Datos multimedia
Desarrollo en serie	Desarrollo iterativo

Estos cambios, imponen una nueva presión sobre las áreas de desarrollo de sistemas de información, cuyos retos son:

TABLA VII

NUEVOS RETOS PARA TECNOLOGÍA DE INFORMACIÓN.

ANTES	HOY
Actualizaciones anuales.	Implantación Justo a Tiempo.
Disponibilidad 7x24, de vez en cuando.	Disponibilidad permanente 7x24.
Los usuarios eran entrenados y por tanto expertos.	Los usuarios son comunes, sin entrenamiento.

Estos nuevos requerimientos están ocasionando que las Intranets corporativas, pasen a ser de un medio abierto para compartir información, a una plataforma de desarrollo de aplicaciones; transformando el proceso de diseño y desarrollo de aplicaciones, desde la arquitectura centrada en el servidor, hacia aplicaciones distribuidas orientadas a la red de “3 capas”. Dentro de las principales ventajas que brinda éste modelo, tenemos:

- ✓ La lógica del negocio puede ser centralizada y estar basada en componentes.
- ✓ Facilita el mantenimiento y la instalación, lo que representa menor costo de tenencia.

- ✓ Se puede mejorar la disponibilidad y el desempeño, configurando instalaciones con capacidades de balanceo de carga, distribuyendo tanto la capa del negocio, como la capa de datos en varios servidores físicos.
- ✓ Se puede emplear bien sea distintos lenguajes de programación, escogiendo los más adecuados para cada tarea; así como múltiples tecnologías asociadas a un mismo lenguaje de programación (Java 2 Enterprise Edition).
- ✓ Las bases de datos no están expuestas directamente a los clientes, sino a los componentes; creando un ambiente más seguro y haciendo un uso más eficiente de los recursos (manejo de arreglos de conexiones a la base de datos).

Pese a todo lo mencionado, éste modelo presenta también algunas desventajas:

- ✓ Hay que definir la separación lógica (como se dividen las funciones) y la separación física (donde corren las funciones); lo que demanda un mejor diseño arquitectónico de la solución, con niveles de conocimiento más especializados.

- ✓ Se demanda un manejo transaccional para las operaciones muy concurrentes.

En la Figura 4-7 se muestra un diagrama conceptual de estas aplicaciones [28]:

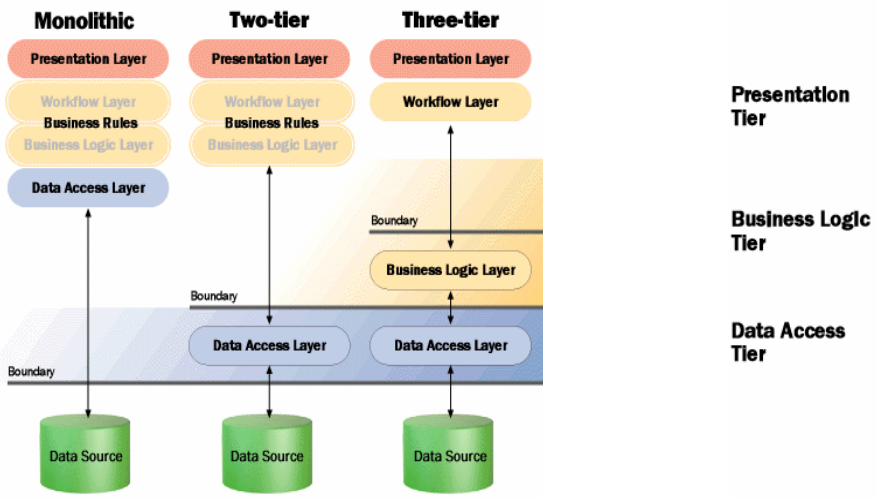


FIGURA 4.7. APLICACIONES DE TRES CAPAS DE FINALES DE LOS AÑOS 90

El modelo conceptual de tres capas ha sido depurado buscando una mayor especialización y un bajo acoplamiento entre las distintas lógicas, en la medida que han surgido estándares que permitan obtener una especificación de arquitectura lo suficientemente completa para satisfacer los requerimientos de la nueva era de la información. Hoy en día hablamos de un modelo

de “n capas”, cuyas ventajas a más de las incluidas en el modelo de tres capas son las siguientes:

- ✓ La lógica del interfaz de usuario es pura interfaz. Su principal preocupación es la usabilidad adaptada a los múltiples formatos y dispositivos de visualización de hoy en día. Su función se limita a simples validaciones de entrada.
- ✓ La lógica de negocios está distribuida en varios servicios combinados, todos basados en una arquitectura de componentes empresariales distribuidos. Estos componentes encapsulan los objetos del negocio y sus procesos.
- ✓ La lógica de acceso a los datos, está dividida por tipo de operación (consultas o procesos), y dividida por diferentes tipos de bases de datos (motores de cualquier fabricante).

Técnicamente, este concepto está definido como una arquitectura basado en servicios. El modelo propuesto fruto de esta evolución se muestra en la Figura 4-8 [28]:

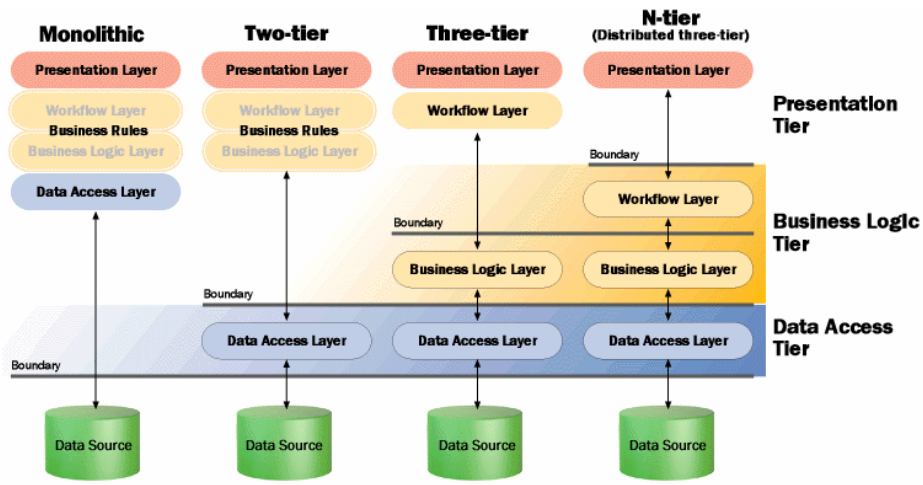


FIGURA 4.8. APLICACIONES DE "N" CAPAS

Las aplicaciones centradas en red son construidas siguiendo una arquitectura generalmente propuesta y aceptada por la industria, o una gran parte de ella; es decir utilizando el modelo de arquitectura Java 2 Enterprise Edition, o Microsoft .Net, según sea preferencia de la Institución.

Sin embargo, la independencia de plataforma de las aplicaciones centradas en red significan más que reducir costos en el desarrollo y mantenimiento de aplicaciones. Es una propiedad fundamental del desarrollo de aplicaciones de arquitectura centrada en red. Una lección clave que nos deja el Internet, es que la mayoría de aplicaciones corporativas van eventualmente a comunicarse con servicios del Intra/Internet, y no solo con servicios detrás del

cortafuegos o firewall de la red corporativa. Esto significa que aún cuando se puede desarrollar aplicaciones centradas en red dependientes de plataforma o propietarias, sería como confiar la telefonía corporativa a un solo tipo particular de tecnología telefónica propietaria y no pública, útil puertas adentro, pero inútil para comunicarse con el mundo.

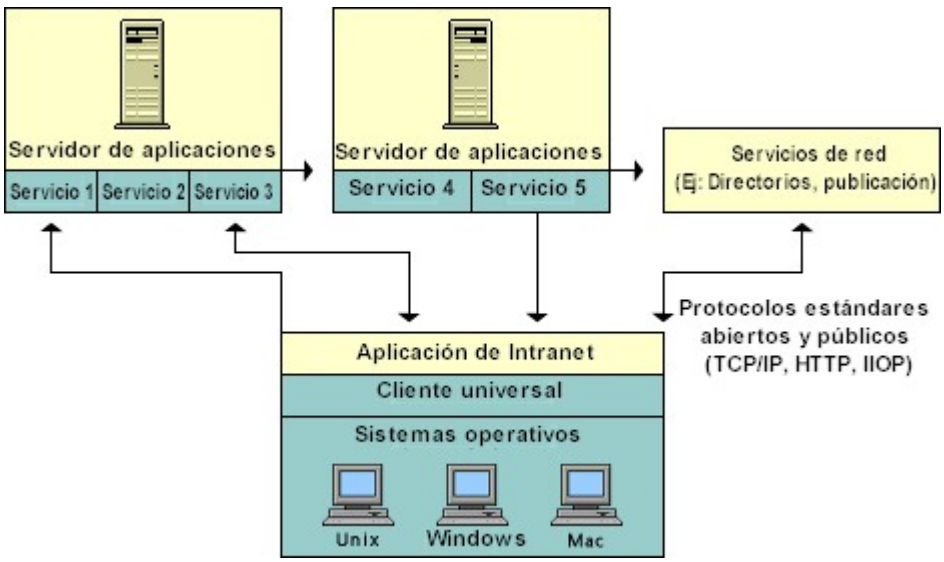


FIGURA 4.9. ARQUITECTURA CENTRADA EN RED DE UNA APLICACIÓN TÍPICA DE UNA INTRANET

En la Figura No. 4-9 se describe la arquitectura centrada en red de una aplicación típica de una Intranet. Cuando hay un requerimiento de un usuario, la parte cliente de la aplicación que

es independiente de plataforma, se descarga desde un servidor de aplicaciones y se ejecuta en un navegador web, habilitado para Java. El cliente luego utiliza los protocolos estándares de Internet para interactuar con la parte de la aplicación del lado del servidor, así como con cualquier servicio estándar del Inter/Intranet.

En una organización tan grande como la Armada, se debe insistir en este tipo de aplicaciones para poder integrar verdaderamente a todos los repartos, en organizaciones más comunicativas, colaborativas y cooperativas.

En el mercado existen ya muchos producto basados en esquemas o marcos de referencia que han adoptado la apertura y la innovación en reemplazo de estrategias basadas en candados propietarios. Cualquiera de estos enfoques es recomendable emplear como base del desarrollo de aplicaciones para la Intranet siempre y cuando se apegue a los estándares públicos, entre los que podemos nombrar los siguientes:

- ✓ La arquitectura abierta de SUN Microsystems, creada inicialmente por Netscape Communications, “Open Network Environment, ONE”.

- ✓ La arquitectura distribuida de Microsoft, “Microsoft .Net”.
- ✓ La arquitectura de red de Oracle, “Oracle Network Computing Architecture”.
- ✓ El marco de referencia para aplicaciones e-business de IBM.

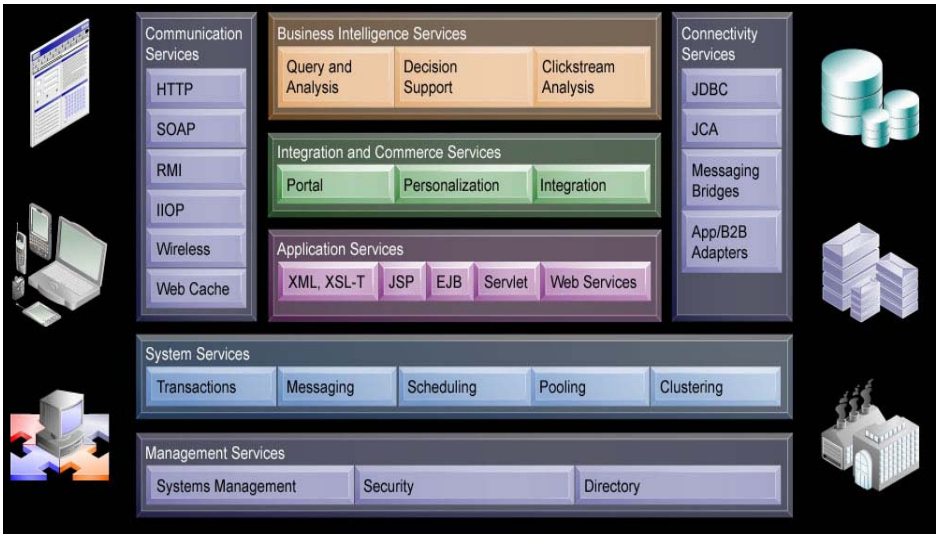


FIGURA 4.10. ORACLE NETWORK COMPUTING ARCHITECTURE [29]

Lo importante de estos marcos de referencia o esquemas es que permitan el desarrollo ágil, robusto, flexible y reutilizable de aplicaciones dinámicas e independientes de plataforma para el Inter/Intranet, con excepción de la arquitectura Microsoft .Net, que solo corre sobre el Sistema Operativo Windows. La Figura 4.10, describe la arquitectura Network Computing de Oracle.

4.3.2 Java y el Ambiente de Aplicaciones Distribuidas

Habíamos dicho anteriormente, que toda aplicación tiene en términos generales tres elementos: Interfaz de usuario, lógica del negocio y datos. Aún cuando estos elementos podrían estar ubicados en la misma computadora, hemos visto que existe una clara tendencia a separarlos en más de un computador de modo que exista más modularidad y eficiencia en el uso de los recursos de procesamiento. Las aplicaciones distribuidas están basadas en ésta premisa.

Un sistema distribuido divide una aplicación en distintos módulos independientes. El fallo de uno de éstos módulos tiene menos impacto en el sistema completo, lo que lo hace más disponible, escalable y mantenible. Los sistemas distribuidos tienen módulos pequeños, ágiles y adaptables; a diferencia de los sistemas monolíticos que son grandes, inflexibles y de difícil adaptabilidad.

Un ejemplo claro de esto son las aplicaciones desarrolladas para el ambiente web: El navegador web implementa la interfaz del usuario, mostrando la información y respondiendo a los eventos generados por las acciones del usuario con el ratón y el teclado.

Dependiendo de las características y el ancho de banda disponible en la red, ésta interfaz puede estar desarrollada con un enfoque centrado en el servidor, o un enfoque centrado en el cliente. Si el ancho de banda de la red es un recurso limitado, por ejemplo: Internet, se desarrolla un interfaz liviana basada generalmente en formularios HTML; pero si se dispone de mayor capacidad de ancho de banda, se puede mejorar las características del interfaz, proveyendo elementos gráficos más avanzados e interactivos, generalmente implementados con Java applets. Los elementos del interfaz realizan un procesamiento liviano normalmente limitado a proveer la estructura de navegación de la aplicación y la validación de datos ingresados.

Las aplicaciones web dividen la lógica del negocio en clases que se ejecutan en uno o más servidores, bien sea a través de Java Servlets, programas independientes tipo CGI, u otros esquemas más sofisticados que serán tratados más adelante. Lo importante a resaltar es que el procesamiento de la lógica y la información se realiza en otro equipo: **el servidor de aplicaciones**. Finalmente, los datos que deban ser recordados, es decir que sean persistentes, son almacenados y administrados por otro equipo en

un Sistema de Administración de Bases de Datos Relacionales, RDBMS. En términos generales podemos mostrar en la Figura No. 4.11 un diagrama esquemático de una aplicación distribuida:

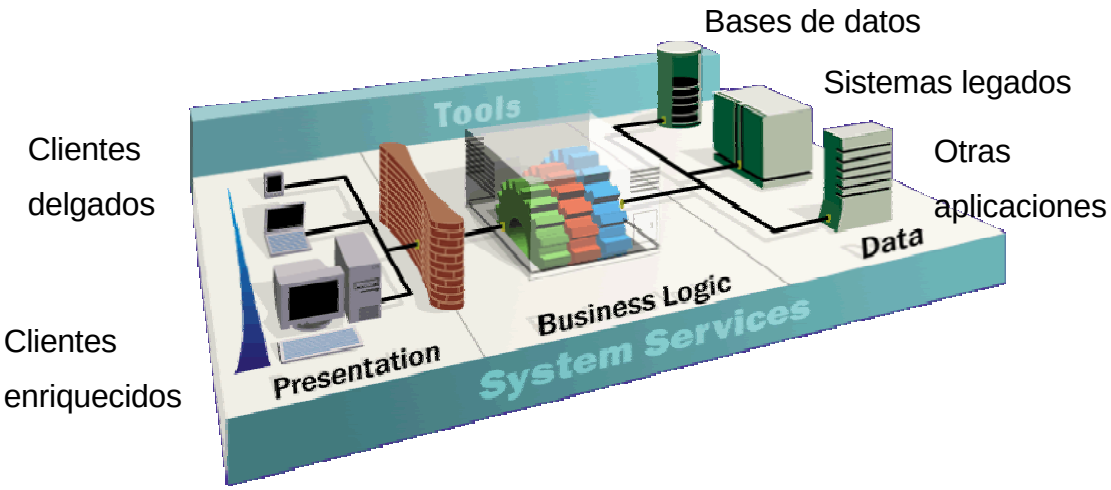


FIGURA 4.11. ESQUEMÁTICO DE UNA ARQUITECTURA DISTRIBUIDA [28]

Java es un lenguaje de programación orientado a objetos creado por SUN Microsystems, basado en las características de C++, pero proveyéndole determinadas capacidades que se debieron a su propósito original de ser empleado en artefactos electrónicos, que le permiten ser de plataforma neutra, por tanto portable. Esta característica más adelante lo hicieron ideal para el desarrollo de pequeñas aplicaciones para el World Wide Web, convirtiéndolo en un estándar de facto para su uso en el Internet. En éste punto es

oportuno nombrar algunas de las características esenciales de Java y como su esquema de operación le permite conseguir la independencia de plataforma.

Las principales características de Java son [30]:

- ✓ Relativamente simple.
- ✓ Orientado a objetos.
- ✓ Distribuido.
- ✓ Robusto.
- ✓ De arquitectura neutra.
- ✓ Seguro.
- ✓ Portable.
- ✓ Interpretado de alto desempeño.
- ✓ Multithreading.

No se pretende descubrir el porque de cada una de estas características, sino más bien cual es el enfoque de la operación de Java para garantizar el cumplimiento de estas características.

La figura No. 4.12 muestra la estructura del ambiente de desarrollo y ejecución de aplicaciones desarrolladas en Java.

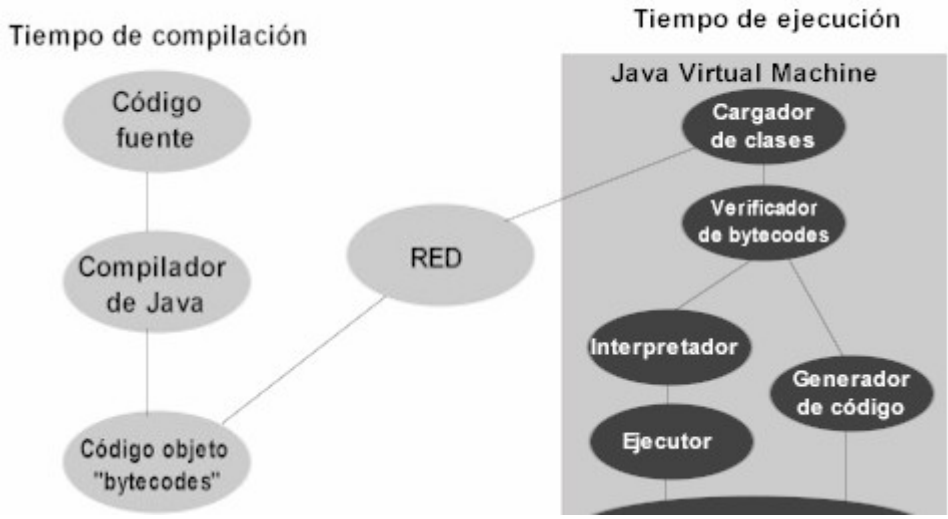


FIGURA 4.12. ESTRUCTURA DEL AMBIENTE DE DESARROLLO Y EJECUCIÓN EN JAVA

Para que Java forme parte integral de las redes de computadoras, el compilador de Java obtiene un código objeto independiente de plataforma, en archivos que contienen los bytecodes de Java. Así, cualquier computador que tenga en su sistema una máquina virtual de Java, sea esta de cualquier plataforma, puede interpretar y ejecutar este código objeto.

Los bytecodes están diseñados para ejecutarse en una máquina hipotética, Java Virtual Machine (JVM); la que es específica de cada plataforma de hardware; ésta máquina virtual interpreta los bytecodes de acuerdo a las especificaciones de cada plataforma, consiguiéndose así la independencia de plataforma. La máquina virtual carga las clases que obtiene a través de una referencia a un archivo con los bytecodes en el caso de un applet, o a través de la ejecución del interpretador para una aplicación stand-alone, lo que le da la capacidad de ser distribuido y portable. El verificador de bytecodes revisa cada una de las instrucciones asegurándose de que éstas no sean dañinas, ni violen los esquemas de seguridad de modo que garantice la integridad y seguridad del código distribuido a ser ejecutado.

4.3.3 Arquitecturas Distribuidas (CORBA – RMI)

1. ¿Qué son los objetos distribuidos?

En términos simples, la tecnología de objetos distribuidos permite a objetos cargados en memoria principal (RAM) de diferentes máquinas en la red, enviarse mensajes entre sí de modo que en conjunto colaboren proveyendo una funcionalidad prevista.

2. CORBA

Common Object Request Broker Arquitecture, es el primer estándar para el desarrollo de aplicaciones distribuidas. Es una especificación de arquitectura de software desarrollada por el grupo de administración de objetos, Object Managment Group (OMG), que permite el desarrollo de sistemas distribuidos habilitando la comunicación de objetos cargados en memoria de diferentes máquinas sin importar el hardware, sistema operativo o lenguaje de programación en que estos objetos corren o fueron implementados.

Cada implementación de la especificación de CORBA define un agente de pedido de objetos, Object Request Broker (ORB), el que es responsable de conectar a la aplicación cliente con los objetos que ella desea utilizar. Así la aplicación cliente no tiene que conocer donde estos objetos residen, sea en la máquina local o en una máquina remota en la red. Lo único que tiene que conocer la aplicación cliente, es el nombre del objeto que tiene los servicios que desea utilizar y la interfaz para utilizar estos servicios; el ORB se encarga de encontrar el objeto, enrutar el pedido y retornar los resultados.

La independencia de plataforma de CORBA permite utilizar a los objetos en la plataforma que más sentido tenga de acuerdo a la funcionalidad del objeto. La independencia del lenguaje de implementación permite integrar los sistemas legados y explotar las habilidades y conocimientos existentes de los programadores en diversos entornos de desarrollo.

Tal como se describe en la figura No. 4.13, los componentes del modelo de arquitectura definida por CORBA, son [31]:

- ✓ El agente de pedidos a objetos (ORB), quien es el responsable del enrutamiento transparente de pedidos a los objetos distribuidos.
- ✓ Los servicios de CORBA, son servicios de propósito general que pueden ser utilizados por cualquier aplicación. Son la base de la interoperatividad.
- ✓ Los recursos de CORBA, que son de uso común y aplicables a la gran mayoría de dominios de aplicaciones. Estas capacidades son comúnmente referenciadas como horizontales, por lo que son útiles resolviendo un amplio rango de requerimientos de negocios.

- ✓ Dominios de CORBA, son servicios que han sido generalizados y son útiles en un mercado específico vertical, como: las telecomunicaciones, finanzas, etc.
- ✓ Objetos de la aplicación, software especialmente diseñado para resolver requerimientos particulares del dominio del problema. Estos utilizan los servicios, facilidades y dominios a través del ORB según sea necesario.

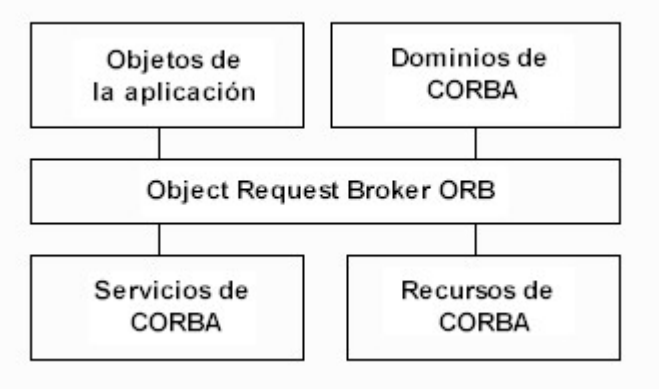


FIGURA 4.13. COMPONENTES DE LA ARQUITECTURA CORBA

Se han definido varios servicios de la especificación CORBA resumidos en cuatro categorías, tal como se muestra en la tabla No. VIII [31]. La categoría de infraestructura incluye servicios relacionados con las funciones del ORB. La categoría de

administración de la información incluye: procesamiento de datos, almacenamiento y recuperación. En la administración de tareas se incluye: manejo de eventos y transacciones. En la administración del sistema se incluye: la administración del ciclo de vida de los objetos, metadatos y licencias.

TABLA VIII

CATEGORÍAS DE LOS SERVICIOS DE CORBA

CATEGORÍA	DESCRIPCIÓN	SERVICIOS CORBA
Infraestructura	Servicios relacionados con los mecanismos del ORB.	Seguridad, temporización.
Administración de Información	Servicios con capacidades básicas para recuperar y manipular datos.	Objetos persistentes, externalización, propiedades, relaciones, consultas, colecciones.
Administración de Tareas	Servicios para la administración de eventos y transacciones de objetos distribuidos.	Eventos, transacciones, concurrencia.
Administración del Sistema	Servicios para la administración de metadatos, licencias y ciclo de vida de los objetos.	Nombramiento, negociación, ciclo de vida y licenciamiento.

Además de las piezas que conforman CORBA, se debe mencionar el lenguaje de definición de interfaces, Interface Definition Language (IDL) y el protocolo Internet Inter-ORB (IIOP).

IDL, es una notación universal para interfaces de software a manera de API's. IDL no se utiliza como lenguaje independiente para la implementación, sino que lenguajes como: C++, Ada, Java, Smalltalk, incluyen herramientas para generación de interfaces IDL. Un apego a IDL no solo consigue la portabilidad y la independencia de plataforma, sino además la independencia del lenguaje de implementación entre objetos clientes y objetos servidores.

IIOP, es el protocolo de comunicación entre ORB's (Internet Inter-ORB Protocol).

En general, la penetración y difusión de CORBA ha sido característica de organizaciones más maduras con altos niveles de implementación de software previo a la difusión del World Wide Web. Si se cuenta con sistemas legados escritos en un lenguaje de programación distinto a Java, con software comercial implementado en otros lenguajes que no soporten esquemas de interconexión como Java Connector Architecture (JCA), o sistemas implementados en un lenguaje de programación específico para el dominio del problema, como Ada en los

sistemas de defensa, y se requiera su integración en sistemas de información distribuidos, CORBA es la opción a utilizar.

Para la mayoría de propósitos fuera de ésta situación, la especificación de la relativamente nueva arquitectura de sistemas distribuidos de alcance empresarial, Java 2 Enterprise Edition, representará la mejor alternativa.

3. REMOTE METHOD INVOCATION (RMI)

La invocación remota de métodos, Remote Method Invocation (RMI) de Java, permite generar un ambiente de aplicaciones Java distribuido en el que existen aplicaciones clientes y aplicaciones servidoras. Un servidor crea un grupo de objetos remotos, crea referencias a estos objetos para que sean remotamente accesibles, y queda en espera de que los clientes invoquen los métodos o servicios que estos objetos pueden ofrecer. Una aplicación cliente típica, consigue las referencias a uno o más objetos remotos del servidor, para luego invocar sus métodos en caso de requerir sus servicios. RMI provee los mecanismos a través de los cuales el servidor y los clientes se comunican enviando información de ida y vuelta. Esta de alguna forma, viene

a ser también una aplicación distribuida pero no de neutralidad con respecto al lenguaje, puesto que su implementación se hace únicamente en Java.

RMI es el mecanismo de bajo nivel desarrollado que sirve de base para la especificación de la arquitectura Java 2 Enterprise Edition.

4.3.4 MVC (Patrón de Diseño)

Basado en el modelo inicial de programación para SmallTalk desarrollado por el centro de investigación de Xerox, PARC alrededor de los años 70, el paradigma o patrón de diseño MVC (Model – Control – View) es una herramienta de enorme utilidad empleada como abstracción del más alto nivel para el diseño de la arquitectura de las aplicaciones web. Permite crear programas que sean fáciles de mantener, y a pesar que demanda mayor esfuerzo inicial en la planificación y codificación, los beneficios en el mediano plazo son superiores.

La idea básica es dividir a la aplicación en tres partes distintas, con la condición de que cada una de las cuales puede ser reemplazada sin afectar a las otras:

El **Model** – que son los datos de la aplicación, junto con la lógica de negocio que define como cambiar y acceder a éstos datos. El Model puede ser compartido con un sinnúmero de objetos del View y del Controller. Puede o no puede exponer directamente la lógica de negocio como métodos. Es capaz de generara un evento cuando sus datos han cambiado, lo que permite que todos los Views conectados sean advertidos que ha sucedido un cambio en los datos y que deben actualizar sus presentaciones para que reflejen tal cambio.

El **View** – que son los medios que permiten representar los datos del Model al mundo exterior de la aplicación. Normalmente se implementa como Interface Gráfica de Usuario (GUI), pueden ser tabulares, reportes, gráficas de barras. Generan el diálogo de la aplicación, incluyen tonos sonoros, imprimen, o incluso interactúan con elementos externos al sistema a los que generalmente controlan, como una central de aire acondicionado en un sistema de control automático de temperatura.

El **Controller** – que son los medios que permiten recolectar los eventos del usuario u otro actor del entorno, proveyendo retroalimentación al Model, cambiando normalmente algunos

datos. En términos generales, el Controller, mantiene sincronizados el View y el Model.

En la Figura No. 4.14 se representa gráficamente lo expuesto:

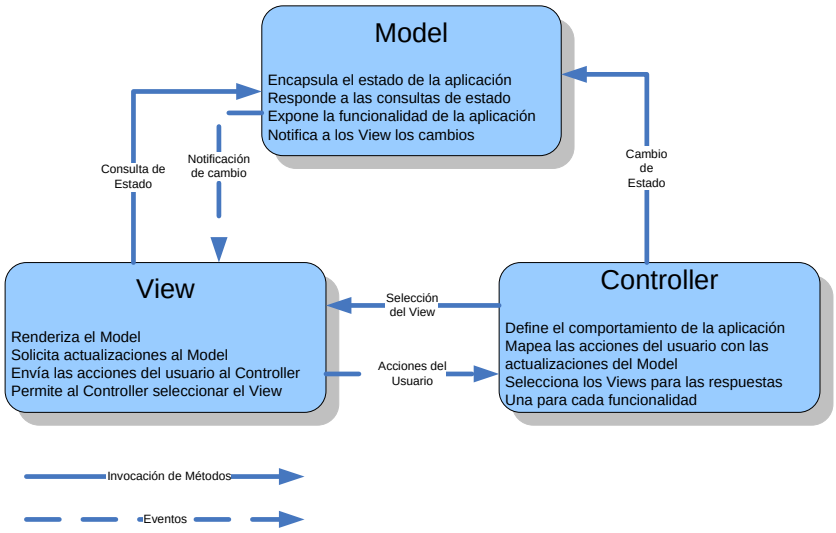


FIGURA 4.14. PRINCIPIO DE DISEÑO MODEL – VIEW – CONTROLLER

1. Interacción entre Componentes

Inicialmente el View, y posiblemente el Controller, piden al Model su estado actual. El View puede presentar los datos al usuario, y el Controller puede verificar los datos para ayudar a decidir como manejar la interacción con el usuario.

Tal como se muestra en la Figura No. 4.15, el View y el Controller estarán pendientes, “escuchando” los cambios en el Model. En Java se implementa esto utilizando eventos. Cada vez que el Model diga que “ha cambiado”, el View y el Controller pueden pedir un nuevo estado de los datos del Model, y luego actualizan la presentación al usuario.

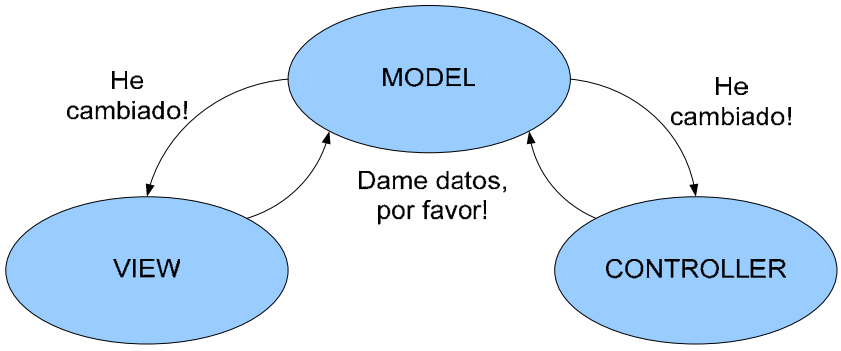


FIGURA 4.15. DIÁLOGO EN EL PATRÓN DE DISEÑO MODEL – VIEW – CONTROLLER

Si el usuario decide interactuar con la aplicación, el Controller se hace cargo. Vigila los ingresos del usuario, tales como los click o movimientos de ratón, o las teclas presionadas en el teclado. El Controller decide lo que éstas interacciones significan, y pide al Model que actualice sus datos y/o al View que cambie la forma de desplegar estos datos. Ver la Figura No. 4.16.

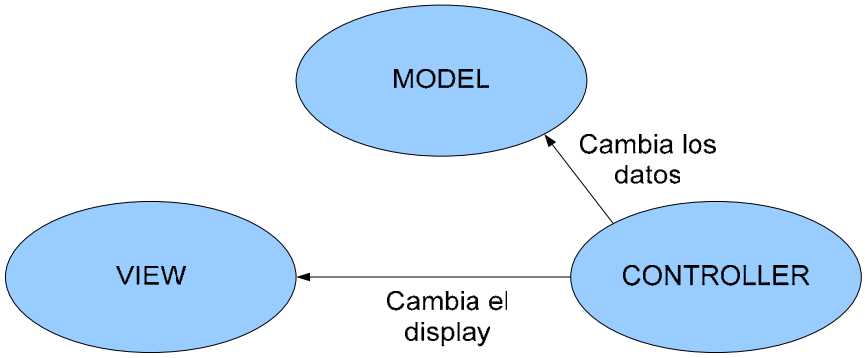


FIGURA 4.16. DIÁLOGO EN EL PATRÓN DE DISEÑO MODEL – VIEW – CONTROLLER

Se pueden tener múltiples Controllers y Views en una misma aplicación, pero solo se puede tener un Model.

Supongamos que se tiene una aplicación que presenta la información de una base de datos en una tabla y en un gráfico de pastel. La tabla puede ser visualizada utilizando controles de barras de desplazamiento verticales y horizontales, y se pueden ingresar nuevos datos a través de un par de cuadros de texto. El patrón MVC puede ser aplicado tal como se muestra en la Figura 4.17:

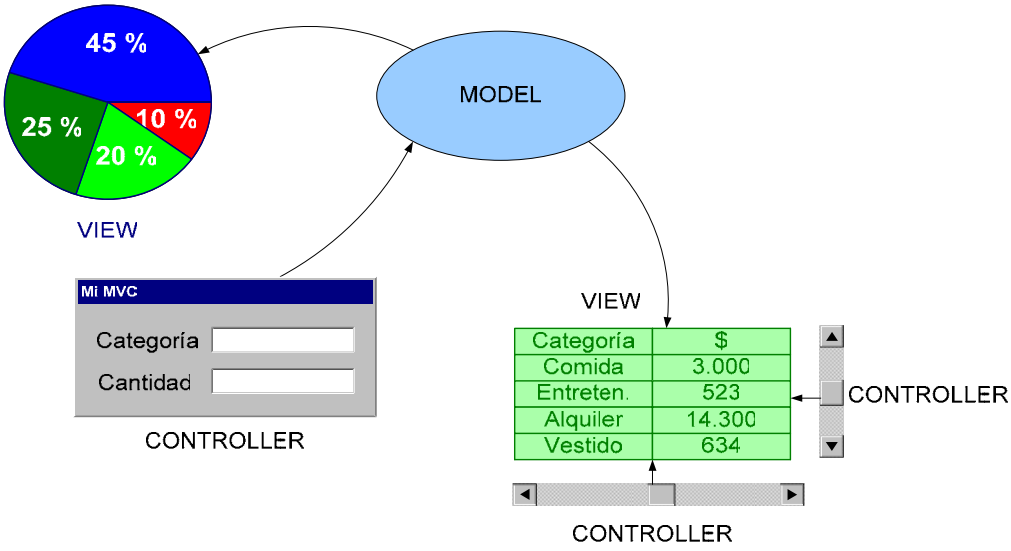


FIGURA 4.17. EJEMPLO DEL PATRÓN DE DISEÑO MODEL – VIEW – CONTROLLER

En éste ejemplo se incluye un Model, dos Views y tres Controllers. Los Controllers de barra de desplazamiento actualizan únicamente el View de la tabla, mientras que el Controller del cuadro de texto actualiza el Model.

Patrón delegación – combinando el View y el Controller

En teoría debe haber una separación entre el View y el Controller, pero en la práctica eso puede ser muy difícil de lograr. Por esta razón el paradigma MVC a menudo se simplifica combinando el View y el Controller. Este patrón de diseño se lo denomina usualmente Delegación.

Así el delegado como un “solo todo”, se comunica con el Model en la misma forma antes descrita. La separación entre el Model y el Delegado, es la clave para el éxito de éste patrón. Aún cuando ésta versión de aplicación del patrón de diseño MVC es algo simplificada, continua siendo básicamente un diseño basado en el patrón MVC original.

Un buen diseño arquitectónico del software centrado en red, como una aplicación web, en el que se aplica al más alto nivel el principio de diseño MVC deberá incluir al menos lo que se muestra como diagrama de bloques en la Figura 4.18:

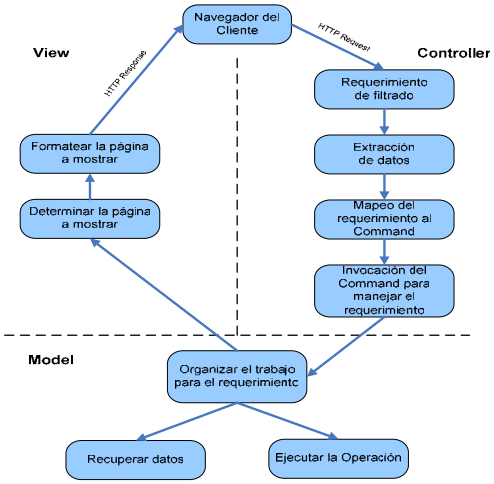
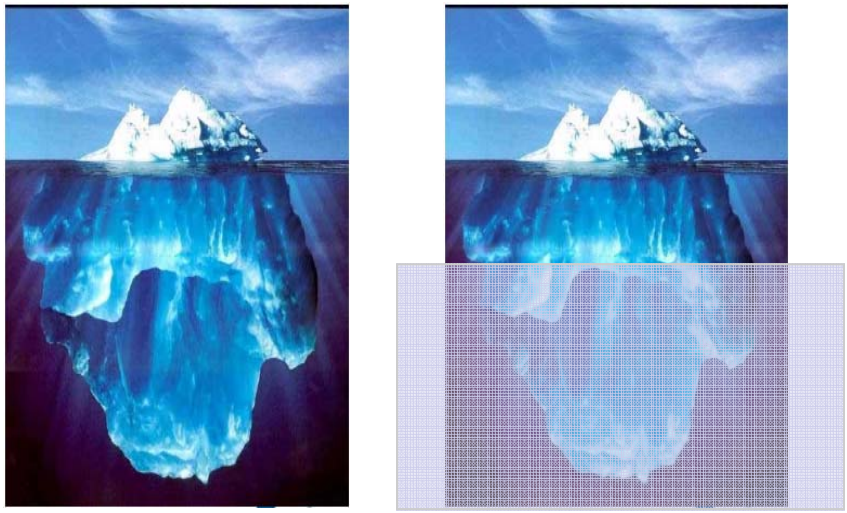


FIGURA 4.18. APLICACIÓN DEL PATRÓN DE DISEÑO MVC A UNA APLICACIÓN WEB

2. Porqué es tan Importante el Patrón MVC

A pesar que lo mencionado parece ser mera teoría, y además demandar bastante trabajo, se debe tener presente que el desarrollo de una aplicación, representa típicamente el 10% de esfuerzo o menos del ciclo de vida de dicha aplicación. Por tanto el mantenimiento de la aplicación, debe ser uno de los aspectos más importantes a tener presente durante el diseño. Un diseño claro y entendible es un gran comienzo, pero para que sea efectivo debe separar la lógica del negocio de la interfaz de usuario. Los sistemas de información están sujetos al cambio siempre; y sino consideramos todo el ciclo de vida del sistema, y la arquitectura del sistema no cuenta con un buen diseño, estaríamos viendo tan solo la punta del iceberg. En la Figura 4.19 se muestra el efecto “Iceberg” en los costos ocultos del mantenimiento del software.



Altos costos de mantenimiento debido a un mal diseño arquitectónico de software

Reducción de costos de mantenimiento debido a un buen diseño arquitectónico de software

FIGURA 4.19. EL EFECTO ICEBERG EN LOS COSTOS OCULTOS DEL MANTENIMIENTO DE SOFTWARE

Solo pensemos algunas de las posibles razones por las cuales un sistema cambia en el tiempo:

- ✓ El estado actual del diseño de las Interfaces Gráficas de Usuario ha evolucionado (algo común en una aplicación web), y se ha decidido actualizar las interfaces. Una simple decisión de actualizar la imagen corporativa o hacer un diseño de interfaces de usuario más fáciles de utilizar.

- ✓ La organización cambió la arquitectura de su red, hay más ancho de banda disponible y se quiere mejorar las aplicaciones que antes tenían limitaciones de ancho de banda.

- ✓ La organización desea poner en producción en el Internet una versión limitada de su aplicación para Intranet.

- ✓ La organización quiere proveer una nueva forma de analizar los datos existentes.

Cambios como éstos, normalmente involucra la revisión del diseño de la Interfaz Gráfica de Usuario, o de la lógica de negocio de la aplicación. Si la Interfaz Gráfica de Usuario y la lógica de negocio, tienen un alto nivel de acoplamiento, hacer tales cambios puede ser muy difícil. Si se utilizó el patrón de diseño MVC durante el diseño original en cambio, estos cambios serán mucho menos costosos, y más que todo, serán cambios aislados que reducirán el riesgo de introducir defectos en código que aparentemente no tiene relación con los cambios hechos directamente.

Utilizando los principios del diseño MVC los cambios antes mencionados son mucho más simples de realizar:

- ✓ La actualización de la Interfaz Gráfica de Usuario requiere cambios únicamente en el código de la GUI. La lógica del negocio no tiene porqué ser tocada.

- ✓ La actualización de la arquitectura de red, quizás cambios en la topología física de la aplicación de dos a tres capas o “n” capas, requerirán modificar únicamente parte del Model. La Interfaz Gráfica de Usuario no tiene porqué ser tocada.

- ✓ La creación de una aplicación limitada para el Internet, será cuestión de subclasificar el Model para bloquear el acceso a algunas características. La Interfaz Gráfica de Usuario no tiene porqué ser tocada.

- ✓ Añadir nuevas formas de analizar los datos es solo cuestión de añadir una nueva View. Normalmente no es necesario realizar cambios al Model, y no es tampoco necesario modificar otros Views.

Otro aspecto muy importante del principio de diseño MVC, es que al separar la lógica de negocio del Interfaz Gráfica del Usuario, permite separar las tareas de codificación. Se pueden conformar grupos de desarrollo más especializados trabajando casi en

paralelo, teniendo desarrolladores especialistas en Interfaces Gráficas de Usuario, y desarrolladores especialistas en lógica de negocio.

4.3.5 Plataforma JAVA 2 Enterprise Edition

Hoy en día las aplicaciones empresariales o corporativas, deben ser capaces de explotar la velocidad, seguridad, capacidad de procesamiento y confiabilidad de la tecnología del lado del servidor. Para ello, la plataforma J2EE provee un enfoque basado en componentes para: diseñar, desarrollar, ensamblar e implantar aplicaciones empresariales. Contempla un modelo de aplicaciones distribuidas basado en múltiples capas, la habilidad de reutilizar componentes, integra a XML para el intercambio de datos, un modelo de seguridad unificado y un control transaccional flexible.

La lógica de la aplicación está dividida en componentes de acuerdo a su función; y estos componentes que hacen la aplicación J2EE están instalados en máquinas distintas de acuerdo a las diferentes capas que la aplicación tenga.

Los componentes de una aplicación J2EE son [32]:

- ✓ Componentes de capa cliente, que se ejecutan en la máquina cliente.
- ✓ Componentes de capa web, que se ejecutan en el servidor J2EE dentro del contenedor web.
- ✓ Componentes de capa de negocio, que se ejecutan en el servidor J2EE dentro del contenedor EJB.
- ✓ Software de la capa de sistemas de información empresariales, que se ejecuta en servidores de sistemas de información empresariales.

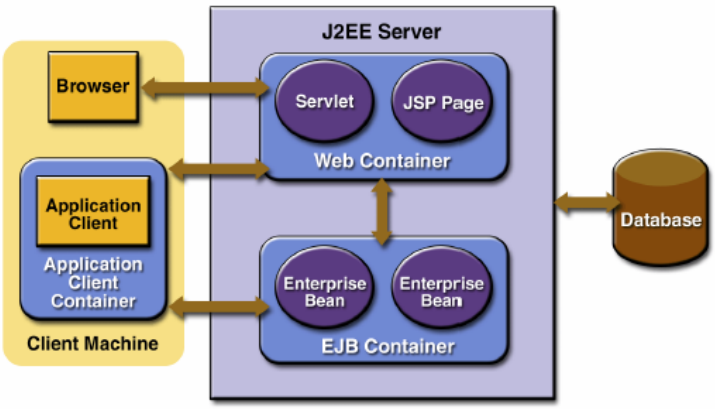


FIGURA 4.20. DIAGRAMA DE BLOQUE DE UNA APLICACIÓN J2EE [32]

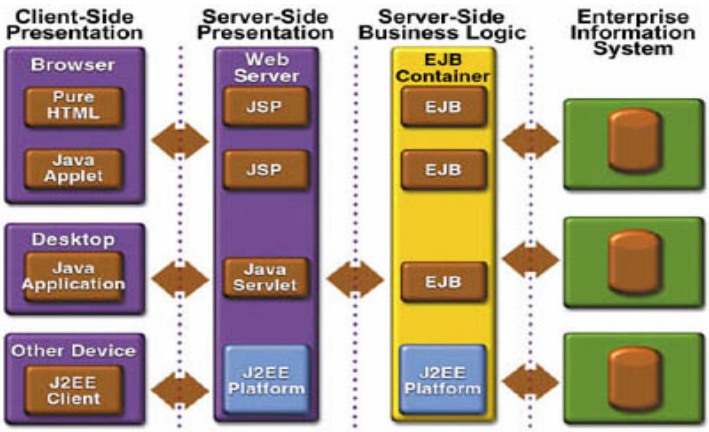


FIGURA. 4.21. MODELO DE APLICACIÓN J2EE

El modelo de aplicación propuesto por la especificación J2EE tiene las siguientes ventajas:

- ✓ Aumenta la modularización del sistema, reduciendo el acoplamiento y favoreciendo a la reutilización de componentes.
- ✓ Se logra una mejor distribución del procesamiento y el paralelismo de tareas, lo que implica un mejor uso de recursos.
- ✓ Se tiene una replicación de servicios más eficiente.

Pero el modelo tiene también las siguientes desventajas:

- ✓ Mayor latencia. (tiempo de respuesta).
- ✓ Mayor complejidad.

Una aplicación J2EE está basada en componentes. Un componente es una unidad de software autocontenida, que es ensamblada dentro de una aplicación J2EE con todas sus clases y archivos relacionados, y que es capaz de comunicarse con otros componentes. Las especificaciones J2EE definen los siguientes tipos de componentes [33]:

- ✓ Aplicaciones clientes o applets, que son componentes que se ejecutan en el cliente.
- ✓ Componentes de tecnología Java Servlet y JavaServer pages (JSP), que son componentes web que se ejecutan dentro del contenedor web en el servidor J2EE.
- ✓ Componentes de tecnología EnterpriseJava Beans (EJB) que son componentes de negocio que se ejecutan dentro del contenedor EJB en el servidor J2EE.

1. Clientes Web

Un cliente web está constituido de dos partes:

- ✓ Páginas web conteniendo diferentes tipos de lenguaje de marcado (HTML, XML, etc) que son generadas dinámicamente por componentes web que se ejecutan en el contenedor web.

- ✓ Un navegador web que genera las páginas recibidas desde el servidor y las presenta al cliente.

También se lo conoce como cliente delgado. No consulta una base de datos, no hace operaciones complejas de negocio y no se conecta a sistemas legados; todo lo complejo lo hace un componente EJB desde el servidor J2EE, donde se puede explotar las características de seguridad, velocidad y desempeño; los servicios y la confiabilidad de la tecnología del lado del servidor.

2. Clientes Applets

Una página recibida desde un servidor web puede incluir un applet incrustado. Un applet es una pequeña aplicación cliente escrita en Java que se ejecuta dentro de la JVM del navegador web. Este Applet se ejecuta normalmente con las restricciones propias impuestas y por efectos de eficiencia no se recomienda que

incluyan interfaces gráficas de usuario muy sofisticadas, para lo que es mejor emplear una aplicación cliente.

3. Aplicación Cliente

Se ejecuta en la máquina cliente y provee una interfaz gráfica de usuario enriquecida que es requerida para determinadas tareas. Típicamente su GUI está basada en Swing o AWT.

Las aplicaciones cliente acceden directamente los EJB en la capa de negocio; y a pesar de que no se requiere pueden acceder a componentes web a través de HTTP y establecer alguna conexión con un Servlet.

Una aplicación J2EE puede utilizar un cliente delgado basado en el navegador web o una aplicación del tipo cliente gordo; la decisión depende de las ventajas y desventajas de cada caso. Si es necesario tener bastante funcionalidad cerca del usuario en el cliente, es mejor utilizar una aplicación del tipo cliente gordo; pero si se puede enviar la funcionalidad al servidor se utilizará un cliente delgado.

Mientras más funcionalidad se envíe al servidor, más fácil es distribuir, implantar y administrar la aplicación; sin embargo cuanto más funcionalidad se pone del lado del cliente mejora la experiencia del usuario con la aplicación.

4. Componentes Web

Básicamente los componentes web, transforman la información de un modelo de datos, en un modelo de presentación que pueda ser exhibido a los clientes. Pueden ser Servlets o JavaServer Pages (JSP). Los Servlets son clases que procesan dinámicamente requerimientos y construyen respuestas; básicamente controlan los pedidos y requerimientos. Las páginas JSP son documentos basados en texto que se ejecutan como servlets pero proveen una forma más natural de generación de contenido dinámico. Pueden generar contenido HTML/XML con tags y scriptlets.

Las páginas HTML y los Applets pueden empacarse como componentes Web, pero según la especificación no son considerados como tales.

Al igual que la capa cliente, la capa web puede incluir componentes JavaBeans para administrar el ingreso de datos del

usuario y el envío de éstos datos a los componentes EJB ejecutándose en la capa de negocio. Los componentes JavaBeans se utilizan principalmente para el formateo de los datos adecuándolos a una presentación más elegante.

Las librerías de etiquetas, Tag Library, automatizan la generación de contenido sin código JSP.

Los componentes web se ubican dentro del modelo de una aplicación J2EE, tal como se muestra en la Figura 4.22:

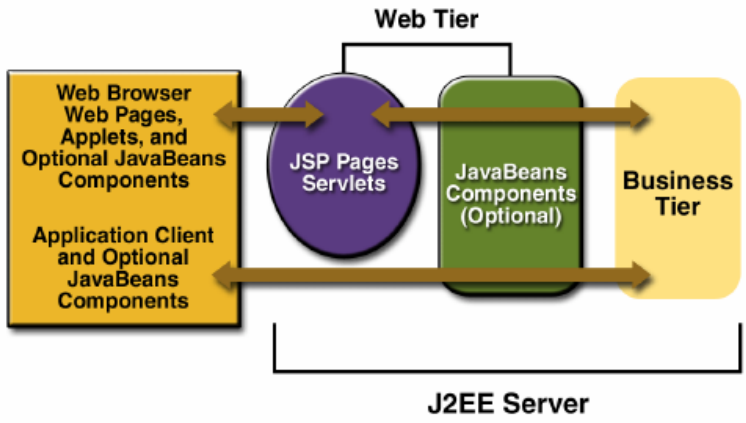


FIGURA 4.22. COMPONENTES WEB DE UNA APLICACIÓN J2EE [33]

5. Componentes de negocio

El código almacenado en la capa de negocio, que es la lógica que resuelve y satisface las necesidades de un dominio de negocio en particular como: la banca, una tienda virtual, las finanzas, etc; es implementado como componentes de negocio EJB.

Tal como se muestra en la Figura 4.23, un componente EJB recibe los datos desde los programas cliente, los procesa, y envía los resultados al Sistema de Información Empresarial para almacenarlos. Un componente EJB también recupera datos del almacenamiento, los procesa y los envía de regreso al programa cliente.

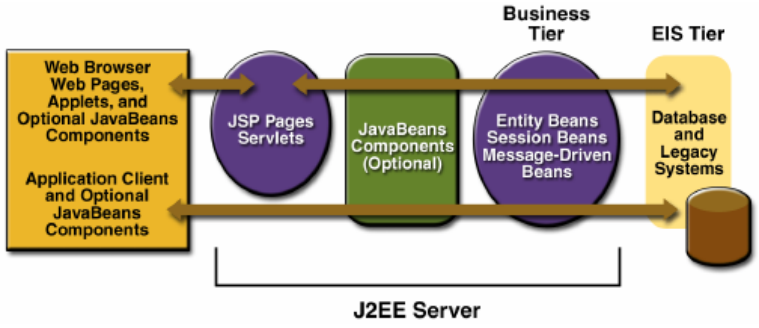


FIGURA 4.23. COMPONENTES DE NEGOCIO EJB DE UNA APLICACIÓN J2EE

Existen tres clases de componentes EJB:

- ✓ Los **Session Bean** que sirven para instrumentar una conversación transiente con el cliente. Una vez que el cliente termina la ejecución de su sesión, el Session Bean y sus datos se pierden.
- ✓ Los **Entity Bean** que representa a los datos persistentes almacenados en registros de una base de datos. Si el cliente termina su sesión de manera normal o accidental, los servicios de la infraestructura se encargan de guardar los datos del Entity Bean.
- ✓ Los **Message-driven Bean** que combina las características de un Session Bean y los servicios JMS (Java Message Service), un listener de mensajes que permite a un componente de negocio recibir un mensaje asíncronamente.

El desarrollador de aplicaciones define las interfaces remotas del objeto para interactuar con el componente empresarial de negocio (EJB), y la interfaz remota Home para gestionar su ciclo de vida.

El desarrollador escribe los objetos de negocio para lo cual puede:

- ✓ Emplear un Session Bean, para gestionar un workflow o controlar un caso de uso.
- ✓ Emplear un Entity Bean, para la implementación de un modelo o una entidad de una base de datos.
- ✓ Emplear un Message Driven Bean, para implementación síncrona o asíncronas a través de cola de mensajes vía JMS.

6. Capa de Sistemas de Información Empresarial

Son todos aquellos sistemas a los que una aplicación J2EE puede requerir algún tipo de acceso. Dentro de ésta capa tenemos a los sistemas de administración de bases de datos relacionales, los sistemas de administración de recursos empresariales (ERP), los sistemas transaccionales basados en mainframe, sistemas legados, etc.

7. Contenedores J2EE

Para evitar que los desarrolladores de aplicaciones tengan que enfrentarse a las complejas tareas de desarrollar enorme cantidad de código requerido para manejar transacciones, administrar

estados, administrar múltiples hilos de la aplicación, conglomerados (pools) de recursos y otros detalles de bajo nivel; el servidor J2EE provee servicios de infraestructura en forma de contenedor para cada tipo de componente, liberando de dicha responsabilidad al desarrollador.

Un contenedor es la interfaz entre los componentes y la funcionalidad específica de bajo nivel provista por la plataforma que soporta el componente. Antes de que un componente web, componente EJB o aplicación cliente se ejecute, debe ser ensamblada dentro de una aplicación J2EE e implantada dentro de su contenedor. El proceso de ensamblaje implica la configuración del contenedor específico para cada componente de la aplicación J2EE. La configuración del contenedor personaliza los servicios de infraestructura provistos por el servidor J2EE, los que incluyen: seguridad, gestión de transacciones, búsquedas JNDI y conectividad remota.

Tenemos cuatro tipos de contenedores bajo la especificación J2EE [33]:

- ✓ El contenedor EJB que gestiona la ejecución de los componentes EJB de las aplicaciones J2EE. Tanto los

componentes EJB como los contenedores se ejecutan en el servidor J2EE.

- ✓ El contenedor Web que gestiona la ejecución de JavaServer Pages (JSP) y Servlets. Los componentes web y los contenedores web se ejecutan en el servidor J2EE.
- ✓ El contenedor de aplicación cliente que gestiona la ejecución de los componentes de la aplicación cliente. Los componentes cliente y su contenedor se ejecutan en la aplicación cliente.
- ✓ El contenedor Applet que gestionan la ejecución de los applets. Consisten de un navegador web y su pluggin ejecutándose en el cliente.

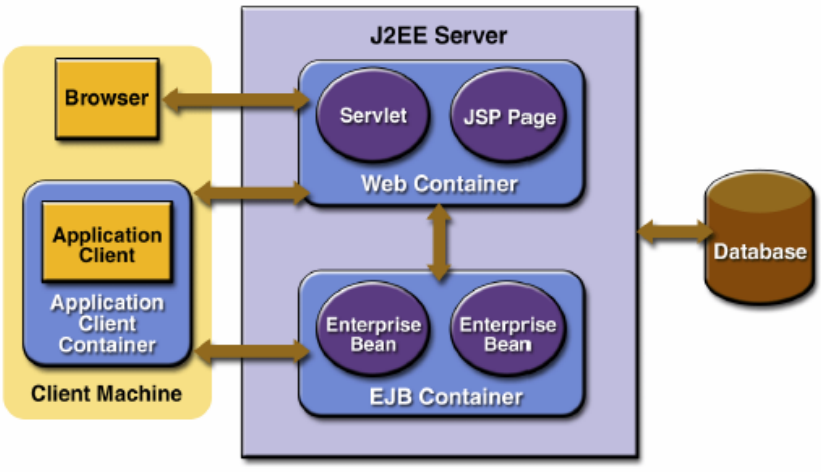


FIGURA 4.24. TIPOS DE CONTENEDORES EN LA ESPECIFICACIÓN J2EE [33]

Los componentes J2EE son empacados por separado y envueltos para su implantación. Cada componente con sus archivos relacionados de recursos (páginas HTML, imágenes gif, clases y descriptor) son ensamblados en un módulo y añadidos a la aplicación J2EE. Tanto la aplicación J2EE como sus módulos tienen un archivo XML conocido como descriptor de implantación, que contiene toda la información de configuración de la implantación del módulo. Al ser ésta información declarativa, puede ser modificada en el momento de implantación sin que sea necesario modificar el código fuente. En el momento de la ejecución, el servidor J2EE lee el descriptor de implantación, y ejecuta el componente de manera adecuada.

En la Tabla IX comparamos las tareas que son llevadas a cabo por los contenedores y las que son llevadas a cabo por los componentes. Como se verá más adelante en los roles dentro de la plataforma J2EE, los fabricantes de servidores J2EE son responsables de la implementación de los contenedores; mientras los desarrolladores de aplicaciones, de los componentes y su implementación en los contenedores.

TABLA IX

TAREAS A CARGO DE CONTENEDORES Y COMPONENTES

TAREAS A CARGO	
CONTENEDOR	**COMPONENTE**
• Concurrencia. • Seguridad. • Disponibilidad. • Escalabilidad. • Persistencia. • Transaccionalidad. • Gestión del ciclo de vida. • Administración.	• Presentación. • Lógica del negocio.

El contenedor maneja la concurrencia, es decir se encarga de los accesos concurrentes de los diferentes clientes a sus componentes de negocio, liberando la responsabilidad de tal implementación al desarrollador. Cada fabricante de servidor J2EE puede utilizar diferentes esquemas de sincronización para soportar la concurrencia.

Los contenedores proveen un marco de referencia (framework) de seguridad empotrado, de modo que se implementa la seguridad a las aplicaciones configurando algunas opciones de autenticación y

control de acceso, al momento de la implantación y no en el desarrollo.

Los fabricantes de servidores J2EE compiten con diferentes implementaciones que soporten la escalabilidad y la disponibilidad. Uno puede proveer alta disponibilidad manteniendo la información de sus sesiones en almacenamiento persistente, otro puede escoger implementarlo de manera diferente.

La persistencia y la transaccionalidad pueden ser gestionadas por el contenedor, pero si uno lo desea puede como desarrollador implementarla a su manera, escribiendo su propio código de manera más personalizada.

En cuanto a la gestión del ciclo de vida, los contenedores gestionan la creación y destrucción de instancias de los componentes empresariales según el esquema de implementación.

8. Roles de desarrollo sugeridos por la especificación J2EE

Proveedor de productos J2EE, es típicamente el fabricante del software base de infraestructura, incluye a los fabricantes de

sistemas operativos, bases de datos, servidor de aplicaciones, servidores web, cumpliendo las especificaciones J2EE.

Proveedor de herramientas, fabricante de herramientas de desarrollo, ensamblaje, empacamiento, implantación, las mismas que son utilizadas por los otros roles.

Proveedor de componentes de aplicación, son los desarrolladores de componentes.

Desarrollador de EJBs, provee un archivo EJB JAR. Escribe y compila código fuente, específica el descriptor de implantación y empaca los archivos .class y el descriptor de implantación en un mismo archivo EJB JAR.

Desarrollador de componentes web, provee un archivo WAR. Escribe y compila código fuente de servlets, escribe archivos JSP y HTML; específica el descriptor de implantación de componentes web, y empaca los archivos .class, .jsp y .html junto con el descriptor de implantación en un archivo WAR.

Desarrollador de aplicación cliente, provee un archivo JAR. Escribe y compila código fuente, especifica el descriptor de

implantación, y empaca los archivos .class y el descriptor de implantación en un archivo JAR.

Ensamblador de aplicaciones, recibe los archivos JAR de los proveedores de componentes y los ensambla en un archivo EAR. Puede editar los descriptores de implantación directamente o utilizar herramientas para la selección de etiquetas XML.

Implantador y administrador de aplicación, configura e implanta la aplicación J2EE, administra la infraestructura de procesamiento y red donde se ejecuta la aplicación, y revisa y monitorea el ambiente de producción. El implantador debe establecer controles transaccionales, atributos de seguridad y especificar las conexiones a las bases de datos.

Tales roles se describen de manera simplificada en la Figura 4.25:

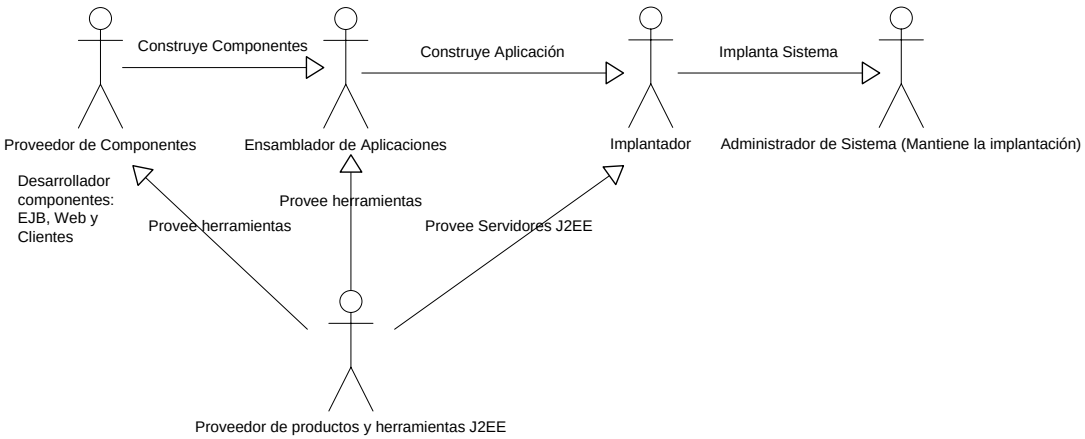


FIGURA 4.25. ROLES EN LA ESPECIFICACIÓN J2EE

En la Tabla X se describe brevemente las principales tecnologías e Interfaces de Programación de Aplicaciones, APIs, que conforman la arquitectura J2EE [33]:

TABLA X

TECNOLOGÍAS E INTERFACES DE PROGRAMACIÓN DE APLICACIONES (APIs) QUE CONFORMAN LA PLATAFORMA JAVA 2 ENTERPRISE EDITION

Tecnologías y APIs de la Plataforma J2EE	
Tecnologías de Servicios	
JDBC Java Database Connectivity	Permite invocar sentencias SQL desde los métodos programados en Java. Normalmente los componentes EJB no incluyen código JDBC, puesto que su persistencia es gestionada por el contenedor (CMP: Container Management Persistense). En cambio si se requiere que un Servlet o una Página JSP tenga acceso a una base de datos, se empleará

Tecnologías y APIs de la Plataforma J2EE	
Tecnologías de Servicios	
	JDBC.
JTA Java Transaction API	Se utiliza para demarcar transacciones. Por defecto provee un auto commit. Sin embargo si es necesario incluir en la misma transacción dos o más operaciones a la base de datos dependientes, se utilizar JTA para demarcar donde la transacción comienza, incluyendo las operaciones, y cuando se reversa o compromete. Funciona soportado por los servicios JTS.
JTS Java Transaction Services	Es un conjunto de interfaces de bajo nivel utilizadas por los componentes EJB. El código cliente nunca interactúa con éstas interfaces. JTS permite soportar transacciones en un ambiente distribuido y heterogéneo, y está basado en la especificación OTS (Object Transaction Service) que es parte de CORBA.
JNDI Java Naming and Directory Interface	Provee la funcionalidad de nombramiento y directorio, brindando métodos a las aplicaciones para ejecutar operaciones estándar de directorio, como asociar atributos con objetos, y búsqueda de objetos basados en atributos. Con JNDI se puede almacenar y recuperar cualquier tipo de objeto Java nombrado. Se puede utilizar múltiples servicios de directorio, como: LDAP, NDS, DNS y NIS.
JAAS Java Authentication and Authorization Service	Provee mecanismos para que una aplicación autentique y autorice a un usuario o grupo de usuarios específico. Es la versión del marco de referencia (framework) PAM (Pluggable Authentication Module) que hereda la arquitectura de seguridad de J2EE para soportar la autorización basada en usuario.
JCA J2EE Connector Architecture	Utilizada por los fabricantes de herramientas J2EE e integradores de sistemas para adaptadores de recursos que soporten acceso a sistemas de información empresarial (ERP) que se conecten directamente a un producto J2EE.

Tecnologías y APIs de la Plataforma J2EE	
Tecnologías de Servicios	
JAXP API para procesamiento XML	Para procesamiento de documentos XML utilizando: DOM, SAX (Simple API for parsing XML) y el lenguaje de transformación de hojas de estilo XML (XSLT). Con JAXP se puede hacer un análisis sintáctico de documentos XML y transformarlos de manera independiente de una implementación de procesamiento XML en particular. Con JAXP se puede utilizar cualquier procesador XSL compatible con parser XML y soporte al esquema W3C.
JAXR API para registro XML	Permite acceder a registros de negocio y propósito general en el web. Soporta los estándares de registro y repositorio ebXML y las especificaciones UDDI.
JAX-RPC API Java para RPC basado en XML	Utiliza los estándares SOAP y HTTP para que los clientes puedan hacer invocaciones RPC basados en XML sobre el Internet. Soporta WSDL para importar y exportar documentos WSDL.
SAAJ API SOAP para adjuntos Java	Es un API de bajo nivel del cual depende JAX-RPC. Permite la producción y consumo de mensajes conforme a la especificación SOAP 1.1 y con adjuntos.
Tecnologías de Comunicación	
JMS Java Message Server	Estándar de mensajería que permite a los componentes de una aplicación J2EE crear, enviar, recibir y leer mensajes asíncronos. Permite una comunicación distribuida con bajo acoplamiento, confiable y asíncrona.
JavaMail	Sirve para enviar notificaciones vía email.

Otras Tecnologías	
Tecnología EJB Enterprise Java Beans	Es la piedra angular de la arquitectura J2EE. Es una tecnología de componentes del lado del servidor para

Otras Tecnologías	
	desarrollo de aplicaciones de clase empresarial. **Por su importancia será presentada con mayor detalle.**
Java Servlets	Permiten definir clases servlet HTTP específicas, que heredan las capacidades de aplicaciones alojadas en los servidores con el modelo de aplicación petición – respuesta. Se utilizan comúnmente para extender las aplicaciones alojadas en los servidores web, generando contenido dinámico. En el patrón de diseño MVC, el Controller se implementa normalmente con Servlets.
JSP Java Server Pages	Permiten colocar partes de código de un servlet, directamente en una página basada en un documento. La página JSP tiene dos tipos de texto: • Una parte estática, expresada en cualquier formato basado en texto, HTML, XML ó WML. • Elementos JSP que determinan como se construye el contenido dinámico de la página. En el patrón de diseño MVC, los View normalmente se implementan con JSPs.
JAF JavaBeans Activation Framework	Está incluido en la plataforma J2EE porque JavaMail lo utiliza. Provee servicios para: determinar el tipo de una pieza de datos, encapsular el acceso a ellos, descubrir las operaciones disponibles en ellos, y crear los componentes JavaBeans adecuados para llevar a cabo esas operaciones.
RMI y RMI-IIOP Java Remote Method Invocation Internet Inter-ORB Protocol	Los componentes EJB dependen especialmente de la tecnología RMI. RMI es un mecanismo de comunicación interprocesos y de invocación de métodos ubicados en otras máquinas de manera remota. RMI abstrae al programador de los detalles de codificación de aspectos de bajo nivel como: soporte de redes, parámetros de bajo nivel, orden de bytes en las máquinas, etc. Soporta características como descarga dinámica de clases, activación automática de objetos remotos, y un recolector de basura distribuido, para

Otras Tecnologías	
	eliminar objetos remotos que ya no están en uso. RMI-IIOP es una extensión de RMI que utiliza el protocolo IIOP utilizado para la integración de J2EE con CORBA.
Java IDL	Es la implementación de IDL para integración de Java con otras aplicaciones distribuidas escritas en otros lenguajes. Permite aprovechar los servicios CORBA que pudiesen estar disponibles, logrando total compatibilidad.
JSTL Java Server Pages Standard Tag Library	Encapsula funcionalidad medular común para la mayoría de aplicaciones JSP, estableciendo un conjunto estándar de etiquetas como iteraciones y condicionales para control de flujo, etiquetas para manipular documentos XML, etiquetas para soportar internacionalización, etiquetas para acceder a bases de datos utilizando SQL, y otras funciones comunes.
Custom Tags	Una etiqueta personalizada (custom tag) es un elemento de lenguaje JSP definido por el usuario. Se utilizan normalmente para operar en objetos implícitos, procesamiento de formularios, operaciones de acceso a bases de datos u otros servicios empresariales como correo electrónico o directorios, e implementación de control de flujo. Las etiquetas personalizadas aumentan la productividad porque pueden ser reutilizadas en más de una aplicación dentro de la Organización.
JavaServer Faces	Es un marco de referencia (framework) de componentes de interfaz de usuario del lado del servidor para aplicaciones web basadas en tecnología Java. Está compuesto por dos componentes principales: • Un API para representar componentes de interfaz de usuario y gestionar su estado; manejar eventos, realizar validaciones del lado del servidor, y conversión de datos; definición de la navegación de la página; soporte a internacionalización y accesibilidad; y provisión de extensión de todas éstas características.

Otras Tecnologías
• Dos librerías de etiquetas personalizadas JSP para expresar los componentes de interfaz de usuario dentro de las páginas JSP y para relacionar los componentes a los objetos del lado del servidor.

En la Figura 4.26 se muestran los diferentes elementos de la plataforma J2EE: componentes, contenedores, interfaces de programación y tecnologías.

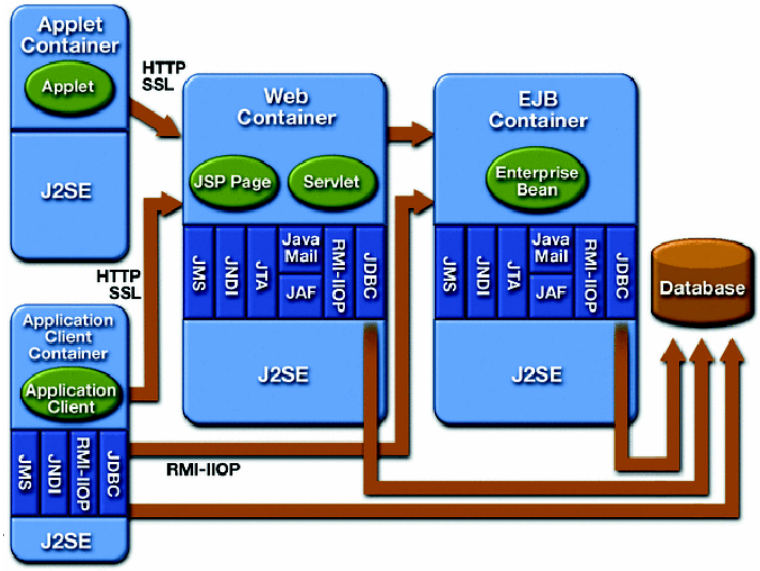


FIGURA No. 4.26 ELEMENTOS DE LA PLATAFORMA J2EE

En el patrón de diseño de arquitectura de software Model View Controller (MVC), el Model se implementa normalmente con

componentes empresariales EJB, y residen en el contenedor EJB del servidor J2EE; el Controller se implementa normalmente con componentes web Servlets, y residen en el contenedor Web del servidor J2EE; y los View se implementan con JSPs. En la Figura No. 4.27 se muestra lo dicho:

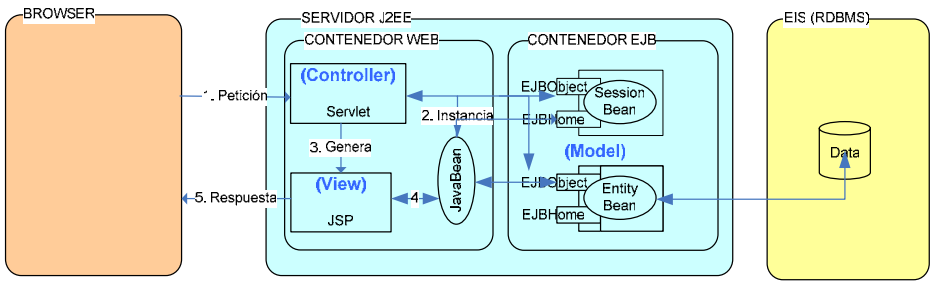


FIGURA No. 4.27 IMPLEMENTACIÓN DEL PATRÓN DE DISEÑO MVC EN LA PLATAFORMA J2EE

En el Apéndice C se detalla las tecnologías que componen la arquitectura y las interfaces para programación de aplicaciones J2EE.

9. Tecnología EJB

Tal como se dijo antes, la tecnología EJB es la piedra angular de la plataforma J2EE, razón por la cual merece al menos una presentación resumida.

EJB es una tecnología de componentes del lado del servidor, que facilita el desarrollo de aplicaciones Java, con calidad empresarial; es decir que sean: transaccionales, distribuidas, múltiple capa, portables, seguras, escalables y confiables.

Los componentes EJB son alojados en el contenedor EJB del servidor J2EE, el que les provee los siguientes servicios: gestión de recursos (pool de conexiones a base de datos), coordinación de transacciones (gestionadas por el contenedor), y gestión de la persistencia. Además de la portabilidad a diferentes servidores J2EE, se puede tener adaptación a diferentes ambientes operacionales, con diferentes políticas de seguridad, bases de datos y modelos transaccionales, gracias al descriptor de implantación. Modificando el descriptor de implantación, se puede modificar el comportamiento de un componente EJB de manera declarativa, sin topar el código.

El desarrollador de componentes EJB escribe tres archivos en Java: la interfaz Home EJB que define los métodos que utilizarán los clientes para crear y ubicar su componente; la interfaz Remote EJB, que define los métodos de negocio del componente; y el componente en sí que implementa todos los métodos. Los objetos

Home y Remote, son objetos intermediarios del componente, que permiten el manejo de la concurrencia por parte del contenedor. En la Figura 4.28 se muestra un esquema de la tecnología EJB [33]:

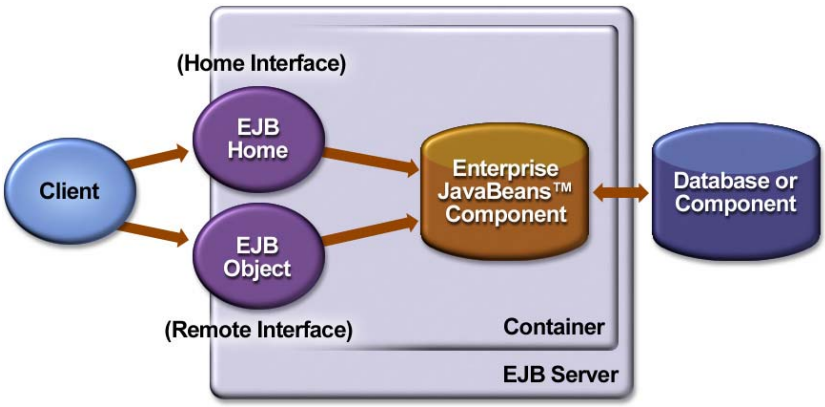


FIGURA No. 4.28 MODELO DE OPERACIÓN DE LA TECNOLOGÍA EJB

Existen tres tipos de componentes EJB: los Session Bean, los Entity Bean, y los Message-Driven Bean.

Session Bean

Son objetos que representan “trabajo en ejecución”, un proceso de negocio. Implementan lógica de negocio, reglas de negocio y flujos de trabajo, como por ejemplo: cotización de precios, ingreso

de orden, compresión de video, transacción bancaria, mercado de valores, etc.

Un Session Bean “vive” mientras dure la sesión del cliente que lo invocó. Una vez que el cliente se desconecta y se pierde su sesión, el servidor de aplicaciones elimina la instancia del Session Bean.

Un Session Bean es utilizado por un solo cliente a la vez, es decir no son compartidos entre clientes. El servidor de aplicaciones es el responsable de gestionar el ciclo de vida del Session Bean.

Hay dos tipos de Session Bean:

- **Stateful Session Beans.-** Algunos procesos se ejecutan en una sola petición, otros requieren múltiples peticiones y transacciones, como por ejemplo el carrito de compras. Éste es un proceso en el que el componente debe controlar el estado del usuario de petición en petición. Para ese tipo de procesos se utiliza un Stateful Session Bean, que puede retener el estado de un cliente individual.

- **Stateless Session Bean.**- Sirve para procesos de negocio de una sola petición, en el que no se requiere mantener el estado entre diferentes invocaciones de sus métodos. Por ejemplo: la invocación de un motor de alto desempeño que resuelve operaciones matemáticas complejas, como la compresión de video.

Entity Bean

Los procesos de negocio casi siempre utilizan datos permanentes almacenados en algún sistema de persistencia, como una base de datos relacional. El Entity Bean representa los datos persistentes. Como ejemplo tenemos: una cuenta bancaria, una orden, un item de compra, etc.

Los Entity Bean representan objetos del mundo real como clientes, productos, empleados. No contienen lógica de procesos de negocio, solo modelan datos. Los Session Bean utilizan Entity Beans para representar los datos que requieren los procesos implementados.

Los Entity Bean permiten combinar la funcionalidad de datos persistentes con la conveniencia de la encapsulación de los

objetos. Un Entity Bean implementa la lógica de acceso a la capa de datos en una arquitectura múltiple capa. En la Figura 4.29 tenemos una representación de un Entity Bean:

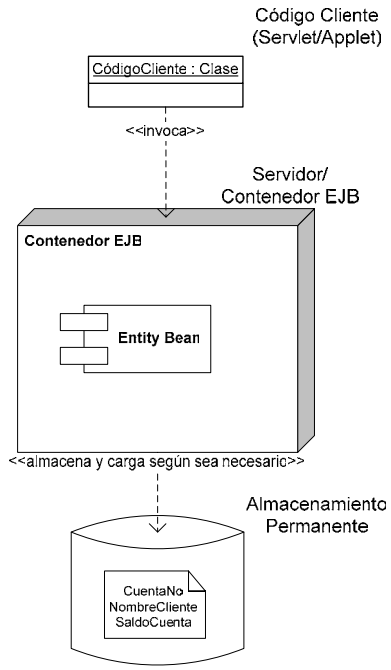


FIGURA No. 4.29 REPRESENTACIÓN DE UN COMPONENTE EJB DEL TIPO ENTITY BEAN

Un Entity Bean puede ser accedido por múltiples clientes simultáneamente, soportando concurrencia. Para aislar la manipulación de datos por múltiples clientes entre sí, se utilizan las transacciones, lo que garantizará la integridad de los datos en un ambiente multiusuario.

Hay dos tipos de Entity Beans:

- **Bean-Managed Persistent Entity Bean (BMP).-** Es un componente cuya persistencia es manejada a mano. El desarrollador del componente escribe el código para mantener los mismos datos de sus campos en memoria en el sistema de persistencia, encargándose de almacenar, cargar y encontrar datos dentro del Entity Bean. El desarrollador utiliza un API de persistencia como JDBC ó SQL/J.

- **Container-Managed Persistent Entity Bean (CMP).-** Evita a los desarrolladores codificar la lógica de la persistencia. El contenedor se encarga de las operaciones de persistencia: almacenar, cargar y encontrar datos del componente. En éste esquema el desarrollador no se preocupa de tratar con las API de persistencia, sino que el contenedor se encarga de todas las operaciones de persistencia por uno.

- **Message-Driven Bean (MDB).-** Sirven para soportar el paso de mensajes asincrónicos, combinando la

funcionalidad de los componentes EJB con los servicios JMS (Java Message Service). En la mensajería asincrónica, un mensaje en cola no es persistente. Un MDB se utiliza para consumir mensajes, a pesar de que puede enviar y recibir mensajes. Las características de un componente MDB son:

- Son anónimos, no visibles al cliente. No mantienen ningún estado por parte del cliente.
- Todas las instancias de un MDB en particular, son equivalentes.
- El contenedor puede crear un consorcio de instancias.
- No tiene interfaz remota ni local.
- Es invocado asíncronamente por el contenedor.
- Los componentes viven en el contenedor, quien gestiona su ciclo de vida y su entorno.

La principal diferencia con otros componentes EJB, es que el MDB no puede ser invocado directamente por el cliente, por lo que no tiene interfaces Home, Remote o Local; por esto es menos propenso al mal uso por parte del cliente.

Servicios Web

Una tecnología emergente muy importante que ha surgido en los últimos tiempos son los servicios web. Son aplicaciones empresariales basadas en el web, que utilizan estándares abiertos XML y protocolos de transporte para intercambiar datos en respuesta a invocaciones de clientes.

Al permitir Java portabilidad de código de las aplicaciones, y XML portabilidad de datos; la traducción de datos a cadenas de datos estandarizadas basadas en XML es lo que hace que los servicios web y los clientes escritos en Java con los API Java XML sean totalmente interoperables.

Los servicios web son importantes por dos razones fundamentales:

- ✓ **Ubicuidad.-** Es un término frecuente empleado por las dos plataformas líderes de implementación de aplicaciones empresariales: J2EE y Microsoft .Net.

- ✓ **Facilidad de uso.-** Requiere mucho menos habilidades técnicas para su implementación. La tecnología de servicios web está orientada hacia una comunidad con menos destrezas técnicas, emplea herramientas más simples que ha facilitado su adopción.

La necesidad de integración entre dos enfoques diferentes de desarrollo de aplicaciones empresariales, hace que los servicios web sean una palabra de moda. Definitivamente, es la forma más simple y fácil de integrar J2EE, CORBA y Microsoft .Net.

Los servicios web son tecnología complementaria a otras tecnologías como J2EE, CORBA y Microsoft .Net; no las reemplaza.

Algunas definiciones previas

WSDL

Es un formato XML estandarizado que permite describir un servicio web. La descripción incluye la siguiente información:

- ✓ Nombre del servicio,
- ✓ Ubicación del servicio, e,
- ✓ Indicaciones de cómo comunicarse con el servicio.

Las definiciones WSDL (Web Services Description Language) se almacenan en registros UDDI publicados en el web.

SOAP/UDDI

Son una propuesta desarrollada en conjunto por Microsoft e IBM. SOAP (Simple Object Access Protocol) fue escrito por IBM y ofrecido a la fundación Apache, por lo que la plataforma Apache AXIS es la referencia para la norma SOAP en el W3C. SOAP es un protocolo de comunicación para servicios web, utilizado para intercomunicar aplicaciones. Dentro de los principales problemas de SOAP, es que todavía se siguen experimentando entre los desarrolladores, no resuelve completamente el problema de

autenticación y no está totalmente soportado en ambientes de desarrollo ampliamente difundidos en el web, como PHP.

SOAP es la alternativa de interoperabilidad de los servicios web implantados tanto en la plataforma J2EE como en la plataforma Microsoft .Net.

UDDI (Universal Description, Discovery and Integration) es un sistema de registro que permite a las organizaciones publicar interna o externamente sus servicios web, y es donde la información puede ser leída y consultada, y globalmente accedida por los clientes. En términos corrientes, funciona a manera de páginas amarillas.

Los servicios web se basan en un modelo de petición – respuesta, donde existe un cliente que solicita un servicio, y existe un proveedor del servicio que responde. Ambos interactúan a través los estándares plenamente definidos. En la Figura 4.30 se muestra un modelo conceptual de la arquitectura para servicios web SOAP/UDDI/WSDL:

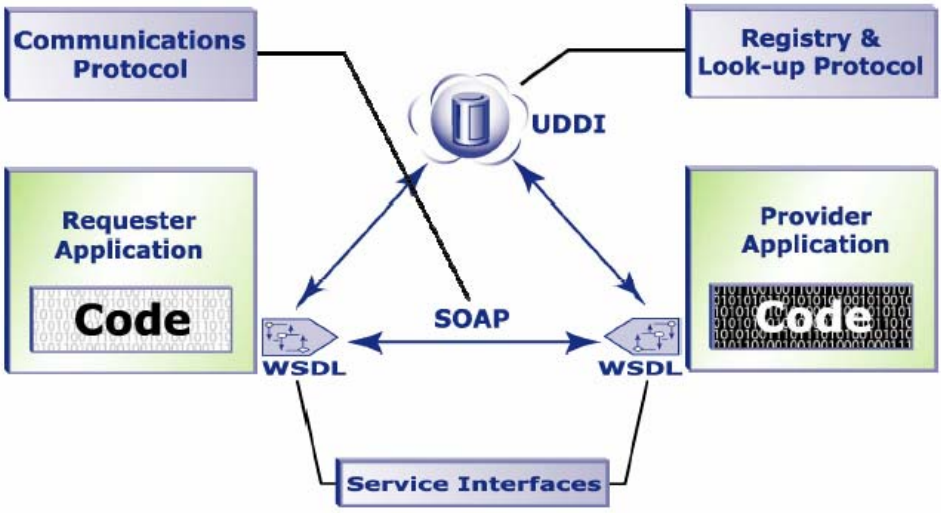


FIGURA 4.30 MODELO DE OPERACIÓN DE SOAP/UDDI/WSDL

ebXML

Es un estándar global para definir un marco de referencia (framework) propuesto por las Naciones Unidas en OASIS (**O**rganization for the **A**dvancement of **S**tructured **I**nformation **S**tandards), que trata de resolver la problemática de las comunicaciones entre empresas, con énfasis a proveer un esquema que permita conducir transacciones del tipo B2B (Business to Business), basado en XML.

ebXML utiliza SOAP como medio de transporte, y se dice que es el sucesor de EDI (Electronic Data Interchange). El cliente invoca

un servicio web de mensajería enviando un documento completo con un conjunto de parámetros. El servicio web, acepta el documento y retorna una respuesta, la misma que puede ser asíncrona.

ebXML es una colaboración entre servicios web a través de XML. En ebXML tenemos los siguientes componentes:

- ✓ **Registro.-** Provee un “contenedor” para los modelos de procesos, vocabularios y perfiles.

- ✓ **Procesos de negocio.-** Definidos como modelos, expresados en XML.

- ✓ **Acuerdos entre socios colaborativos.-** Expresados en XML, donde se especifican los parámetros para la colaboración.

- ✓ **Componentes centrales.-** Pequeños bits de información que se emplean generalmente para proveer “semántica” al contenido.

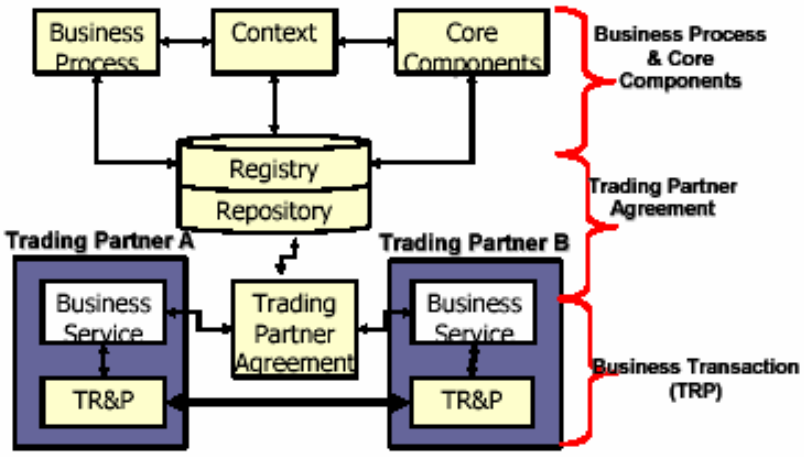


FIGURA 4.31 MODELO DE OPERACIÓN DE ebXML

Ciclo de vida de un servicio web en J2EE desde el punto de vista del proveedor

Lo primero que hace un desarrollador de un servicio web en la plataforma J2EE, es definir la interfaz del servicio en WSDL, que es el estándar de facto. Una vez definido el servicio, se lo puede implementar, para posteriormente ser implantado. Finalmente, el servicio web debe ser publicado.

La definición del servicio web en WSDL hace las veces de contrato entre el proveedor y el cliente del servicio.

Las características de la arquitectura J2EE de implantar la lógica del negocio como componentes que se ejecutan en un contenedor, son las que sirven de base para implementar e implantar un servicio web en la plataforma J2EE. El contenedor de servicios web, de manera similar a los otros contenedores en J2EE, provee un ambiente de alojamiento de los front end de los servicios web para su ejecución. En éste ambiente de ejecución se provee una vinculación a un transporte y a un puerto. El front end de un servicio web, puede ser el manejador de mensajes SOAP que invoca las funciones de negocio de los componentes J2EE.

Ciclo de vida de un servicio web en J2EE desde el punto de vista del cliente

Un cliente descubre e invoca un servicio web en la plataforma J2EE. El proceso de invocación más sencillo es a través de una invocación RPC (Remote Procedure Call), o enviando un mensaje. Típicamente el cliente utilizará un talonario el cual tendrá toda la lógica necesaria para comunicarse con el servicio web.

El proceso de descubrimiento involucra encontrar el documento WSDL, o encontrar el talonario cliente cuando esté disponible; el

mismo que puede ser generado dinámicamente desde el documento WSDL durante la implantación del cliente o en tiempo de ejecución. El API empleado es JAXR utilizado para servicios de registro como UDDI y ebXML.

El talonario cliente contiene todo el código necesario para la invocación del servicio web, es decir que conoce el transporte requerido y a que punto terminal (puerto) debe conectarse ese transporte para la invocación del servicio web.

En la Figura 4.32 se muestra la representación del enfoque dado por la plataforma J2EE, para la provisión de servicios web:

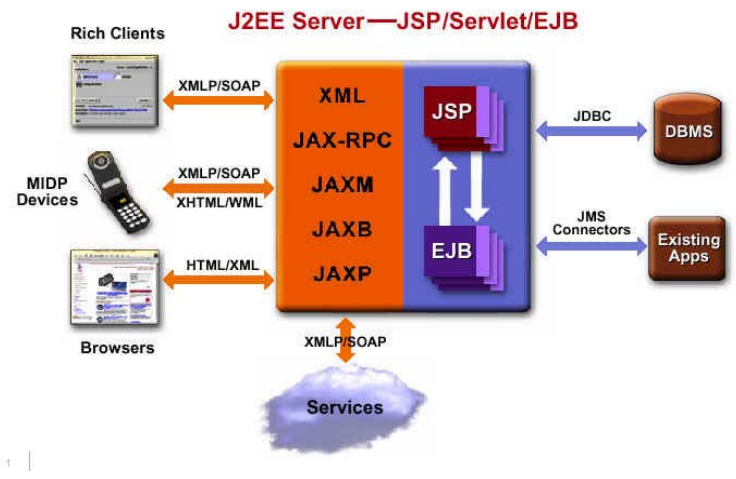


FIGURA 4.32 Modelo DE OPERACIÓN DE SERVICIOS WEB SOBRE J2EE

4.4 Diseño Macro de la Intranet, Distribución Física de los Servidores en los Data Center

Para el presente diseño, se pretende seguir los siguientes principios:

- ✓ **Minimizar la inversión de hardware.-** Lo necesario para proveer los servicios planteados en las secciones anteriores.

- ✓ **Alcanzar los niveles adecuados en los servicios propuestos.-** Estos servicios incluyen los de usuario: Administración y compartición de la información, Comunicación y colaboración, Navegación en las fuentes de información, Acceso a las aplicaciones centradas en red. Y también los de red: Directorios de usuarios, Replicación de la información, Certificación y seguridades, Administración de la red.

- ✓ **Hacer un uso efectivo del ancho de banda.-** Si bien es cierto las Fuerzas Armadas cuentan con un sistema de telecomunicaciones propio, con un costo de operación asociado relativamente bajo, también hay un alto costo de oportunidad al no emplearlo adecuadamente, optimizando los recursos existentes. Por lo tanto se considera que se puede utilizar todo el ancho de banda

disponible para cada sector geográfico, pero optimizando su empleo a través de una ubicación adecuada de los servidores que contribuyan a obtener mejores tiempos de respuesta especialmente para aquellas aplicaciones y servicios que se consideren críticos, y contribuyan al mejoramiento de la disponibilidad del sistema, minimizando el costo de tenencia.

- ✓ **Desarrollar una infraestructura de soporte adecuada.-** Contar con el mínimo de personal técnico encargado de la gestión y mantenimiento de la infraestructura, debido a la dificultad y limitación propia de contar con suficientes técnico que tengan un perfil adecuado, con habilidades y conocimientos de administración y soporte de redes de datos, y con un adecuado entrenamiento sobre los servicios de la Intranet, para que conformen la infraestructura necesaria de soporte.

- ✓ **Minimizar el impacto en las infraestructuras de redes existentes.-** En el caso particular de la Armada, donde la infraestructura existente se centra especialmente a unas cuantas redes de área local, se deberá tratar de emplear ésta infraestructura, mejorando el esquema de conexión y acceso al sitio central a través

de enlaces de red de área ampliada o a través de los backbone de los campus principales.

4.4.1 DISEÑO DE LA INTRANET DE LA ARMADA

Las infraestructuras tecnológicas en organizaciones grandes como la Armada, son complejas: con componentes que son provistos por diferentes proveedores. Estas infraestructuras distribuyen una variedad de servicios tanto dentro como fuera de la organización, mucho de los cuales son de misión crítica.

Para soportar de manera efectiva a la organización con los servicios provistos dentro del Intranet, y responder adecuadamente a las necesidades cambiantes de los usuarios, gestionando adecuadamente el cambio tecnológico, evitando una pérdida del control en el crecimiento de la infraestructura tecnológica y la proliferación de múltiples soluciones por doquier, se propone un esquema estandarizado, estructurado y ordenado.

La infraestructura tecnológica debe tener características de disponibilidad, seguridad, escalabilidad y fácil administración de la plataforma. Los principales beneficios que se proveen con la infraestructura tecnológica planteada son:

- ✓ Reducir los tiempos y costos de implementación, asegurando reducir el tiempo para obtener beneficios.
- ✓ Desempeño predecible y confiable.
- ✓ Niveles de disponibilidad que permitan alcanzar los niveles de servicio requeridos.
- ✓ Niveles de seguridad coherentes con las características de la organización.
- ✓ Escalabilidad para satisfacer las demandas de los usuarios.
- ✓ Reducir los riesgos de implementación y operación.

Los síndromes de crecimiento desordenado que se deben evitar en la implantación de la infraestructura o en el reordenamiento de la infraestructura existente son los siguientes:

- ✓ **Proliferación de servidores.-** El crecimiento desordenado causa principalmente la proliferación de servidores de diferentes tipos, funciones y tamaños. Más servidores requieren más técnicos para administrarlos y mantenerlos, lo que

aumenta el Costo Total de Tenencia de la infraestructura (TCO).

- ✓ **Proliferación de plataformas.-** El enfoque de contar con la mejor solución para cada tipo de problema es la principal causa de la proliferación de plataforma. Cuando la organización encuentra que el mejor sistema de gestión de inventarios lo encontró sobre la plataforma UNIX, el mejor sistema de correo electrónico lo encontró sobre Windows, y que la mejor solución de servidor de archivos sobre Linux; termina con una mezcla poco deseada de plataformas que causa que el soporte total de la plataforma, su mantenimiento y los costos de operación eleven el Costo Total de Tenencia. A pesar de que es muy difícil unificar una sola plataforma en una organización grande, es deseable tratar de definir una plataforma para la mayoría de servicios, y minimizar la necesidad de otra.

- ✓ **Proliferación del almacenamiento.-** Existe una demanda creciente de almacenamiento debido al aumento de la información digitalizada. Pero éste almacenamiento ha crecido desordenadamente basado en múltiples discos duros en los computadores de escritorio, o en pequeños servidores de

archivos departamentales. La gestión del almacenamiento de manera segura y ordenada, garantizando integridad y disponibilidad de la información bajo éste enfoque es imposible.

Otras variables a considerar al momento de proponer una infraestructura tecnológica son:

- ✓ **La presión del Alto Mando para reducir los costos en tecnología de información.-** Cada inversión en tecnología de información debe ser justificada y mostrar un verdadero retorno sobre ésta, en una situación fiscal deficitaria, austera y compleja.

- ✓ **La seguridad**.- Aspecto central en cuanto al manejo de la información ordinaria y calificada en una organización militar, y particularmente relevante cuando el Internet es uno de los mecanismos importantes para la comunicación con otras entidades y organizaciones. Es vital por tanto tener una estrategia coherente para asegurar los sistemas y los datos de modo que se garantice la continuidad de las operaciones informáticas en la Institución.

- ✓ **Cumplimiento de los niveles de servicio requeridos cada vez más complejos**.- Para tal efecto se requiere que la gente, los procesos y la tecnología, funcionen efectivamente en un entorno ordenado y controlado, de modo que se pueda optimizar los servicios al momento de tener que alcanzar un determinado nivel dentro de las limitaciones propias de la Institución.

- ✓ **La operación efectiva y la administración de los sistemas y servicios**.- Son vitales para mantener los niveles de servicio requeridos. La mayoría de fallas de servicios son debido a fallas de personas o procesos, los que a menudo se produce cuando gestionan una infraestructura compleja y desordenada.

1. Metas del diseño [34]

Disponibilidad.- La disponibilidad depende principalmente de un diseño cuidadoso y disciplina operacional. Esto incluye control de cambios, rigurosas pruebas previas, actualizaciones y mecanismos de recuperación de caídas. La clave para alcanzar alta disponibilidad es aislar la funcionalidad de un servicio de las fallas de componentes individuales. Para ello se tiene que diseñar con la

idea de que el componente fallará. Cada componente de la infraestructura tecnológica propuesta es una solución o una estrategia para proveer alta disponibilidad. Se provee en conjunto técnicas y tecnologías para evitar caídas totales del sistema y poder satisfacer las necesidades de procesamiento. Para evitar puntos únicos de fallas en el diseño, se dota de redundancia o especialización funcional para contener las fallas empleando dispositivos que son unos respaldo de otros, estableciendo múltiples rutas de comunicación entre servidores, y empleando tecnologías especializadas como los conglomerados o clusters de servidores. El enfoque empleado para cada capa de la infraestructura tecnológica es diferente, por ejemplo en la capa de servidores de presentación se emplea principalmente balanceo de carga entre servidores relativamente similares; mientras que en la capa de administración de datos, se utiliza un cluster activo más especializado y dependiente de la base de datos.

Seguridad.- La propuesta implementa una estrategia de defensa en profundidad, lo que nos permite poseer un esquema seguro y monitoreable. El enfoque incluye desde seguridad periférica de la red, hasta seguridad de los datos almacenados. La defensa en

profundidad va más allá de tecnología meramente, implica seguridad física, detección de intrusos, políticas de seguridad y procedimientos de reacción. Es decir combina aspectos proactivos y reactivos.

Escalabilidad.- Escalabilidad es la habilidad de una infraestructura tecnológica para gestionar demandas de procesamiento crecientes a un nivel aceptable de desempeño. Para la necesidad real de la Armada, se propone un esquema de escalamiento horizontal, empleando máquinas pequeñas de hasta dos procesadores, por ser el esquema más equilibrado en cuanto a costos y al resto de metas de diseño. La capa tecnológica que gestiona la base de datos está provista en un cluster real activo, mientras que las capas de servidores de aplicación y servidores web, están configurados en un esquema de balanceo de carga.

Fácil Administración.- Solución completa y centralizada para la implantación, monitoreo, gestión de alertas y alarmas, y administración de toda la infraestructura y contenido implantado. Para lograr esto es necesario tener un enfoque que considere al menos lo siguiente:

- ✓ **Propósito.-** Mantener escenarios en el que se cuente con servidores, sistemas y dispositivos de propósito específico; de modo que la configuración e implantación sea más sencilla y tome menos tiempo, así la infraestructura al contar con servidores especializados se vuelve más confiable y tendrá un comportamiento predecible.

- ✓ **Monitoreo y gestión de alarmas.-** No es posible medir el desempeño, predecir problemas, o mantener disponibilidad de la infraestructura tecnológica, sin un mecanismo adecuado de monitoreo y gestión de alarmas. Cualquier falla que se produzca debe ser conocida inmediatamente por un administrador de sistema, de modo que se tomen las medidas correctivas de manera oportuna. Un monitoreo adecuado contribuye a través de la auditoría a proveer un ambiente más seguro. La definición de alarmas basadas en el uso de recursos, estableciendo valores umbrales (thresholds), permite tomar decisiones de crecimiento proactivamente, antes de que el nivel de servicio se degrade y sea percibido por el usuario. El monitoreo y la gestión de alarmas son el principal mecanismo

empleado para la planificación de capacidades de la infraestructura tecnológica.

- ✓ **Administración remota.-** El soporte de infraestructuras complejas se mejora cuando las tareas administrativas se pueden ejecutar remotamente a través de la red corporativa. La administración remota evita el tiempo y los costos asociados al traslado de técnicos especializados y administradores para la resolución de situaciones que mayoritariamente se pueden llevar a cabo a través de la red.

Confiabilidad.- Una solución confiable es aquella que tiene un comportamiento consistente bajo toda condición de carga de procesamiento.

Facilidad de soporte.- Debido a las restricciones de disponibilidad de recurso humano técnicamente calificado, la solución propuesta provee una facilidad de soporte a través de la centralización de los recursos complejos de la infraestructura.

La disposición de equipos en la infraestructura tecnológica es un juego que busca tener un equilibrio entre desempeño, flexibilidad, escalabilidad, seguridad y facilidad de administración, a través de la

combinación de capas físicas y zonas lógicas. En las capas se utiliza tecnología de conglomerados o clustering, existiendo básicamente dos tipos de clusters:

Cluster para balanceo de carga.- Que se refiere básicamente al clonamiento de una capa de aplicación del tipo “solo lectura”, entre dos o más nodos que son accesibles a través de una misma dirección IP virtual. Se utiliza típicamente en los servidores web (componentes de interfaz de usuario) y servidores de aplicaciones (componentes de reglas de negocio). Este tipo de cluster mejora la escalabilidad en sentido horizontal y mejora la disponibilidad. En éste tipo de cluster, un nuevo requerimiento de algún cliente es despachado al servidor que tenga en ese momento menos carga de procesamiento. En caso de que se presente alguna falla en ese servidor, el requerimiento no será recuperado hasta que el cliente vuelva a hacer el requerimiento y éste sea nuevamente despachado a otro servidor.

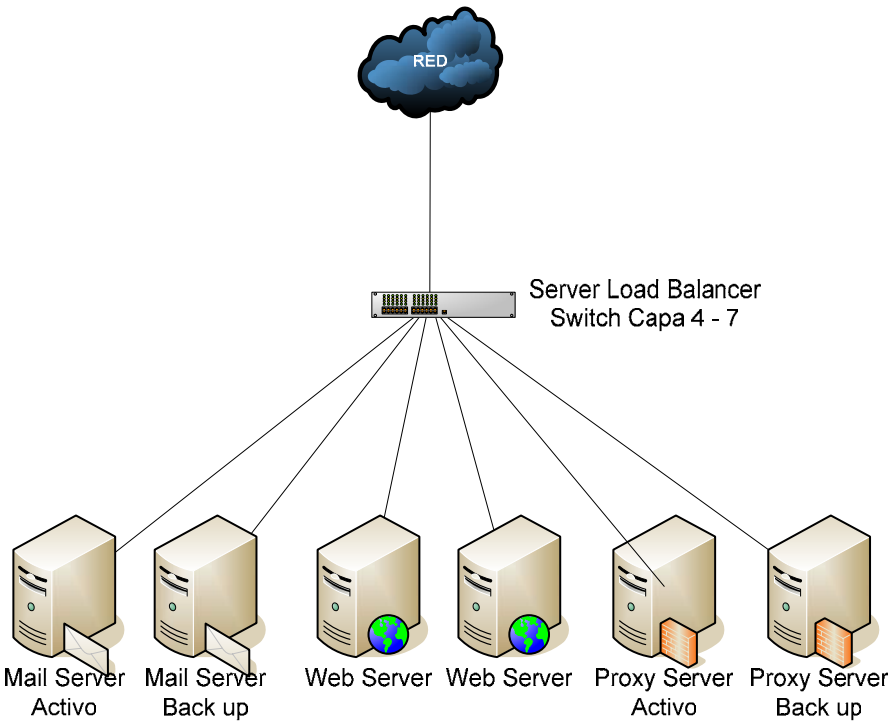


FIGURA 4.33 CLUSTER CON BALANCEO DE CARGA EN CAPAS INTERMEDIAS CON SWITCHES CAPA 4 – 7

Cluster de recuperación de fallas.- Este tipo de cluster se refiere a una capa de aplicación del tipo “lectura – escritura”, típicamente la base de datos. Existen cluster de recuperación de fallas en frío y en caliente. En los cluster de recuperación de falla en frío, la base de datos está particionada en varios nodos siguiendo alguna lógica de partición (orden alfabético de clientes ó repartos, ubicación geográfica, etc) en un esquema conocido como base de datos

federada. En caso de presentarse una falla en uno de los nodos que está procesando una transacción, se termina el procesamiento y la transacción es reversada. Dependiendo el tipo de daño que existe en los nodos y la configuración de hardware que se tenga, se podrá recuperar la capacidad de procesamiento en varias horas. Si la aplicación es de misión crítica y susceptible a un tiempo prolongado de caída, se estila tener en el cluster un servidor con suficientes características de hardware y software, que sea capaz de soportar el procesamiento de su porción de la base de datos y la porción equivalente de la base de datos del nodo que falló; con software de partición lógica o emulación de máquina virtual (Ejemplo: VMWare), se restaura la porción de la base de datos en la partición lógica nueva del servidor de recuperación de fallas, evitando así tener que modificar la lógica de acceso a los datos en las diferentes sentencias SQL de la aplicación, hasta restaurar totalmente la capacidad de procesamiento normal. Otra limitación que tiene un cluster de recuperación de fallas en frío, es que no tiene capacidad de balanceo de carga, puesto que los datos están particionados como habíamos dicho siguiendo alguna lógica.

En un cluster de recuperación de fallas en caliente, la base de datos es totalmente compartida a través de un arreglo de discos externo único para todos los nodos. Estos a su vez tienen capacidad de proveer balanceo de carga y recuperación de fallas. En este tipo de cluster cuando un nodo falla, el cluster detecta la falla, y las sesiones de clientes que no fueron culminadas exitosamente, son reversadas y posteriormente recuperadas una vez que la base de datos recupero su consistencia, para nuevamente ser procesadas. La disponibilidad de un cluster de recuperación de fallas en caliente es mucho mayor a un cluster de recuperación de fallas en frío. La diferencia de tiempo de recuperación de una falla típica mayor en los servidores del cluster de la base de datos varía de varias horas en el primer esquema, a algunos minutos en el segundo esquema.

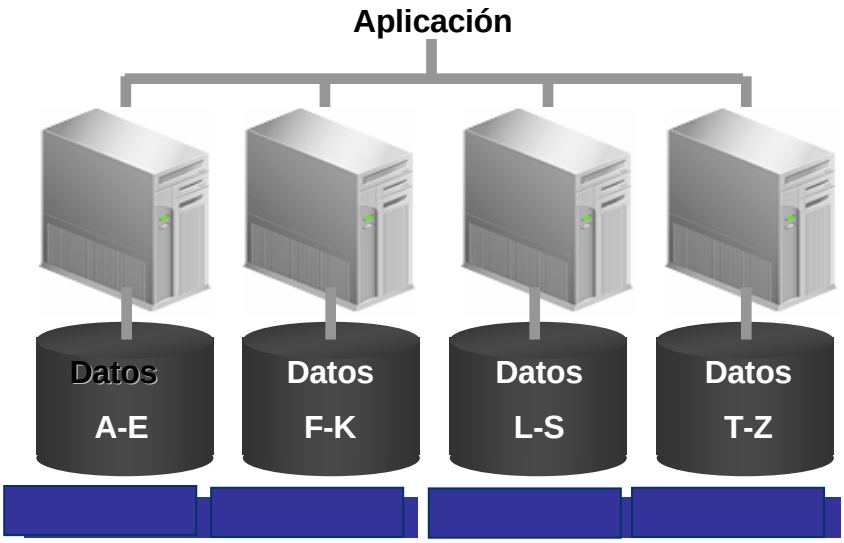


FIGURA 4.34 CLUSTER DE RECUPERACIÓN DE FALLOS COLD FAILOVER

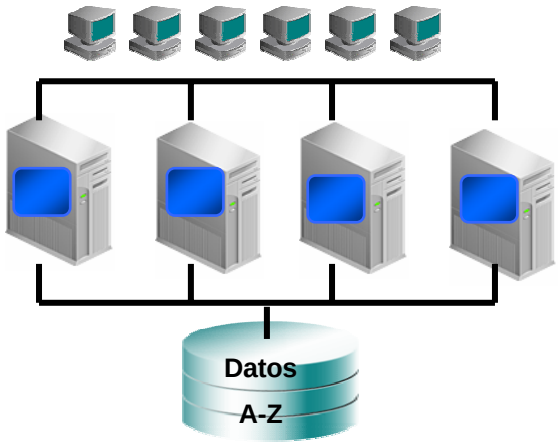


FIGURA 4.35 CLUSTER DE RECUPERACIÓN DE FALLOS HOT FAILOVER

4.4.2 INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO

Las zonas de confianza o zonas de seguridad, se refieren a las redes de servidores limitadas por cortafuegos o Firewalls, a través de los cuales se limitan los protocolos de comunicación y se regula el tráfico entre una red y otra. Estas zonas son protegidas con barreras contra los ataques que pueden comprometer la seguridad de la infraestructura tecnológica y los datos, y son definidas típicamente a partir de una política de seguridad. La estrategia implementada es una defensa en profundidad, lo que implica tener tres zonas de confianza:

- ✓ **Zona Desmilitarizada Pública (DMZ Pública).-** Infraestructura Tecnológica accesible desde el Internet, por cualquier cliente o servidor a los servicios definidos como públicos.

- ✓ **Zona Desmilitarizada Privada (DMZ Privada).-** Infraestructura Tecnológica accesible desde cualquier cliente o servidor dentro de la red corporativa de la Armada.

- ✓ **Zona Militarizada (MZ).-** Infraestructura Tecnológica que únicamente es accesible por determinados recursos de la red corporativa de la Armada.

Detrás de todo el esfuerzo de montar la infraestructura tecnológica, está la provisión de servicios a los usuarios.

En la Zona Desmilitarizada Pública están todos los servicios públicos de Internet, es decir:

- ✓ Servicios de Mensajería Electrónica Corporativa.
- ✓ Servicios Web y HTTP.
- ✓ Consola Antivirus.
- ✓ Servicios de Proxy Transparente y DNS.
- ✓ Balanceo de Carga.
- ✓ Almacenamiento Externo Tipo NAS.
- ✓ Sistema de Detección de Intrusos (IDS).
- ✓ Firewall de Borde.

En la Figura 4.36 se muestra la Infraestructura Tecnológica de Procesamiento de la Zona Desmilitarizada Pública – Internet Servers:

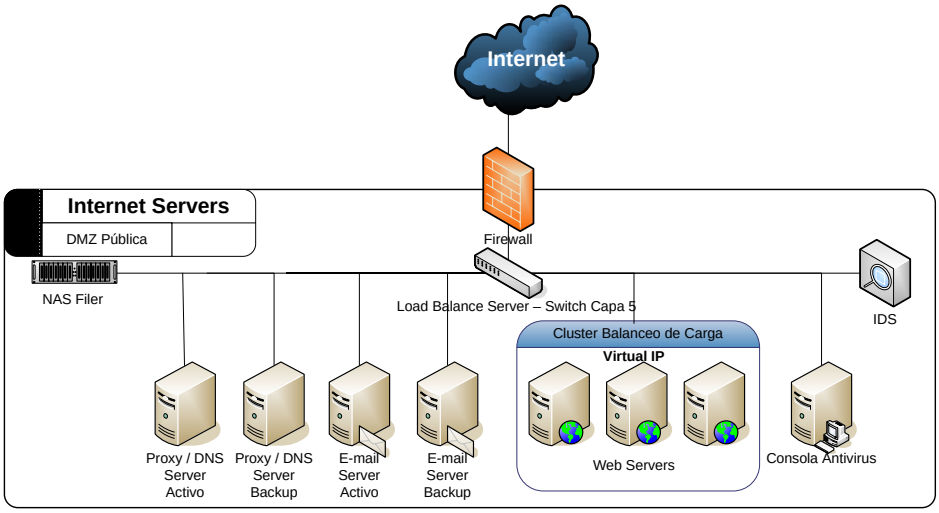


FIGURA 4.36 INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO DE LA ZONA DESMILITARIZADA PÚBLICA – INTERNET SERVERS

En la Zona Desmilitarizada Privada están todos los servicios corporativos privados, es decir:

- ✓ Servicios de Infraestructura de Claves Públicas / Certificados Digitales.
- ✓ Servicios Web y HTTP (Privados).
- ✓ Servicios de Directorio Corporativo.
- ✓ Servicios Colaborativos.

- ✓ Servicios de Audio y Video en Demanda.
- ✓ Servicios de Contenido.
- ✓ Servicios Terminales Windows – Citrix.
- ✓ Servicios DHCP.
- ✓ Servicios de Administración de la Infraestructura.
- ✓ Sistema de Detección de Intrusos (IDS).
- ✓ Firewall Interior.

La Zona Desmilitarizada Privada está separada de la Zona Desmilitarizada Pública a través de un Firewall de cuatro zonas: DMZ Pública, DMZ Privada, MZ y Consola de Administración (NOC).

En la Figura 4.37 se muestra la Infraestructura Tecnológica de Procesamiento de la Zona Desmilitarizada Privada – Intranet Servers:

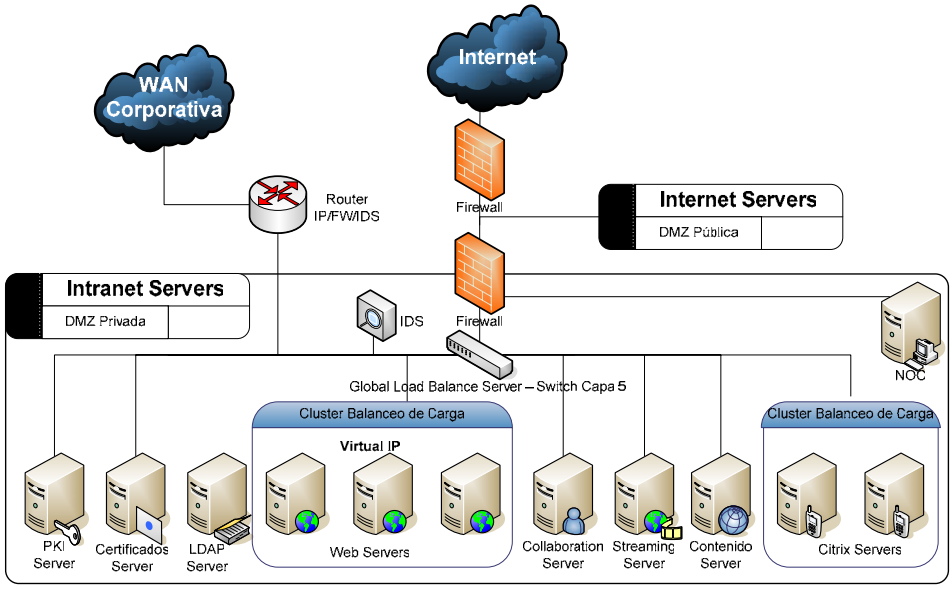


FIGURA 4.37 INFRAESTRUCTURA TECNOLÓGICA PROCESAMIENTO DE LA ZONA DESMILITARIZADA PRIVADA – INTRANET SERVERS

En la Zona Militarizada todos los recursos de la infraestructura tecnológica están orientados a mantener los datos corporativos en bases de datos y archivos. Estos por su sensibilidad deben estar debidamente protegidos y bajo un esquema de seguridad apropiado, la infraestructura en ésta zona se muestra en la Figura 4.38:

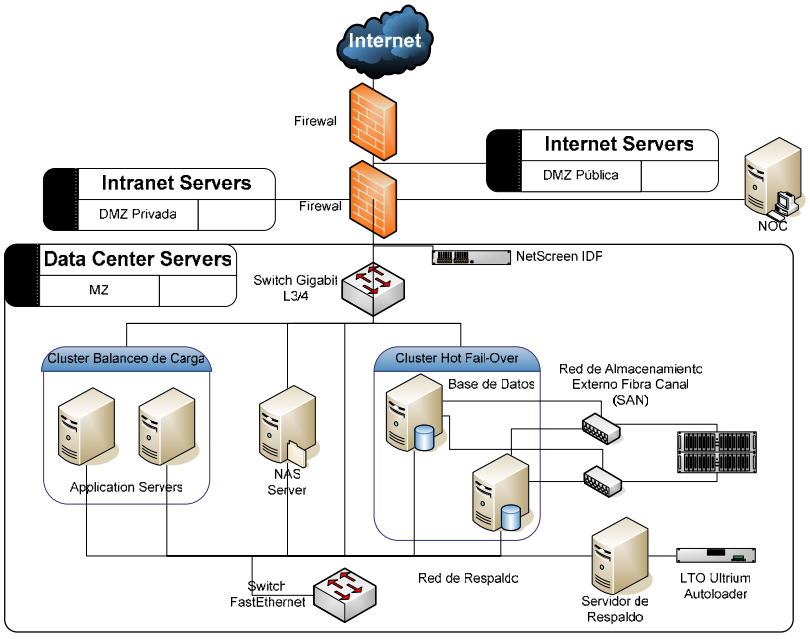


FIGURA 4.38 INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO Y ALMACENAMIENTO DE LA ZONA MILITARIZADA – DATA CENTER SERVERS

El detalle de los equipos propuestos se muestra en el Apéndice D – Plataforma Tecnológica de Procesamiento.

Ventajas del diseño de infraestructura propuesto

- ✓ Es factible tener capacidad de escalar o crecer de manera independiente en las capas de presentación, reglas de negocio y datos.

- ✓ Es más fácil lograr aislamiento de posibles fallas o abuso de mal uso de recursos en cada una de las capas.

- ✓ La disponibilidad de recursos en la capa de presentación, reglas de negocio o gestión de datos puede ser garantizada de manera independiente y gradual según tenga sentido.

Desventajas del diseño de infraestructura propuesto

- ✓ Se requiere esfuerzos de configuración mayores dentro de cada capa (comparado con una aplicación cliente – servidor tradicional).

- ✓ Se requiere una configuración de seguridad por separado en cada una de las capas.

- ✓ El desempeño se ve afectado por la latencia de la red (debido a la invocación de servicios entre componentes divididos físicamente en diferentes máquinas).

- ✓ El diagnóstico de problemas se vuelve más complejo.

- ✓ La implantación de las aplicaciones es más compleja debido a tener que tratar y afinar diferentes máquinas, y a la incidencia de los cortafuegos que dividen las distintas zonas del modelo.

4.5 Diseño de la Red de Datos [34]

Los requerimientos en cuanto a infraestructura tecnológica de comunicaciones para la Red de Datos, al más alto nivel pueden definirse de la siguiente manera:

"Los usuarios necesitan conectarse a los sistemas de información y servicios provistos en base a tecnología de información de manera eficiente, confiable y segura."

La arquitectura de red a diseñar por tanto tendrá como objetivos los siguientes:

- ✓ Proveer un movimiento de paquetes de datos confiable y eficiente desde un dispositivo fuente a un dispositivo destino.

- ✓ Cumplir con la política de seguridad corporativa.

La red corporativa propuesta está basada en una combinación de las siguientes tecnologías y elementos:

- ✓ **Segmentos de red de área local (LAN).-** Un segmento de red de área local, se define como dos o más dispositivos que se comunican entre sí a nivel de capa 2 del modelo OSI, utilizando dispositivos de conectividad LAN de capa 2, sin ruteo a nivel de capa 3 entre ellos. Los segmentos de red pueden ser físicos o lógicos, en cuyo caso son referidos como redes de área local virtuales (VLAN). Existen también segmentos LAN en el que se interconectan múltiples segmentos de red LAN utilizando un dispositivo de capa 3.

- ✓ **Redes de área extendida (WAN).-** Las redes de área extendida se forman uniendo dos o más redes de área local a través de dispositivos y tecnologías WAN. En el diseño propuesto, los dispositivos terminales de acceso a las redes de área extendida, pertenecen a la Armada, pero los dispositivos y la infraestructura entre tales dispositivos, pertenecen al sistema de telecomunicaciones del Comando Conjunto de Fuerzas Armadas, y no están bajo control directo y administración de la Armada, por lo que son empleados tal cual están.

- ✓ **Dispositivos de conectividad LAN.-** Son los dispositivos que proveen conectividad en capa 2 y 3 en los segmentos LAN, o entre LANs.

    - **Dispositivos de conectividad LAN de capa 2.-** Dispositivos cuya función principal es simplemente mover paquetes de datos a nivel de capa 2 entre hosts o dispositivos en el mismo segmento de red. En el diseño propuesto, es funcionalidad típicamente provista por un switch.

    - **Dispositivos de conectividad LAN de capa 3.-** Dispositivos cuya función principal es mover paquetes de datos a nivel de capa 3 entre múltiples segmentos de red. En el diseño propuesto Ruteadores (incluidos switches de capa 3 y 4) y dispositivos de balanceo de carga son empleados para tal propósito. Emplean en éste diseño la pila de protocolos TCP/IP. En ésta categoría también se debe resaltar los dispositivos corta fuegos y servidores de acceso que proveen control del flujo de tráfico basado en reglas de seguridad.

- ✓ **Tecnologías y dispositivos de conectividad WAN.-** Proveen la funcionalidad para interconectar clientes o sitios remotos a un Data Center de aplicaciones, una infraestructura central de acceso a Internet, o a redes de terceros que por su relación con la Organización requieren así hacerlo.

- ✓ **Protocolos de red.-** Para cada escenario es muy importante hacer una definición de que protocolos de red están en uso en la Organización, lo que debe ser cuidadosamente planificado.

- ✓ **Política de Seguridad.-** La arquitectura de la red debe añadir características que le permita asegurar la integridad y disponibilidad del tráfico de datos que soporta. Por ejemplo, debe controlar que puertos TCP/UDP pueden establecer conexiones entre dispositivos de la red. La política de seguridad determina aspectos que afectan al diseño de la arquitectura de una red.

Para el diseño de la red, es indispensable establecer lo siguiente:

- ✓ **Definición de Zonas de Seguridad.-** Se debe definir las zonas de seguridad agrupando una o más capas de la infraestructura, de modo que se cumplan con los requerimientos de seguridad

de la manera más adecuada, buscando permanentemente un balance entre el nivel de seguridad deseado y el desempeño.

- ✓ **Restricción de datos en las Zonas de Seguridad.-** Se deben definir los protocolos que están autorizados para mover datos entre las zonas de seguridad. Esta información debe obtenerse aplicando la política de seguridad vigente.

- ✓ **Comunicación de datos requeridas por las capas.-** Con la información detallada se indica que capas necesitan comunicarse con que otras, que puerto TCP y UDP se requieren, y que protocolos serán empleados.

- ✓ **Desempeño de comunicaciones requerido en los servidores y disponibilidad de datos.-** Se debe proveer una información detallada de los niveles de latencia aceptables, niveles de disponibilidad y las necesidades de ancho de banda entre cada uno de los computadores origen y destino.

4.5.1 REQUERIMIENTOS INSTITUCIONALES

La Armada requiere desarrollar una infraestructura estándar que le permita crecer con flexibilidad de manera segura y confiable.

Ésta infraestructura incluye el empleo del Internet, permitiendo la provisión de servicios basados en el Internet tanto para usuarios internos como externos. Entre los principales servicios basados en Internet tenemos:

- ✓ Presencia en el Web a través de un portal corporativo para usuarios internos y externos que incluya:
  - Información Institucional.
  - Información de contacto.
  - Información de eventos y acontecimientos relevantes.
  - Acceso al correo electrónico basado en web de manera segura.
  - Información y aplicaciones de valor agregado para usuarios internos, proveedores y organizaciones relacionadas con la Institución.
- ✓ Redes Privadas Virtuales para facilitar los siguientes tipos de comunicación:

- Comunicación con proveedores y organizaciones relacionadas con la Institución. (Extranet)

- Acceso remoto a usuarios de la institución. (Intranet)

- Conexiones seguras desde las agregadurías y misiones en el exterior a la red corporativa a través de la red pública. (Internet)

✓ Como parte de los servicios de red se requiere además:

- Un servicio de directorio unificado que soporte una administración centralizada, con registro único (single sign on), y que tenga capacidades de auditoría.

- Conectividad LAN y WAN segura.

- Almacenamiento consolidado a nivel corporativo.

- Encriptamiento basado en infraestructura de claves asimétricas (PKI)

- Herramientas colaborativas y de mensajería.

Teniendo a la seguridad como el principal requerimiento técnico impuesto, el diseño debe asegurar que todos los mecanismos apropiados sean implementados en las capas apropiadas de la arquitectura de red para minimizar los riesgos de ataques a los recursos institucionales. Éste diseño pretende satisfacer los siguientes requerimientos:

- ✓ Todos los servicios tienen alta disponibilidad.
- ✓ Los servicios de red, incluyendo las comunicaciones a través del Internet, son seguras de extremo a extremo.
- ✓ Todas las comunicaciones a través de la red que no están explícitamente permitidas, son denegadas.
- ✓ Todos los servicios utilizan un mecanismo de autenticación centralizado.
- ✓ Todas las aplicaciones son autenticadas y auditables.
- ✓ Se tiene capacidades de administración centralizada de la infraestructura.

- ✓ La salud de los servicios es monitoreable de modo que se prevean caídas costosas.

- ✓ La integridad de los datos está garantizada y bajo ningún caso se la puede exponer.

4.5.2 DEFINICIÓN DE LAS ZONAS DE SEGURIDAD

La Definición de Zonas de Seguridad ha sido tomada en parte de acuerdo a las recomendaciones de arquitectura de sistemas de Microsoft (30), pero han sido adaptadas por los autores de éste trabajo al modelo de la arquitectura de software de la plataforma propuesta: Java 2 Enterprise Edition.

Para comenzar a definir las zonas de seguridad en términos generales diferenciamos dos Zonas: la Zona Internet, y la Zona Privada.

Zona Internet.- El Internet y el segmento de conexión a la interfaz externa del elemento activo de conexión de la Armada (ruteador de borde) son parte de la Zona Internet. Los usuarios externos que acceden a los servidores web públicos, las agregadurías y misiones navales en el exterior, y los usuarios que se conectan a

la red a través de Redes Privadas Virtuales (VPN) son parte de ésta zona.

Zona Privada.- Incluye todas las capas de conectividad, capas de aplicación y segmentos de red conectados en el lado interno del ruteador de borde de la Institución. El propósito de ésta zona es separar el tráfico de red interno, del tráfico hacia y desde la Zona Internet. La frontera entre la Zona Privada y la Zona Internet es un ruteador en cuya capa 3 de acuerdo al modelo OSI se implementa Listas de Control de Acceso (ACL) para controlar el tráfico entrante, aplicando la política de seguridad de la Institución. La Zona Privada está compuesta por la Zona de Borde Público, la Zona Desmilitarizada Pública, la Zona Desmilitarizada Privada, la Zona de Borde Confiable, la Zona Militarizada y la Zona de Clientes.

Zona de Borde Público.- Conocida también como “Zona No Confiable”, contiene las capas que llevan a cabo alguna funcionalidad de control de acceso que aísla la Zona Internet de la Zona Desmilitarizada Pública. En ésta Zona está únicamente la capa de servicios cortafuegos o Firewall de borde para simplificar

la administración y creación de reglas de seguridad para el tráfico de salida y entrada hacia la Zona Internet.

Zona Desmilitarizada Pública.- Esta zona contiene las capas que están limitadas por alguna función de control de acceso impuesta entre la Zona Internet y el resto de Zonas dentro de la Zona Privada. El propósito de ésta Zona es facilitar la creación de políticas de seguridad de modo que el tráfico pueda ser filtrado entre las Zonas Internet y Privada. Ésta Zona es conocida como Red Perimetral y mantiene información semiconfiable. Contiene las capas que proveen servicios públicos, tales como DNS, servicios de información, servicios web, aplicaciones públicas, correo electrónico y el servicio de acceso a clientes de redes privadas virtuales. Los equipos dentro de ésta Zona tienen una dirección IP pública, y por tanto tienen algún tipo de acceso desde la Zona Internet. A pesar que hay capas de control de acceso implementadas entre la Zona Internet y la Zona Desmilitarizada Pública, debemos estar concientes que los equipos de ésta Zona son los blancos más expuestos a ataques maliciosos. La Zona Desmilitarizada Pública a su vez está subdividida en las siguientes Zonas adicionales: Zona de Servicios de Información Perimetral,

Zona de Servicios Web Perimetral, Zona de Servicios de Nombramiento Perimetral, Zona de Correo Electrónico Perimetral, Zona de Servicios Proxy Perimetral, Zona de acceso de clientes servicio de Redes Privadas Virtuales y la Zona de Administración Antivirus.

Zona de Servicios de Información Perimetral.- Esta Zona contiene la capa de servidores web. Sobre ésta zona el control de acceso es implementado para controlar el flujo de tráfico entre ésta Zona y la Zona Internet. Al establecer ésta Zona se pueden establecer controles más restrictivos con filtros de puertos.

Zona de Servicios de Aplicaciones Perimetral.- Esta Zona incluye la capa de servidores de aplicación con un control de acceso de mayor granularidad para implementar un control de flujo de tráfico entre ésta Zona y la Zona Internet. Ésta Zona tiene mayor control de acceso que la Capa de Servidores Web de la Zona anterior, siendo una especie de Zona anidada de ésta.

Zona de Servicios de Nombramiento Perimetral.- En ésta Zona está la capa de servidores DNS públicos. La Armada contará con sus propios servidores DNS en lugar de utilizar los servidores DNS

del ISP, lo que le permitirá tener mayor flexibilidad. Se crea ésta Zona para que el control de acceso pueda ser implementado entre ésta Zona y la Zona Internet.

Zona de Correo Electrónico Perimetral.- Zona compuesta por la capa de servicios de mensajería electrónica pública. En ésta capa están los servidores de correo electrónico activo y de respaldo.

Zona de Servicios Proxy.- Ésta Zona está compuesta por la capa de Proxy. El servicio Proxy recibe los requerimientos de parte de los clientes internos, pueden ser proxies de sitios regionales, y recuperan la información requerida desde el Internet. Estadísticamente se ha comprobado que la mayoría del tráfico HTTP bajado desde el Internet es repetitivo, es decir los usuarios generalmente visitan las mismas páginas web durante el día. Desde éste punto de vista es ventajoso establecer un servidor Proxy HTTP transparente de tal manera que todo paquete cuyo destino sea el puerto 80 sea interceptado y redirigido a éste Proxy. Esto puede ahorrar hasta un 10% de ancho de banda. Bajo algoritmos determinísticos, un servidor Proxy asume que parte del contenido solicitado por un usuario, puede haber sido ya solicitado

antes por otro usuario, evitando así hacer el requerimiento nuevamente, descongestionando el tráfico.

Zona de Acceso Clientes de Redes Privadas Virtuales (VPN).- Ésta Zona contiene la capa que provee acceso de clientes a través de la implementación de Redes Privadas Virtuales, simulando redes privadas a través de establecer túneles en una red pública por los cuales se transmite el tráfico. Los túneles VPN encapsulan los datos privados en paquetes encriptados, que son enviados a través de las redes públicas. Esto asegura tanto la confidencialidad como la autenticación con una integridad validada de extremo a extremo.

Zona de Administración Antivirus.- Ésta Zona incluye las consolas de actualización de las definiciones de virus informáticos.

Zona de Borde Confiable.- Conocida también como “Zona Confiable”, contiene capas que llevan a cabo funcionalidad de control de acceso que aísla la Zona Desmilitarizada Privada del resto de Zonas. En ésta Zona está únicamente la capa de cortafuegos internos para simplificar la administración y creación

de reglas de seguridad para el tráfico de salida y entrada hacia la Zona Desmilitarizada Privada.

Zona Desmilitarizada Privada (DMZ Privada).- Esta zona contiene las capas que están limitadas por las funciones de control de acceso impuestas entre la Zona Desmilitarizada Pública y el resto de Zonas dentro de la Zona Privada. El propósito de ésta Zona es facilitar la creación de políticas de seguridad de modo que el tráfico pueda ser filtrado entre la Zona Desmilitarizada Pública, la Zona Militarizada y las Zonas de Clientes. Ésta Zona mantiene información confiable de uso interno, contiene las capas que proveen servicios privados, tales como servicios de claves asimétricas, certificados digitales internos, servicios de directorio corporativo, servicios privados de información, servicios web privados, aplicaciones privadas, servicios colaborativos de mensajería estructurada, provisión de contenido y multimedia. Los equipos dentro de ésta Zona tienen direcciones IP privadas, y por tanto tienen reglas de acceso más estrictas. A pesar que hay capas de control de acceso implementadas hacia la Zona Desmilitarizada Privada, debemos estar concientes que los equipos de ésta Zona son los blancos de ataques maliciosos

propiciados desde el interior de la red. La Zona Desmilitarizada Privada a su vez está subdividida en las siguientes Zonas adicionales: Zona de Servicios de Información Privados, Zona de Servicios Web Privados, Zona de Servicios de Infraestructura, Zona de Accesos Remotos, Zona de Aplicaciones Privadas y la Zona de Administración.

Zona de Servicios de Información Privados.- Esta Zona contiene la capa de servidores web internos (Intranet). Sobre ésta zona el control de acceso es implementado para controlar el flujo de tráfico entre ésta Zona y la Zona de Clientes Internos. Al establecer ésta Zona se pueden establecer controles más restrictivos con filtros de puertos y reglas de flujo de información.

Zona de Servicios de Infraestructura.- En ésta Zona está la capa de servidores que permiten operar la infraestructura privada de manera segura y que están relacionados con el manejo de claves privadas y públicas, certificados digitales internos, servicios de directorio y servicios de autenticación AAA. La Armada contará con sus propios certificados digitales y firmas digitales basadas en una solución PKI, en lugar de utilizar certificados emitidos por una Autoridad de Certificación para uso externo. Se crea ésta Zona

para que el control de acceso pueda ser implementado entre ésta Zona y las Zonas de Clientes Internos. El servidor de Autenticación, Autorización y Auditoría está basado en TACACS+. En primera instancia el propósito de este servidor es verificar a través de la autenticación, “quien” tiene privilegios de acceso a “que” servicios de Internet y “cuando” a través de la autorización, llevando un registro al respecto.

Zona de Accesos Remotos.- Ésta Zona contiene la capa que provee acceso remoto a los recursos internos. Ésta capa básicamente concentra los servidores de acceso remoto basados en la red telefónica pública y privada a través de modems analógicos.

Zona de Aplicaciones Privadas.- Zona compuesta por la capa de aplicación para provisión de servicios de mensajería electrónica estructurada con herramientas colaborativas, provisión de contenido multimedia y provisión de servicios de computación remota para la habilitación de aplicaciones cliente – servidor al paradigma del web.

Zona de Administración.- En la Zona Desmilitarizada Privada se encuentran las consolas de administración de la infraestructura con herramientas que permiten monitorear, diagnosticar y resolver problemas de los recursos informáticos en el resto de Zonas, basados en el protocolo SNMP.

Zona Militarizada.- El propósito de ésta Zona Interna es aislar las capas que soportan los servicios internos más críticos de la Institución, y que por lo tanto deben estar protegidos de la manera más confiable posible. Ésta Zona tiene a su vez las siguientes Zonas: Bases de Datos Corporativas, Infraestructura de Aplicaciones Corporativas, e Infraestructura Corporativa. Con ésta medida se separan los servidores corporativos que almacenan los datos de las aplicaciones, del resto de Zonas, especialmente de los Clientes. Los mecanismos de control de acceso son de granularidad muy fina y más estrictos, contando además con mecanismos de respaldo y recuperación ante fallas que protejan los recursos de información.

Zona de Bases de Datos Corporativas.- Contiene la capa de bases de datos corporativas. El propósito de ésta Zona es permitir la implementación de mecanismos de control de acceso

sumamente estrictos a nivel de aplicación. Con ello se tiene pleno control de los privilegios de visualización y edición de los datos contenidos en las bases de datos corporativas a nivel de aplicación.

Zona de Infraestructura de Aplicaciones Corporativas.- En ésta Zona tenemos la capa de alojamiento o los contenedores de los servidores de aplicación a nivel de la capa intermedia, sobre la cual se implementan estrictos controles de acceso por parte de la capa de servidores web en cuanto a accesos en el ambiente de producción, y de los desarrolladores/implantadores en cuanto a publicación de nuevas aplicaciones.

Zona de Infraestructura Corporativa.- Constituida por los recursos que permiten mantener servicios de respaldo y restauración de la infraestructura corporativa en un segmento de red propio que permita realizar las tareas de respaldo sin degradar ni afectar a la disponibilidad de los servicios.

Zona de Clientes.- Contiene en términos abstractos a la capa cliente de la Institución, que constituyen los diferentes segmentos

de red que a través de la infraestructura de red, tienen acceso a los servicios provistos por el resto de capas.

La definición de Zonas se aprecia mejor en la Figura 4.39 que se muestra a continuación:

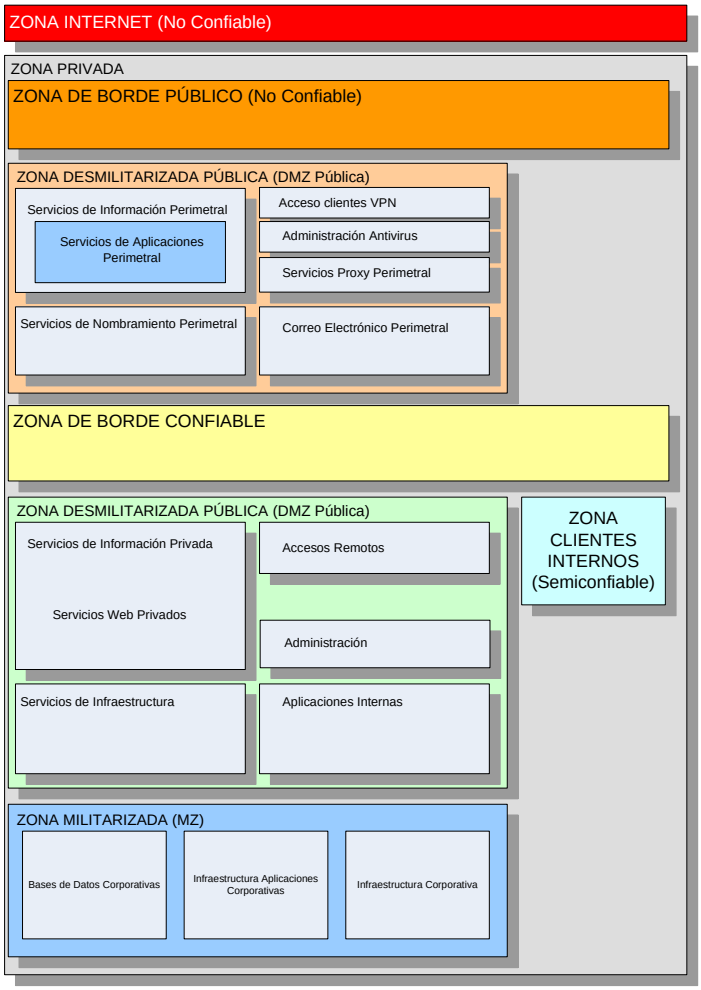


FIGURA 4.39 DEFINICIÓN DE LAS ZONAS DE SEGURIDAD

4.5.3 DEFINICIÓN DE LAS CAPAS DE SERVICIOS

En la Tabla XI se listan las capas que han sido definidas en la infraestructura tecnológica, con información más detallada al respecto:

TABLA XI

CAPAS DE SERVICIOS

Capa	Descripción
Firewall de borde (Público)	Interface externa en el Firewall de borde entre la Zona Internet y la Zona de Borde Público
Firewall de borde (Público)	Interface interna en el Firewall de borde entre la Zona de Borde Público, y, Servicios de Información Perimetral y Servicios de Nombramiento Perimetral.
Firewall de borde (Público)	Interface interna en el Firewall de borde entre la Zona de Borde Público y la Zona de Administración Antivirus.
Firewall de borde (Público)	Interface interna en el Firewall de borde entre la Zona de Borde Público y la Zona de Correo Electrónico Perimetral.
Firewall de borde (Público)	Interface interna en el Firewall de borde entre la Zona de Borde Público y la Zona de Servicios Proxy Perimetral.
Web Perimetral	Servicios http y componentes Web disponibles al público.
Aplicaciones Perimetrales	Servidores de aplicación para acceso público.
DNS Perimetrales	Servicios DNS disponibles para consultas públicas.
Directorio Perimetral	Servicios LDAP y certificados digitales disponibles para usuarios externos a la Institución (Actores suscritos a servicios integrados, Ej: proveedores)
Consola Antivirus	Servicios de actualización de definiciones de virus informáticos.
Proxies Perimetrales	Servicios Proxy transparente para reducción de tráfico de entrada y servicios de caching.
Correo Electrónico	Servicios de correo electrónico público
Firewall interno (Semiconfiable)	Interface externa en el Firewall interno entre la Zona Desmilitarizada Pública y la Zona de Borde Confiable

Capa	Descripción
Firewall interno (Semiconfiable)	Interface interna en el Firewall interno entre la Zona de Borde Confiable y Servicios de Infraestructura.
Firewall interno (Confiable)	Interface interna en el Firewall interno entre la Zona de Información Privada y la Zona Militarizada.
VPN	Servicios VPN para clientes y conexiones sitio a sitio.
Servicios Colaborativos	Servicios de mensajería electrónica estructurada y servicios colaborativos.
Servicios de computación remota	Servicios de terminales basados en computación remota con Citrix.
SQL Interno	Servidor de base de datos Oracle para clientes internos.
SQL	Servidor de base de datos MySQL para aplicaciones perimetrales y clientes externos
Servicios de nombramiento interno	Servicios DNS y WINS para resolución interna de nombres
Directorio interno	Servicios de directorio interno (Oracle Internet Directory) para uso interno.
Acceso Interno	Servicios de autenticación, autorización y registro basado en TACACS+.
Administración	Servicios de administración de la infraestructura (SNMP)
Acceso remoto	Servicios de acceso remoto por líneas telefónicas públicas y privadas bajo demanda.
Aplicaciones internas	Servidores de aplicación para acceso privado (Componentes web y servicios web).
Infraestructura aplicaciones internas	Servidores de aplicación para acceso privado (Componentes empresariales)
Infraestructura Corporativa	Servicios de respaldo de infraestructura y restauración para mantener recursos para recuperación de desastres.
Sitios remotos	Repartos en red con acceso remoto a la infraestructura central
Clientes	Dispositivos de acceso de los clientes

Posteriormente se determina que capas son parte de que Zonas de Seguridad. El resultado se muestra en la Figura 4.40:

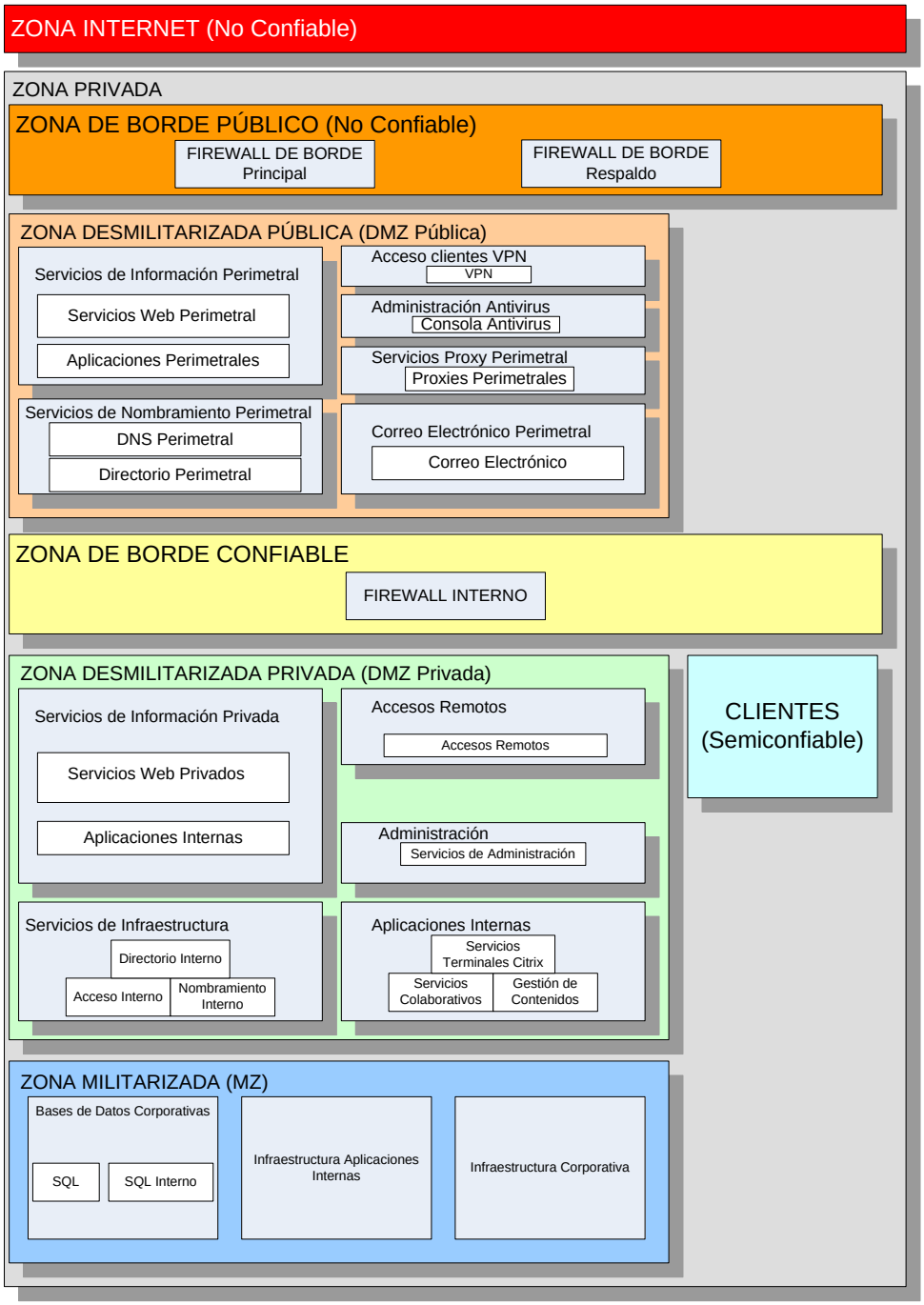


FIGURA 4.40 DEFINICIÓN DE LAS CAPAS DE SERVICIOS EN LAS ZONAS DE SEGURIDAD

Definidas las capas de servicios y ubicadas éstas dentro de cada zona de seguridad, es necesario tener a la mano la lista de puertos y los protocolos que emplean cada una de las aplicaciones específicas a fin de establecer las restricciones de tráfico entre las capas.

Para lograr filtrar el tráfico se pueden aplicar algunas técnicas disponibles. Típicamente se configuran los filtros de tráfico a nivel de Redes de Área Local Virtuales (VLAN), ya que con ello el diseño puede segmentar la red de manera lógica en zonas de seguridad y proveer así un modelo de seguridad más consistente, puesto que los computadores que conforman una misma VLAN normalmente comparten las mismas restricciones de tráfico.

Los filtros se pueden establecer de las siguientes formas:

- ✓ Regla de Firewall a nivel de VLAN o subred.
- ✓ Lista de Control de Acceso (ACL) en el ruteador a nivel de VLAN o subred.
- ✓ Regla de Firewall a nivel de computador.

- ✓ Lista de Control de Acceso (ACL) en el ruteador a nivel de computador.

- ✓ Regla en el computador para una interfaz específica.

4.5.4 DESEMPEÑO Y DISPONIBILIDAD REQUERIDA

Es necesario establecer el desempeño de red esperado y los requerimientos de disponibilidad para cada zona y capa.

Disponibilidad

En la Tabla XII podemos ver la representación del porcentaje de disponibilidad demandado, con su equivalencia en tiempo de caída máximo al año. Esto es útil para proponer esquemas de redundancia y alta disponibilidad en la infraestructura.

TABLA XII

REQUERIMIENTOS DE DISPONIBILIDAD DE SERVICIOS

# de 9s	% Disponibilidad	Caída Anual
2	99.000	3 días, 15 horas, 36 minutos
3	99.900	8 horas, 46 minutos
4	99.990	53 minutos
5	99.999	5 minutos

Por las características de consolidación de la infraestructura tanto para efectos de servicios Internet como servicios internos, se ha establecido como requerimiento que la infraestructura en general sea capaz de proveer una disponibilidad cercana a los 4 dígitos, es decir 99,95%, equivalente a 6 horas, 19 minutos de caída anual.

En la Tabla XIII se representa los niveles de desempeño demandados para cada zona principal:

TABLA XIII

NIVELES DE DESEMPEÑO DE LAS ZONAS DE SERVICIOS

Zona Fuente	Zona Destino	Ancho de Banda Promedio	Máxima Latencia Tolerada	Disponibilidad
Internet	Privada	1 Mbps	500 ms	99,95%
Borde Público	DMZ Pública	10 Mbps	200 ms	99,95%
Internet	Correo Electrónico Perimetral	256 Kbps	500 ms	99,99%
Sitios Remotos (Internet)	DMZ Pública	32 Kbps	500 ms	99%
Sitios Remotos (Intranet)	DMZ Privada	64 Kbps	200 ms	99,95%
Borde Confiable	DMZ Privada	10 Mbps	200 ms	99,5%
DMZ Privada	Infraestructura Aplicaciones Corporativas	100 Mbps	100 ms	99,95%

Zona Fuente	Zona Destino	Ancho de Banda Promedio	Máxima Latencia Tolerada	Disponibilidad
Aplicaciones Internas	SQL	100 Mbps	100 ms	99,95%
Infraestructura Aplicaciones Corporativas	SQL Interno	1000 Mbps	30 ms	99,99%
Clientes	DMZ Privada	10 Mbps	100 ms	99,9%

4.5.5 RESTRICCIONES DE COMUNICACIONES IMPUESTAS

En éste punto es necesario realizar una evaluación de cada requerimiento de comunicación de los servicios y aplicaciones, contra los riesgos de seguridad identificados; con el fin de establecer las limitaciones adecuadas minimizando el impacto en los servicios provistos.

Así mismo en la Tabla XIV, se establecen los siguientes roles de red, los que deben ser relacionados a cada uno de los segmentos de red:

- ✓ Conectividad
- ✓ Seguridad a través de servicios cortafuegos (Firewall)
- ✓ Balance de carga

TABLA XIV

ROLES DE RED POR SEGMENTO

Fuente	Destino	Rol	Rol ID	Razón
Internet	Privada	Conectividad	Ruteador de borde	Proveer conectividad entre el Internet y la Zona Privada.
Privada	DMZ Pública	Servicios cortafuegos	Servicios cortafuegos de borde	Cumplir con la política de seguridad institucional.
Privada	Sitios Remotos	Servicios cortafuegos	Servicios cortafuegos de borde	Cumplir con la política de seguridad institucional.
Dentro de la DMZ Pública		Conectividad	Switch de Perímetro	Proveer conectividad.
Dentro de Servicios de Información Perimetral		Balance de carga	Balanceo de carga de perímetro	Balancear la carga de los servidores Internet Web y aplicaciones perimetrales.
Dentro de Servicios de Nombramiento Perimetral		Balance de carga	Balanceo de carga de perímetro	Balancear la carga de los servidores DNS Perimetral.
Dentro de Servicios Proxy Perimetral		Balance de carga	Balanceo de carga de perímetro	Balancear la carga de los servidores Proxy Perimetral.
Dentro de Servicios Correo Electrónico Perimetral		Balance de carga	Balanceo de carga de perímetro	Balancear la carga de los servidores Correo Electrónico.
Sitios Remotos	DMZ Pública	Conectividad	Ruteador central / Ruteador remoto	Proveer conectividad entre los sitios remotos y el sitio central.
DMZ Pública	DMZ Privada	Servicios cortafuegos	Servicios cortafuegos de borde	Cumplir con la política de seguridad institucional.
DMZ Privada	MZ	Servicios cortafuegos	Servicios cortafuegos de borde	Cumplir con la política de seguridad institucional.
Dentro de la DMZ Privada		Conectividad	Switch Central	Proveer conectividad
Dentro de Servicios de Información Privada		Balance de carga	Balanceo de carga interno	Balancear la carga de los servidores Intranet Web y aplicaciones internas.
Dentro de Servicios de Infraestructura		Balance de carga	Balanceo de carga interno	Balancear la carga de los servidores de directorio interno (OID) y PKI.
Dentro de Servicios de Aplicaciones Internas		Balance de carga	Balanceo de carga interno	Balancear la carga de los servidores de aplicaciones internas Citrix.

Fuente	Destino	Rol	Rol ID	Razón
Clientes Internos	DMZ Privada	Conectividad	Switch central y Switch de distribución	Proveer conectividad de los segmentos de red al backbone.
Dentro de la MZ		Conectividad	Switch Gigabit Interno	Proveer conectividad

A continuación, en la Figura 4.41, se muestra el diagrama lógico de lo indicado en la Tabla anterior:

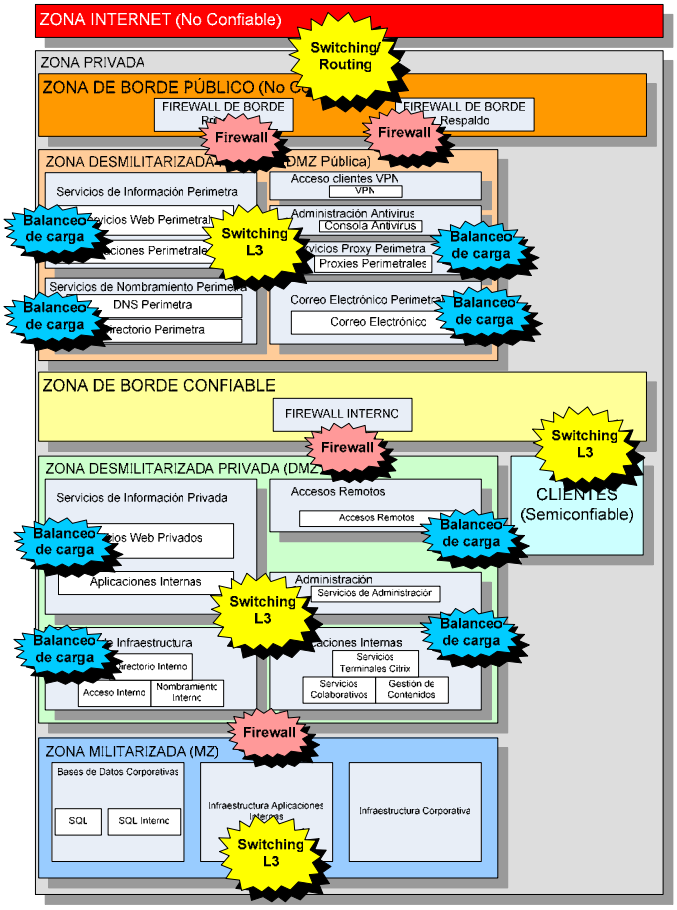


FIGURA 4.41 DIAGRAMA LÓGICO, CAPAS DE SERVICIOS Y ZONAS DE SEGURIDAD

Una vez añadidos los roles de red al diseño, debemos realizar la segmentación de la red para poder satisfacer las necesidades de las zonas de seguridad, las capas de aplicación y los host.

En el diseño propuesto cada zona de seguridad está representada por un segmento de red, en unos casos es física y en otros lógico (VLAN), excepto en aquellas situaciones donde no se considera práctico.

La segmentación de la red permitirá establecer de manera confiable el control de flujo de datos, manteniendo la disponibilidad necesaria para cumplir con los niveles de servicio requeridos.

Todos los segmentos de red en el diseño son lógicos (VLANs), excepto los segmentos que conectan la red de borde a los hosts de bastión perimetrales. Esto permitirá cumplir con el requerimiento de seguridad establecido de tener dispositivos físicos separados para la implementación de la conectividad en el borde. Adicionalmente se mejora la seguridad colocando switches perimetrales detrás de los host de bastión para evitar comunicación directa entre éstos switches y el ruteador de borde.

Se escogió la implementación de VLANs debido a su flexibilidad y facilidad de administración.

La segmentación propuesta se explica posteriormente en la Tabla XVIII, y se muestra posteriormente en la Figura 4.42:

TABLA XV

SEGMENTACIÓN PROPUESTA

ID Segmento de Red	Propósito del segmento	A que otro segmento es ruteado el tráfico a través de direcciones de capa 3?	Razón para la creación.
S1	Conectividad.	Solamente S2.	Así el tráfico puede ser ruteado entre la Red Naval de Datos y el Internet, como mecanismo de seguridad se requiere implementer los servicios de Firewall de borde y Proxy perimetral entre la Zona Internet y la Zona Privada. Se propone tales dispositivos lo que implica la creación de los segmentos S2, S3 y S7. En el diseño se decide un par de dispositivos específicos y separados para el servicio de firewall de perímetro, en configuración redundante activo – activo. Así mismo se opta por utilizar el dispositivo dedicado provisto por el proveedor (ISP) para funciones de conmutación y enrutamiento. Separar éstas funciones permitirá tener un mayor desempeño y tener flexibilidad para crecimiento futuro añadiendo más segmentos en el dispositivo ejecutando tareas de ruteo en el borde.
S2	Conectividad y Seguridad	Solamente S3	Las mismas razones que S1.
S3	Conectividad y Seguridad	S4, S5, S6, S7, S8 y S9	Para permitir el flujo de tráfico desde el dispositivo que desempeña el rol de conmutación en la Zona Desmilitarizada Pública (DMZ Pública) hasta los dispositivos que desempeñan el rol de servicio de

ID Segmento de Red	Propósito del segmento	A que otro segmento es ruteado el tráfico a través de direcciones de capa 3?	Razón para la creación.
			firewall. Así mismo, para permitir el flujo de tráfico desde los dispositivos que desempeñan el rol de servicio de firewall hasta los dispositivos que desempeñan los roles de servicios perimetrales de: web, aplicaciones, DNS, Directorio, Proxy, Correo Electrónico y Actualización Antivirus, en los segmentos S4, S5, S6 y S7. El diseño dispone que el dispositivo de conmutación de borde sea físicamente diferente que el equipo de conmutación de la DMZ Pública.
S4	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de servicios de firewall perimetral, y la capa de servicios web perimetral así como también permitir a los dispositivos de la zona cliente conectarse a los servidores en la capa web perimetral.
S5	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de servicios de firewall perimetral y la capa DNS perimetral, así como permitir a los dispositivos de la Zona Cliente conectarse a los servidores en la capa DNS perimetral para la resolución de nombre internos.
S6	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de servicios de firewall perimetral y el servicio de acceso a los clientes de redes privadas virtuales; al resto de la infraestructura como si fuese un usuario del semento S11.
S7	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de servicios de firewall perimetral y la Consola Antivirus, así como permitir a los dispositivos de la Zona Cliente la actualización de definición de virus desde la Consola.
S8	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de servicios de firewall perimetral y la capa Proxy perimetral, así como permitir a los dispositivos de la Zona Cliente conectarse a la Zona Internet a través de los servidores Proxy.
S9	Seguridad	S3 y S10	Para permitir el flujo de tráfico entre el dispositivo

ID Segmento de Red	Propósito del segmento	A que otro segmento es ruteado el tráfico a través de direcciones de capa 3?	Razón para la creación.
			que desempeña el rol de servicios de firewall perimetral, y la capa de servicios correo electrónico perimetral así como también permitir tanto a los dispositivos de la zona cliente conectarse a los servidores de correo electrónico, así como también al Servidor Colaborativo de la capa aplicaciones internas.
S10	Seguridad y Conectividad	S4, S5, S6, S7, S8, S9, S11 y S12	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de Switching en la Zona Desmilitarizada Pública y el dispositivo que desempeña el rol de servicios de firewall interno. Todos los servidores de las capas de servicios perimetrales de: información (Servicios y aplicaciones web), nombramiento (DNS y Directorio), Correo Electrónico, Proxy y Antivirus enrutan el tráfico a través del dispositivo que se desempeña con el rol de Switching de capa 3 en la Zona Desmilitarizada Pública, para comunicarse con la Zona Cliente. (Ciertos clientes en la zona cliente pueden conectarse a éstos servidores para realizar una administración remota.) El dispositivo de firewall interno debe ejecutar una inspección de paquetes del tipo stateful para controlar el tráfico de red entre la Zona Desmilitarizada Pública y la Zona Desmilitarizada Privada. Este dispositivo en conjunto con los dispositivos de firewall de perímetro, conforman un arreglo de dispositivos de seguridad en una configuración de defensa en profundidad.
S11	Seguridad	S10 y S12	Para permitir el tráfico entre la Zona cliente y las Zonas Desmilitarizadas Pública y Privada, para tener acceso tanto a servicios y aplicaciones públicas de Internet, como servicios y aplicaciones privadas de Intranet.
S12	Seguridad y Conectividad	S13, S14, S15, S16 y S17	Para permitir el tráfico entre el dispositivo desempeñando el rol de firewall interno y el dispositivo que desempeña el rol de switching de la Zona Desmilitarizada Privada. Por seguridad se dispone que el dispositivo que desempeña la función de switching en la Zona Desmilitarizada Pública debe ser físicamente diferente que el dispositivo que desempeña la función de switching

ID Segmento de Red	Propósito del segmento	A que otro segmento es ruteado el tráfico a través de direcciones de capa 3?	Razón para la creación.
			en la Zona Desmilitarizada Privada.
S13	Seguridad	S12, S14, S15, S16 y S17	Para permitir el tráfico entre el dispositivo desempeñando el rol de servicios de firewall interno y la capa de servicios de información privada (servidores web privados y aplicaciones privadas) y las aplicaciones internas (Servicios Citrix, Servicios Colaborativos y Gestión de Contenidos); así como también permitir a los dispositivos de la Zona Cliente conectarse a la capa de servicios de información privada. También permite la comunicación entre la capa de acceso remoto, la capa de servicios de infraestructura para acceso a los servicios de directorio corporativo, los servicios disponibles en la Zona Militarizada (MZ).
S14	Seguridad	S12, S13, S15, S16 y S17	Para permitir el tráfico entre los Servicios de Infraestructura (Directorio interno, acceso interno y nombramiento interno) y los Servicios de Información Privada, la zona de accesos remotos, las aplicaciones internas; así como también la Zona de Clientes.
S15	Seguridad	S12, S13, S14, S16 y S17	Para permitir el tráfico entre el servicio de accesos remotos y los servicios de información privada, los servicios de infraestructura y las aplicaciones internas.
S16	Seguridad	S12, S13, S14, S15 y S17	Para permitir el tráfico entre las diferentes capas y zonas y la capa de administración, habilitando el flujo de paquetes de los protocolos administrativos de manera estrictamente restrictiva hacia ésta capa.
S17	Seguridad y Conectividad	S13, S14, S15, S16 y S18	Para permitir el flujo de tráfico entre el dispositivo que desempeña el rol de Switching en la Zona Desmilitarizada Privada y el dispositivo que desempeña el rol de servicios de firewall interno. Todos los servidores de las capas de servicios privados de: información, (Servicios y aplicaciones web privadas), infraestructura (Directorio interno, Acceso TACACS/RADIUS y Nombramiento interno) y Acceso remoto, Aplicaciones Internas y administración, enrutan el tráfico a través del dispositivo que se desempeña con el rol de

ID Segmento de Red	Propósito del segmento	A que otro segmento es ruteado el tráfico a través de direcciones de capa 3?	Razón para la creación.
			Switching de capa 3 en la Zona Desmilitarizada Privada, para comunicarse con la Zona Cliente. (Ciertos clientes en la zona cliente pueden conectarse a éstos servidores para realizar una administración remota.) El dispositivo de firewall interno debe ejecutar una inspección de paquetes del tipo stateful para controlar el tráfico de red entre la Zona Desmilitarizada Privada y la Zona Militarizada.
S18	Seguridad y Conectividad	S17, S19, S20 y S21	Para permitir el tráfico entre el dispositivo desempeñando el rol de firewall interno y el dispositivo que desempeña el rol de switching de la Zona Militarizada. Por seguridad se dispone que el dispositivo que desempeña la función de switching en la Zona Militarizada debe ser físicamente diferente que el dispositivo que desempeña la función de switching en la Zona Desmilitarizada Privada.
S19	Seguridad	S17, S20 y S21	Para permitir el tráfico entre la Zona de Infraestructura de aplicaciones internas, la Infraestructura Corporativa y la Zona Desmilitarizada Privada (Exclusivamente Servicios de Información Privados y Administración) con la Zona de Bases de Datos Corporativas. Dentro de ésta Zona, a la Capa SQL pueden acceder exclusivamente la Capa de Servicios Públicos de Información basados en bases de datos, y a la Capa SQL Interno, exclusivamente la Capa de Servicios Privados de Información basados en bases de datos.
S20	Seguridad	S18, S19 y S21	Para permitir el tráfico entre la Zona Desmilitarizada Privada (exclusivamente la Zona Clientes y la capa de servicios de información privados que requieran acceso al servicio OID de Oracle), y la Zona de Infraestructura Corporativa a la Zona de Bases de Datos Corporativas.
S21	Seguridad	S18, S19 y S20	Para permitir el tráfico entre la Zona Desmilitarizada Privada (exclusivamente la Zona de Administración al servicio de administración de Oracle) a la Zona de Bases de Datos Corporativas pasando por la autenticación ante el Servicio OID de Oracle.

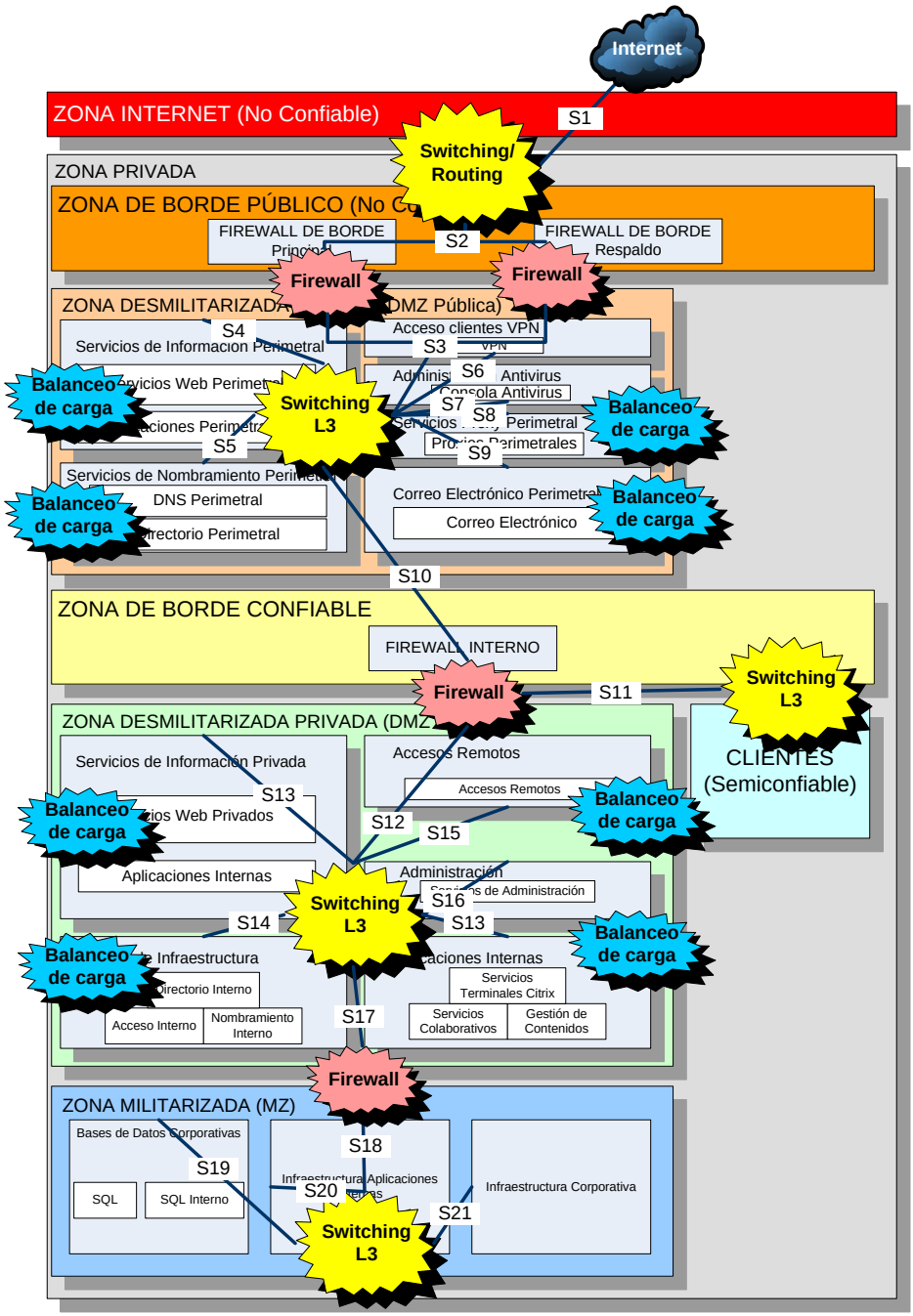


FIGURA 4.42 DIAGRAMA LÓGICO, CAPAS DE SERVICIOS, ZONAS DE SEGURIDAD Y ROLES DE RED

Una vez definidos los diferentes segmentos de red, proseguimos asignando los respectivos dispositivos de red que sean capaces de soportar los diferentes roles en cada segmento.

Conforme al diseño planteado, se requieren los siguientes roles:

- ✓ **Ruteador de borde.-** Rol entre las Zona Internet y la Zona Privada, dispositivo de capa 3 entre los segmentos S1 y S2.
- ✓ **Servicios de Firewall de borde.-** Rol entre los segmentos S2 y S3.
- ✓ **Balanceo de carga servicios de información públicos.-** Entre los host de la capa de servicios de información perimetral; segmento S4.
- ✓ **Balanceo de carga servicios DNS.-** Entre los host de la capa de servicios de nombramiento perimetral; segmento S5.
- ✓ **Balanceo de carga servicios Proxy perimetral.-** Entre los host de la capa de servicios Proxy perimetral; segmento S8.

- ✓ **Balanceo de carga servicios de correo electrónico.-** Entre los host de la capa de servicios de correo electrónico perimetral; segmento S9.

- ✓ **Servicios de conmutación perimetral.**- Rol para la Zona Desmilitarizada Pública (DMZ Pública) que controla el tráfico entre los segmentos S3, S4, S5, S6, S7, S8, S9 y S10.

- ✓ **Servicios de Firewall Interno.-** Rol entre los segmentos S10, S11 y S12.

- ✓ **Balanceo de carga servicios de información privados.-** Entre los host de la capa de servicios de información privada; segmento S13.

- ✓ **Balanceo de carga servicios de infraestructura.-** Entre los host de la capa de servicios de infraestructura: Directorio Corporativo Interno, AAA (TACACS+) y Nombramiento Interno; segmento S14.

- ✓ **Balanceo de carga servicios de aplicaciones internas.-** Entre los host de la capa de servicios de aplicaciones internas:

Citrix, Servicios Colaborativos y Gestión de Contenidos; segmento S13.

- ✓ **Servicios de conmutación privado.**- Rol para la Zona Desmilitarizada Privada (DMZ Privada) que controla el tráfico entre los segmentos S12, S13, S14, S15, S16 y S17.

- ✓ **Servicios de Firewall Interno Militarizado.-** Rol entre los segmentos S17 y S18.

- ✓ **Servicios de conmutación zona militarizada.**- Rol para la Zona Militarizada (MZ) que controla el tráfico entre los segmentos S18, S19, S20 y S21.

El diseño combina el uso de dispositivos consolidados y dispositivos especializados para cada Rol y/o Zona. De ésta manera se combina la ventaja de contar con un diseño flexible basado en los dispositivos multifunción, su facilidad de administración; con la seguridad de utilizar para ciertos roles dispositivos físicamente diferentes.

En un solo equipo para balanceo de carga se combinan los siguientes roles: servicios de información públicos, servicios DNS perimetrales, correo electrónico perimetral y Proxy perimetral.

En un equipo de similares características se combinan los siguientes roles de balanceo de carga: servicios de información privados, servicios de infraestructura y servicios de aplicaciones internas.

En el caso de los servicios de conmutación, necesitamos dispositivos físicos para cada zona: Zona Desmilitarizada Pública, Zona Desmilitarizada Privada y Zona Militarizada.

Los dispositivos de la DMZ Pública y MZ requieren soportar VLANs y filtros ACL. El dispositivo de la DMZ Privada es el switch principal del backbone de toda la Red de Campus de la Base Naval Sur.

Para los servicios de Firewall, de igual manera se emplean dispositivos físicos separados. Para el rol Firewall de borde se utilizan dos equipos con capacidad de trabajar juntos siendo uno respaldo del otro en caso de fallas, estos equipos tienen varios puertos para dar mayor flexibilidad; para los roles de Firewall

interno e interno militarizado, tenemos equipos con cuatro y tres zonas respectivamente.

Los equipos a emplearse en el Data Center, se presentan en la Figura 4.43:

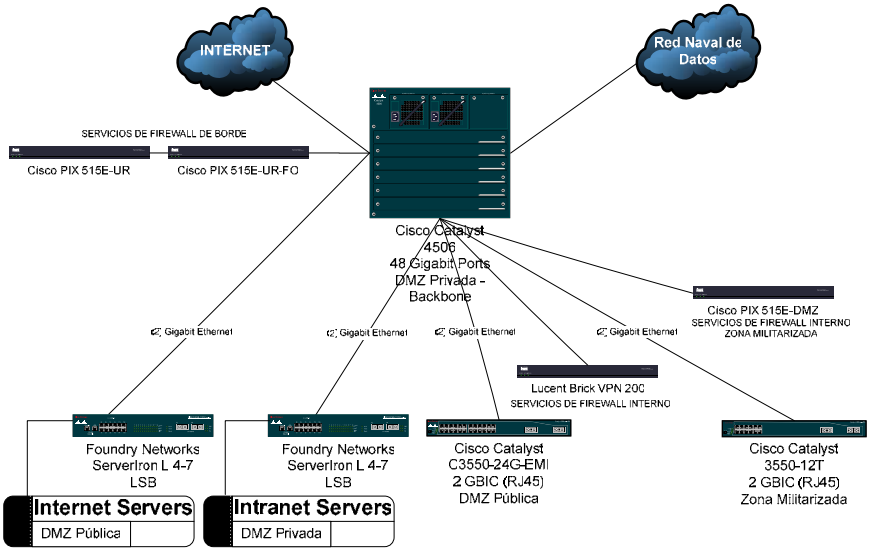


FIGURA 4.43 EQUIPOS DE RED PARA EL DATA CENTER

4.5.6 RED DE CAMPUS DE LA BASE NAVAL SUR (GUAYAQUIL)

El diseño modular de la red planteado, permitirá que la red de datos se ajuste tanto a las necesidades presentes como futuras de la Armada. A nivel del Data Center se tienen la diversidad de roles de red debido a la concentración de servicios a los cuales acceden

principalmente los usuarios, pero en los segmentos de red que conforman la Zona de Clientes Internos, solo tenemos el rol de conmutación que obedece a diferentes niveles funcionales. Pese a que inicialmente se han establecido como requerimiento aplicaciones basadas en servicios IP tradicionales, el diseño deberá tener la suficiente flexibilidad para soportar otro tipo de aplicaciones como:

- ✓ Servicios multicast (Video conferencia – webcasting)
- ✓ Servicios con calidad de servicio diferenciada (QoS)
- ✓ Servicios de seguridad (Basados en ACLs)
- ✓ Facilidad de administración.

Para ello atendiendo a la realidad geográfica y distribución de edificios en la Base Naval Sur, sector geográfico donde se concentra la mayor cantidad de usuarios de la Armada, se ha implementado una Red de Campus, basada en un backbone de fibra óptica horizontal de alta velocidad en forma de delta, al cual se conecta el switch principal y los dos switches de distribución. Estos tres equipos forman un delta para evitar puntos únicos de

falla en las rutas, por los cuales se distribuye los paquetes a las diferentes VLANs a las que pertenecen los diferentes usuarios. Estos switches tienen acceso al backbone a través de interfaces Gigabit. Debido a que usuarios que se encuentran en diferentes edificios pertenecen a la misma VLAN, es necesario propagar la información de las VLAN entre los switches, razón por la cual será necesario implementar el protocolo VLAN Trunking Protocol (VTP). De igual manera, en la red existen dispositivos que deben ser vistos por todas las VLANs creadas (Ej: Servidores Citrix) por lo que necesitan estar en los mismos dominios de broadcast de todas las VLANs; para esto se habilitará trunking en los switches, para que determinados puertos pertenezcan a varias VLANs. Se utilizará el protocolo de etiquetamiento de paquetes (tagging) ISL, soportado por los equipos Cisco. En los switches del backbone está configurado el protocolo PVST (Per VLAN Spanning Tree) con el fin de evitar lazos en el delta, teniendo únicamente una ruta habilitada, pero en caso de fallas el protocolo detectará automáticamente el problema y la red tendrá una convergencia rápida.

En la Figura 4.44 se muestra el esquemático de lo dicho:

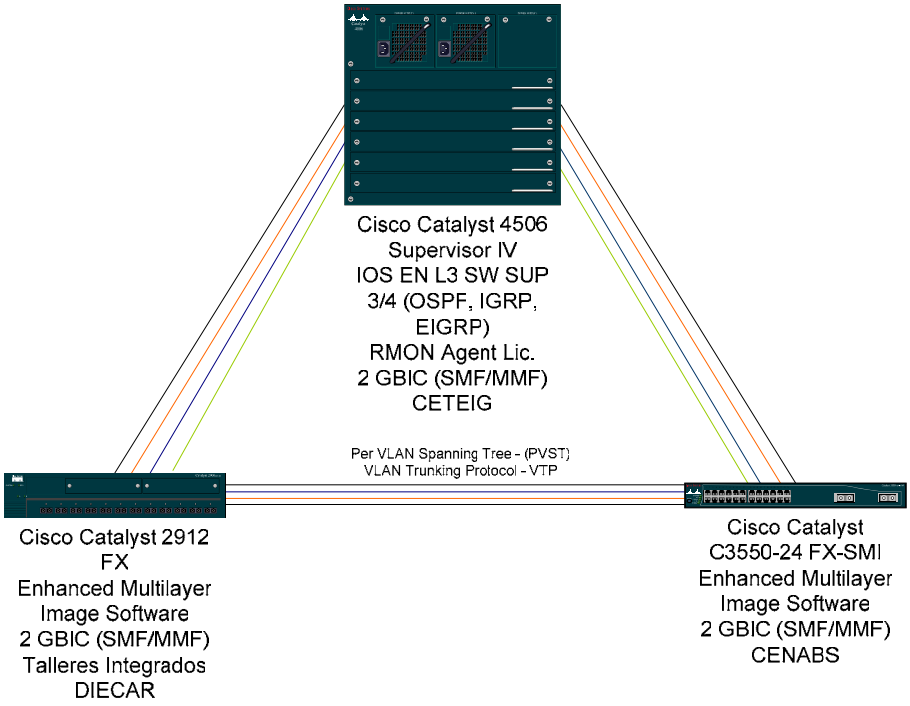


FIGURA No. 4.44 CAPA DE DISTRIBUCIÓN DE LA RED DE CAMPUS DE LA BASE NAVAL SUR

A los switches de la capa de distribución se conectan los switches de la capa de acceso en una topología física de estrella. Estos switches en su mayoría soportarán VLANs, siempre y cuando accedan directamente a través de la red de fibra óptica. En los casos que se accede a través de infraestructura de cobre de

categoría 3, con extensores de LAN, se administra la VLAN a nivel del puerto de la capa de distribución.

En la Figura 4.45 se muestra el esquema para interconectar los equipos de la capa de acceso del Sector Sur de la Base Naval Sur, a la capa de distribución:

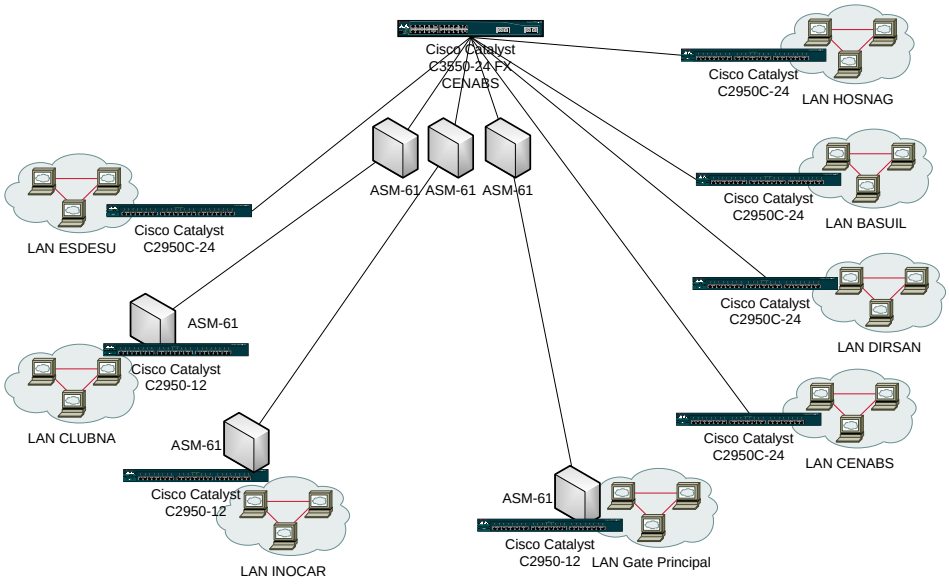


FIGURA 4.45 CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR SUR

En la Figura 4.46 se muestra el esquema para interconectar los equipos de la capa de acceso del Sector del Área Operativa de la Base Naval Sur, a la capa de distribución:

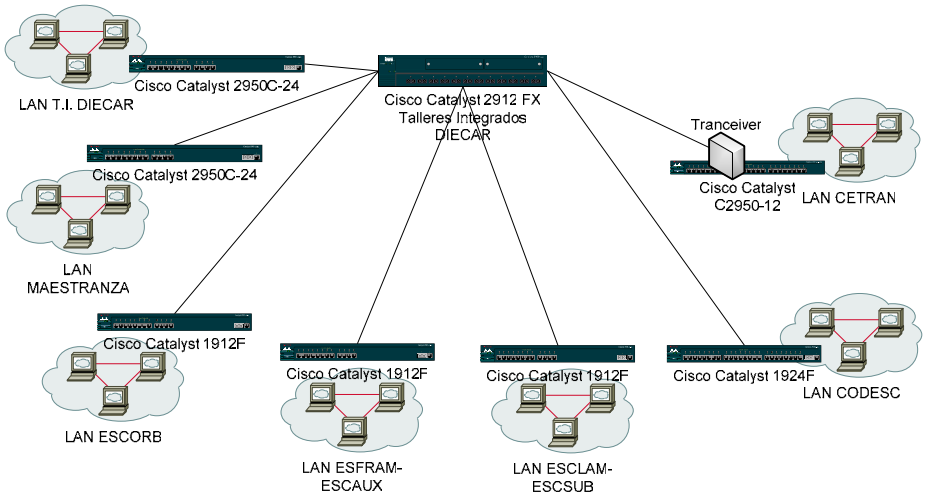


FIGURA 4.46 CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR DEL ÁREA OPERATIVA

En la Figura 4.47 se muestra el esquema para interconectar los equipos de la capa de acceso del Sector Noroccidental y Edificio de la Dirección General del Personal de la Base Naval Sur, a la capa de distribución:

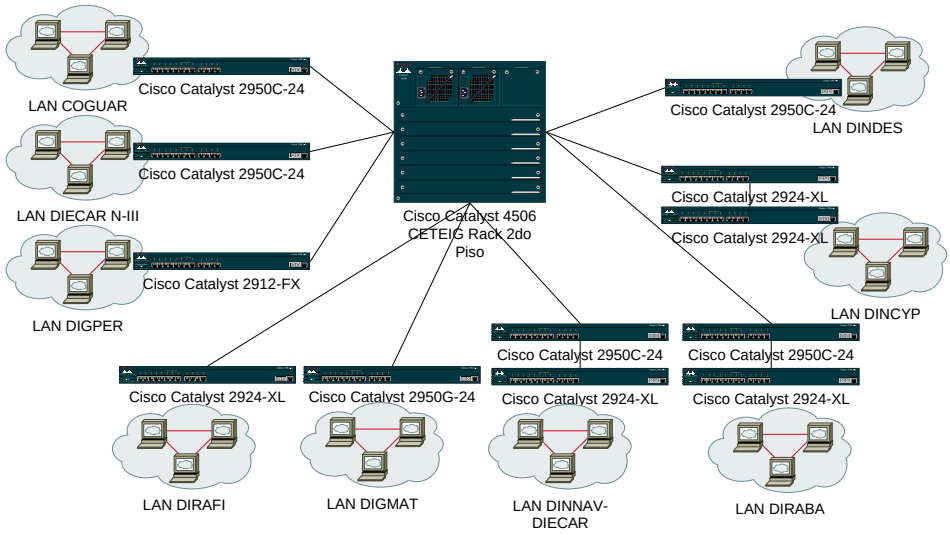


FIGURA 4.47 CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR NOROCCIDENTAL Y EDIFICIO DE LA DIRECCIÓN GENERAL DEL PERSONAL

Red Inalámbrica de la Base Naval Sur

La interconexión de las Unidades de Superficie y Submarinas que se encuentran en los muelles de la Base Naval Sur, no podía resolverse por medios guiados, debido especialmente a las adversidades del medio, y a las características físicas de los muelles, en donde no resultaba práctico emplear medios guiados como cobre o fibra óptica.

Con el desarrollo de la tecnología de redes inalámbricas, surgió como alternativa el empleo de tal tecnología, sin embargo, los movimientos a los que se ven sometidos los buques en todos los sentidos, por efecto de las mareas y corrientes, no facilitaban para el empleo de equipos comunes, por lo que fue necesario emplear una red inalámbrica basada en equipos que tengan características NLOS (No Line Of Sight).

La solución consiste en una celda sectorial que cubre gran parte de la Base Naval Sur, dentro de la cual se colocan radio modems que sin necesidad de mantener un línea de vista permanente con la base de la celda, puede funcionar proveyendo enlaces de 2 Mbps. El sistema está basado totalmente en IP, y provee mecanismos de seguridad con autenticación de 128 bits.

En la Figura 4.48, se muestra el esquemático de la solución implantada:

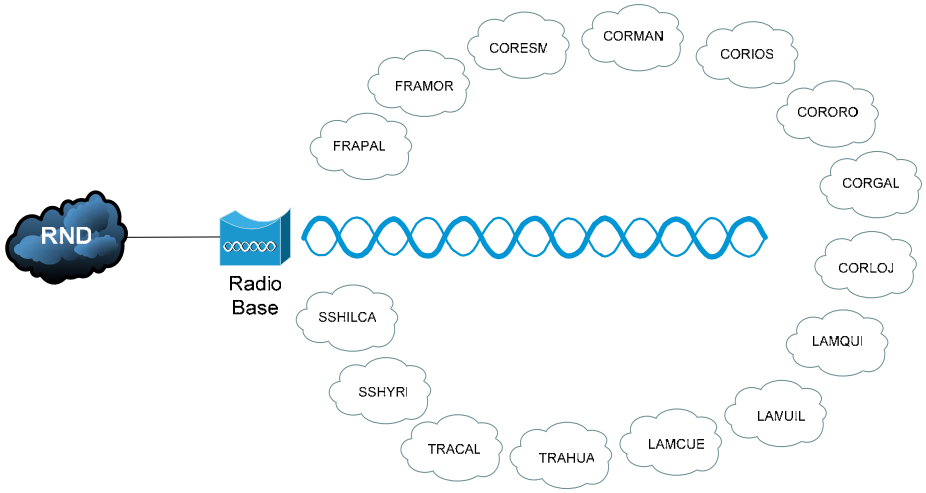


FIGURA 4.48 RED INALÁMBRICA TIPO NLOS PARA LAS UNIDADES DE SUPERFICIE Y SUBMARINAS

4.5.7 REDES DE CAMPUS MENORES

En otras Bases e Instalaciones Navales, donde pese a no existir gran cantidad de repartos navales, pero debido a su importancia o a la distribución geográfica de los usuarios dentro de éstas, ha sido necesario implementar redes de campus que integren las diferentes redes de área local ya existentes.

1. Red de Campus de la Comandancia General de Marina

Este Campus ubicado dentro del Complejo Ministerial de Defensa en Quito, alberga a tres edificios contiguos de la

Armada; entre los cuales se cuenta con una infraestructura de cableado estructurado categoría 5. Estos edificios son: Comandancia General de Marina, Dirección General de Finanzas y Estación Naval de Quito. En el subsuelo de la Estación Naval de Quito, se encuentra el Centro de Tecnología de Información de Quito, donde existe una infraestructura menor de procesamiento que sirve como respaldo al Centro de Tecnología de Información de Guayaquil; el Centro de Tecnología de Información de Quito es el principal centro de procesamiento para el Sistema Financiero de la Armada. En éste Centro se implementa el backbone colapsado del Campus, tal como se muestra en la Figura 4.49:

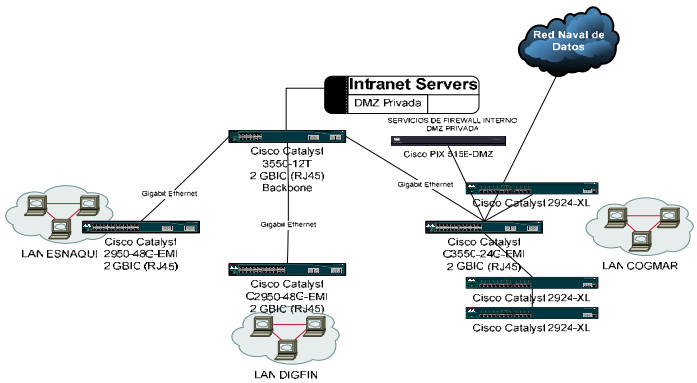


FIGURA 4.49 RED DE CAMPUS DE LA COMANDANCIA GENERAL DE MARINA Y ACCESO A LA RED NAVAL DE DATOS

2. Red de Campus de la Base Naval Norte

Al estar en ésta Base, los principales Institutos Académicos de la Armada, y por tanto requerir acceso con suficiente ancho de banda al Internet, en éste Campus tenemos un acceso directo al Internet, el mismo que será detallado más adelante en la sección correspondiente.

En la Base Naval Norte tenemos que el punto de acceso a la red naval de datos, está en la sala de radio. A esta sala de radio, están integrados todos los repartos de la Base a través de cable de cobre categoría 3, que es el empleado para la telefonía del Sistema de Conmutación de Fuerzas Armadas. La solución prevista es integrar a las redes de área local ya existentes, a través de extensores de LAN por cobre en una topología física tipo estrella, y proveer un segmento de distribución tanto al Internet como a la red naval de datos. El modelo esquemático de la solución propuesta, se muestra en la Figura 4.50:

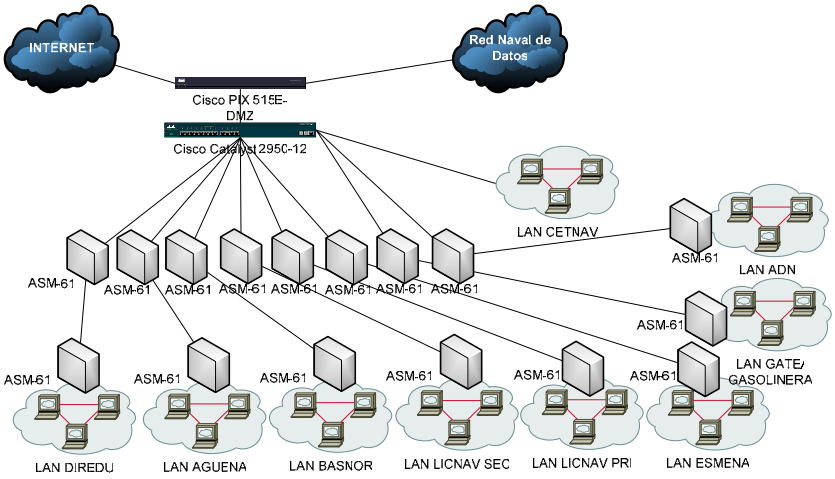


FIGURA 4.50 RED DE CAMPUS DE LA BASE NAVAL NORTE Y ACCESO A INTERNET Y A LA RED NAVAL DE DATOS

3. Red de Campus de la Base Naval de Salinas

En ésta Base está la Escuela Superior Naval y la Escuela de Grumetes, siendo además una importante Base de apoyo logístico. Requiere acceso con suficiente ancho de banda al Internet por lo que se tiene un acceso directo al Internet, el mismo que será detallado más adelante en la sección correspondiente.

En la Base Naval de Salinas tenemos que el punto de acceso a la red naval de datos, está en la sala de radio; a ésta están integrados todos los repartos de la Base a través de fibra óptica y

cable de cobre categoría 3, que es el empleado para la telefonía del Sistema de Conmutación de Fuerzas Armadas. La solución prevista es integrar a las redes de área local ya existentes, a través de la fibra óptica y de extensores de LAN por cobre en una topología física tipo estrella, y proveer un segmento de distribución tanto al Internet como a la red naval de datos. En la Figura 4.51 se muestra la solución propuesta:

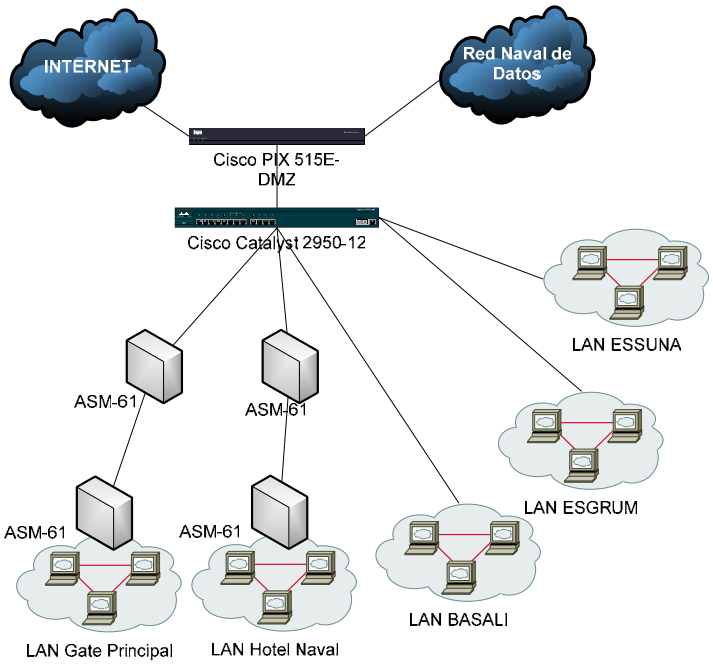


FIGURA 4.51 RED DE CAMPUS DE LA BASE NAVAL DE SALINAS Y ACCESO A INTERNET Y A LA RED NAVAL DE DATOS

4.5.8 REDES DE ÁREA LOCAL

En los diferentes repartos que tienen acceso a la red naval de datos, existen implantadas diferentes redes de área local, en su mayoría basadas en switches de capa 2 marca Cisco. Prácticamente no hay redes que empleen concentradores. Al momento de implantar el diseño, todas las redes deberán modificar su direccionamiento, para establecer un solo esquema de direccionamiento para toda la red.

A estas redes de área local, se las interconectará a la red naval de datos a través de un ruteador con las interfaces debidas según sea el sistema de transmisión que esté disponible en cada caso. El esquema de interconexión o red de área extendida se tratará más adelante.

Las redes de área local existentes y no mencionadas previamente son las siguientes: Comando de Operaciones Navales, Inspectoría General de la Armada, Dirección de Bienestar, Dirección General de Marina Mercante y del Litoral, Aviación Naval, Cuerpo de Infantería de Marina, Instituto de Historia Marítima, Dirección de Empresas de la Armada, Base Naval de Jaramijó, Comando de

Operaciones Norte, Batallón de Infantería de Marina Esmeraldas, Batallón de Infantería de Marina de San Lorenzo, Compañía de Infantería de Marina Jambelí, Dirección General de Intereses Marítimos, Capitanía de Puerto de Esmeraldas, Capitanía de Puerto de Manta, Capitanía de Puerto de Salinas, Capitanía de Puerto de Guayaquil, Capitanía de Puerto Bolívar y Superintendencia Petrolera de Balao.

4.5.9 RED DE ÁREA EXTENDIDA

Los diferentes esquemas de acceso empleados en la Red de Área Extendida dependen del tipo de tecnología disponible a nivel de transmisión.

Como medio de transmisión se empleará el Sistema de Comunicaciones del Comando Conjunto de las Fuerzas Armadas o Red MODE.

Éste sistema está compuesto por cuatro subsistemas, tres de los cuales son de nuestro interés para la red de área extendida:

1. Sistema de transmisión PDH

Es un sistema basado en microondas con cobertura nacional, conformado por cuatro anillos: Central, Nororiental, Occidental y Sur. Cada anillo tiene una configuración de 2+1 enlaces activos y Stand by E3 (34 Mbps); es decir una capacidad total de 102 Mbps. Para los repartos navales que están bajo la cobertura del sistema PDH se puede utilizar directamente el sistema de transmisión, con interfaces seriales de alta velocidad E1 (2 Mbps). La interface física es tipo BNC de 75 Ohmns no balanceada.

2. Sistema de Conmutación Digital

Es un sistema de telefonía digital ISDN, conformado por cuatro centrales principales: Quito, Guayaquil, Coca y Machala. Éstas operan con módulos distribuidos llamados ACT. Cada ACT necesita para su operación normal un enlace E1 principal y un enlace E1 de respaldo, sin embargo la topología física de la red del sistema de transmisión entrega cuatro enlaces E1 en donde hay un ACT. Para éstos repartos siempre que no justifique el empleo directo de un enlace de alta velocidad del sistema de

transmisión se puede emplear enlaces ISDN de 128 Kbps, o enlaces “n x 64 Kbps”. La interfaz física es tipo RJ45.

3. Sistema de Multiacceso

El sistema multiacceso es un sistema de telefonía rural de bajo costo. Emplea enlaces de 64 Kbps. Los repartos que están bajo la cobertura de éste sistema pueden emplear entre uno y dos enlaces de 64 Kbps individuales. La interfaz física es G.703.

4. Topología de la red

La red de área extendida de la red naval de datos, por emplear como sistema de transmisión la Red MODE que es esencialmente una red telefónica, es una red tipo estrella.

Se define un nodo principal en la Base Naval Sur (CETEIG) debido a la alta concentración de repartos navales en éste lugar y por estar ahí ubicado el principal Data Center. El nodo secundario viene a ser la Comandancia General de Marina (CETEIQ), por estar ubicado ahí el Data Center secundario. Al Nodo del CETEIG se conectan los repartos ubicados en la región suroccidental del país, que son la mayoría de repartos de

la Armada; al nodo del CETEIQ se conectan los repartos ubicados en la región nororiental del país.

En la Figura 4.52 y 4.53, se muestran la topología de la Red de Área Extendida dependiente del Centro de Tecnología de Información Guayaquil (CETEIG), y del Centro de Tecnología de Información de Quito (CETEIQ) respectivamente:

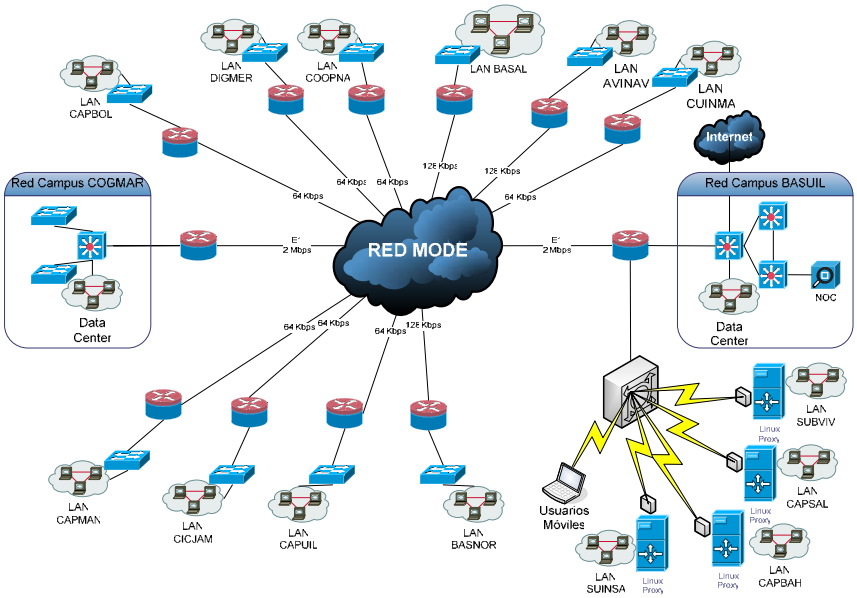


FIGURA 4.52 TOPOLOGÍA FÍSICA DE LA RED DE ÁREA EXTENDIDA CON DEPENDENCIA DEL NODO CETEIG – REGIÓN SUROCCIDENTAL

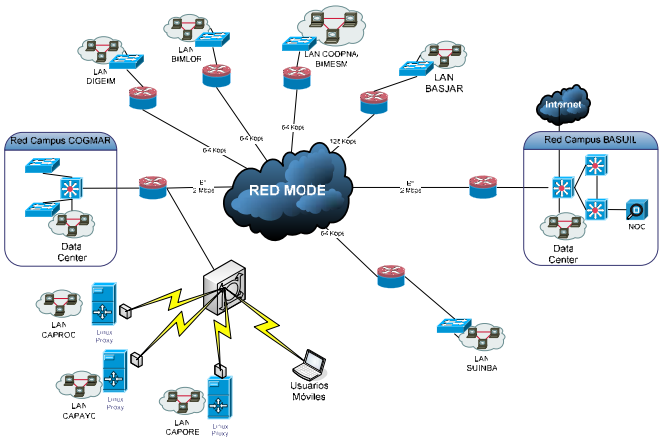


FIGURA 4.53 TOPOLOGÍA FÍSICA DE LA RED DE ÁREA EXTENDIDA CON DEPENDENCIA DEL NODO CETEIQ – REGIÓN NORORIENTAL

5. Enlaces Dedicados ISDN

Los siguientes repartos emplean enlaces ISDN de 128 Kbps por estar bajo la cobertura del sistema de conmutación: BASNOR, BASJAR, AVINAV y BASALI. Todos con excepción de BASJAR se conectan al nodo del CETEIG. BASJAR se conecta al nodo del CETEIQ. Las interfaces ISDN o Terminal Adapters (TA) son propietarios de Alcatel dentro de los cuales viene la tarjeta S0 propietaria también. En la Figura 4.54 se muestra el esquema previsto:

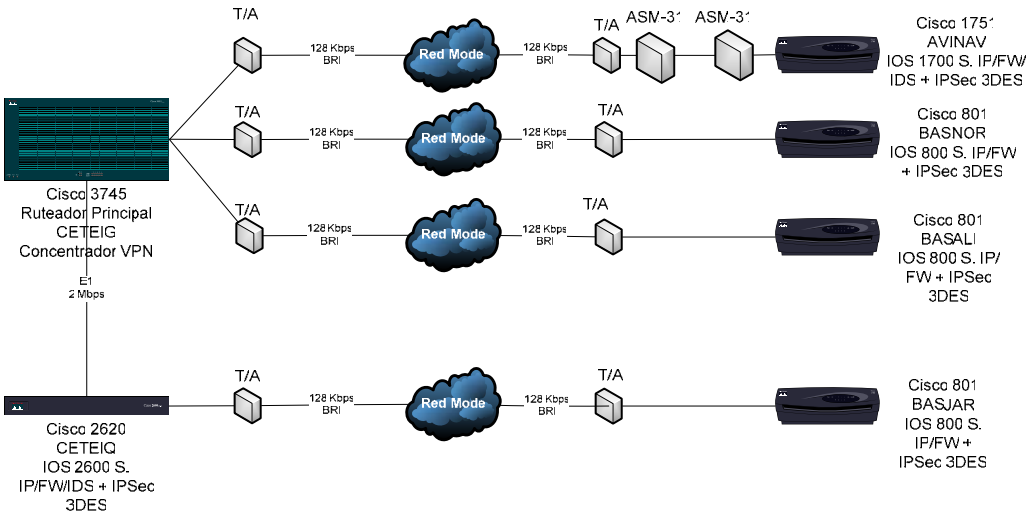


FIGURA 4.54 ESQUEMA DE ACCESO DE LOS REPARTOS CON ENLACES ISDN A LA RED NAVAL DE DATOS

6. Enlaces Dedicados Multiacceso

Los siguientes repartos emplean enlaces seriales de 64 Kbps por estar bajo la cobertura del sistema multiacceso: COOPNA/INSGAR/DIRBIE, CUINMA, CICJAM, DIGMER/INHIMA/DIREMP, COOPNO, DIGEIM, BIMESM y BIMLOR. Los cuatro primeros se conectan al nodo del CETEIG, los cuatro restantes se conectan al nodo del CETEIQ. Se emplean ruteadores con interfaces seriales de baja velocidad que utilizan convertidores de interfaz y velocidad G.703 a V.35.

En la Figura 4.55 se muestra el esquema de los equipos a emplear:

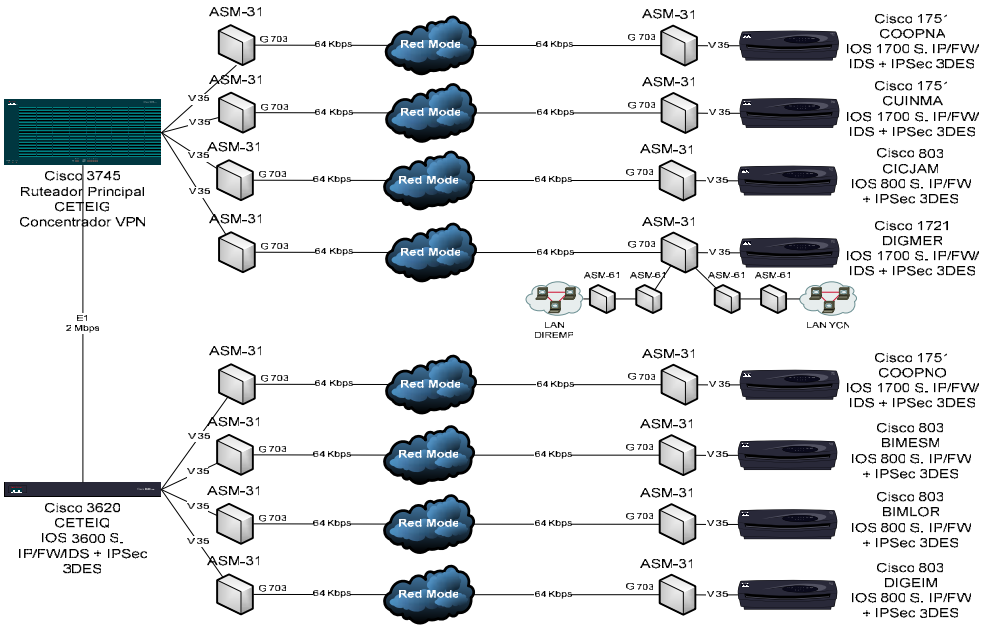


FIGURA 4.55 ESQUEMA DE ACCESO DE LOS REPARTOS CON ENLACES SERIALES POR EL SISTEMA MULTIACCESO A LA RED NAVAL DE DATOS

7. Enlaces E1

Por el momento únicamente está considerado el enlace Quito – Guayaquil con un circuito E1, a pesar de que existe el interés de habilitar este tipo de enlaces con la Base Naval Norte y la Base Naval de Salinas. Hay que considerar que al ser la Red

MODE una red militar, ésta es redundante, segura y de alta disponibilidad. Si a futuro se puede cambiar el sistema de comunicación con el Comando de Operaciones Navales y la Dirección General de Marina Mercante y del Litoral, que actualmente tienen cobertura del sistema multiacceso, a un esquema diferente, se deberá revisar también la posibilidad de proveer mayor ancho de banda en éstos lugares.

En la Figura 4.56 se muestran los equipos requeridos para el enlace E1 Quito – Guayaquil:

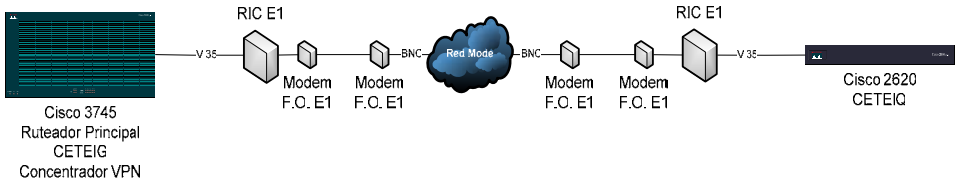


FIGURA 4.56 ESQUEMA DE INTERCONEXIÓN DE QUITO – GUAYAQUIL A TRAVÉS DEL ENLACE E1

8. Enlaces en demanda

Existen ciertos repartos que por su importancia y debido a la limitación de enlaces dedicados disponibles en la Red MODE, emplean una extensión telefónica digital o analógica del

subsistema de conmutación o multiacceso respectivamente, como medio de acceso en un esquema bajo demanda (dial-up). Para esto se han establecido servidores de comunicación basados en Linux, con modems analógicos, por el lado del sitio remoto; y servidores de acceso en los Centros de Tecnología de Información de Quito y Guayaquil. Empleando ésta misma infraestructura, también se brinda acceso a usuarios móviles y usuarios específicos que tienen autorización para acceder desde sus hogares. (VIPs y Administradores). En la Figura 4.57 se muestra el esquema de la solución en demanda:

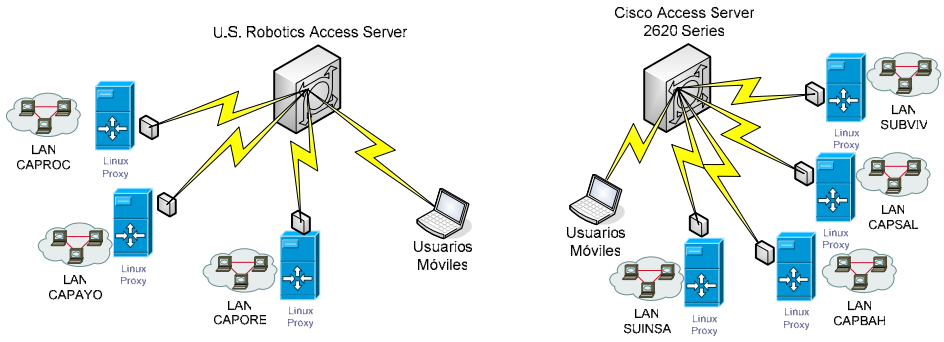


FIGURA 4.57 ESQUEMA DE ACCESO EN DEMANDA A TRAVÉS DE SERVIDORES DE ACCESO

4.5.10 ACCESO A INTERNET

El Internet representa el desarrollo tecnológico más importante de los últimos tiempos. Su efecto puede sobrepasar pronto a la televisión y competirá con seguridad luego con los medios impresos. Como desarrollo tecnológico es un fenómeno evolutivo, pero que poco a poco trae consigo efectos revolucionarios relacionados con casi todos los aspectos de las vidas de las personas, y por tanto de las organizaciones, que van desde la forma de realizar el trabajo, comunicarse, hacer adquisiciones, estudiar, aprender, informarse e informar.

El acceso al Internet es vital puesto que debidamente gestionado conforma un componente fundamental de un sistema de información comunicacional que habilita a los miembros de la Institución con el acceso a la mayor fuente de información disponible en el planeta, lo que a su vez se convierte en un inductor de innovación.

Pero el acceso al Internet debe ser provisto de manera esencialmente segura. Para ello, además de colocar mecanismos de protección como firewalls en varias líneas en

profundidad, es necesario combinar otros mecanismos como la detección de intrusos (IDS) e implementar procesos específicos a la seguridad de la información. El servicio de firewall perimetral está implementado en una configuración redundante bajo una configuración activo – pasivo; lo que permite en caso de fallas del equipo principal, automáticamente recuperar las sesiones por parte del equipo alterno manteniendo la disponibilidad del servicio.

Los ruteadores a emplear en los diferentes nodos remotos de la Red Naval de Datos, traen como característica adicional del sistema operativo, el Firewall para proteger a las redes de posibles accesos no autorizados o ataques provenientes de otra red (asumiendo que una red ha sido atacada). Esto incluye el ruteador principal.

Es necesario además implantar sistemas de detección de intrusos que permita monitorear cualquier comportamiento sospechoso de visitantes foráneos y locales a la Red Naval de Datos. Al establecer los sistemas IDS antes y después del firewall, logramos monitorear a ambos tipos de usuarios. Un sistema IDS tiene un funcionamiento similar a una herramienta

antivirus, es decir opera basado en firmas o patrones de ataques conocidos. Los tipos de ataque que un IDS detecta son:

- ✓ Exploits.- Actividad indicativa de que alguien está intentando ganar acceso o comprometer un sistema dentro de la red, tal como un BackOrifice, intentos de login fallidos y TCP hijacking.

- ✓ DoS.- Actividad indicativa de que alguien está intentando consumir ancho de banda o recursos computacionales para interrumpir las operaciones normales, tales como Trinoo, TFN y SYN floods.

- ✓ Reconnaissance.- Actividad indicativa de que alguien prueba o mapea la red para identificar “blancos de oportunidad”, tales como puertos abiertos; está actividad suele anteceder como hemos dicho a un intento de acceso a la red.

- ✓ Missuse.- Actividad indicativa de que alguien trata de violar la política de seguridad establecida. Esto se puede lograr configurando el IDS para chequear cadenas de caracteres personalizadas en el tráfico de la red; por ejemplo se puede configurar el IDS para enviar una alarma y eliminar la conexión

si se transmite las palabras “Secretísimo”, “Secreto”, “Reservado” en un email o en un FTP.

Los ruteadores a emplear en los nodos remotos que están expuestos a mayores riesgos como las Redes de Campus de la Base Naval Norte y de la Base Naval de Salinas, así como la Comandancia General de Marina, el Cuerpo de Infantería de Marina, y la Dirección General de Marina Mercante, incluyen como característica adicional del sistema operativo el IDS. En el caso del ruteador principal, se incluye un módulo de red especial para ejecutar el IDS principal basado en hardware y software.

Otro mecanismo de seguridad empleado es AAA. Autenticación que permite determinar la identidad de un usuario y verificación de la información. La Autorización que define lo que un usuario autenticado puede hacer, manteniendo un registro de lo que el usuario está haciendo. Y la Contabilidad (Accountability) que constituye la acción de controlar lo que un usuario hace. Para esto se implementa un servidor AAA dentro de la Zona de Infraestructura, en la Capa de Accesos Internos. El software empleado para el servidor AAA es el Cisco Secure Access Control (CSACS).

1. Redes Privadas Virtuales (VPNs)

Al ser la Red Naval de Datos una red militar, debe permitir el intercambio de información confidencial entre diferentes usuarios. La red por lo tanto debe ser lo suficientemente segura para garantizar la confidencialidad y la integridad de la información. Pese a que los sistemas de transmisión empleados forman parte de una red militar estratégica, como es la Red Mode, que de por sí incluye mecanismos sofisticados de seguridad, es necesario garantizar la confidencialidad de la información en el interior de la Institución. De igual manera se prevé conexiones de usuarios móviles a través de redes telefónicas públicas o Internet, así como también de las agregadurías navales en el exterior.

Para resolver los casos de las agregadurías navales en el exterior, se ha considerado el empleo de firewalls en cada una de ellas de modo que puedan habilitar una VPN con el concentrador VPN de la Red Naval de Datos, en éste caso la tarjeta aceleradora VAC+ en los Firewall perimetrales. Con esto se logra que los usuarios de las agregadurías puedan acceder

de manera transparente a los servicios de la Red Naval de Datos a través del Internet de manera segura y confiable.

Para el caso de los Oficiales en Comisión en el exterior que requieran tener acceso a los servicios de la Red Naval de Datos, se lo realiza a través de un cliente VPN que haga de Terminal de la VPN, puede ser el cliente VPN de Cisco, ó IPSec de Windows. En éste caso los Oficiales obtienen acceso a través de un ISP en el exterior, habilitando el acceso a través de su software VPN cliente empleando un certificado digital y su clave de acceso, de tal manera que se habilita un túnel encriptado y el usuario puede acceder a los recursos de la Red Naval de Datos de manera segura y confiable. Para soportar estos accesos también se emplean los recursos del concentrador VPN (VAC+) de los firewall perimetrales.

Para el caso de los nodos remotos que acceden a través de la Red de Área Extendida a los recursos centrales de la red naval de datos, se habilitan a través del sistema operativo Cisco IOS la característica adicional de cliente IPSec Cisco Secure, y se emplea un concentrador a manera de tarjeta aceleradora (VAC+) en el ruteador central.

Para el caso de los accesos remotos a través de las redes telefónicas públicas, se emplea un cliente VPN que haga de Terminal de la VPN, puede ser el cliente VPN de Cisco, ó IPSec de Windows. En éste caso el Terminal es el software IPSec del servidor de acceso.

En términos generales las conexiones desde las agregadurías navales en el exterior y desde los nodos remotos a través de la red Mode, son VPN dedicadas. Las conexiones de usuarios móviles tanto en el exterior a través de Internet, como en el país a través de las redes telefónicas públicas, son VPN en demanda.

En la Figura 4.58 se muestra el modelo funcional de los mecanismos de seguridad de red empleados, de modo que se pueda utilizar el Internet de manera segura y confiable:

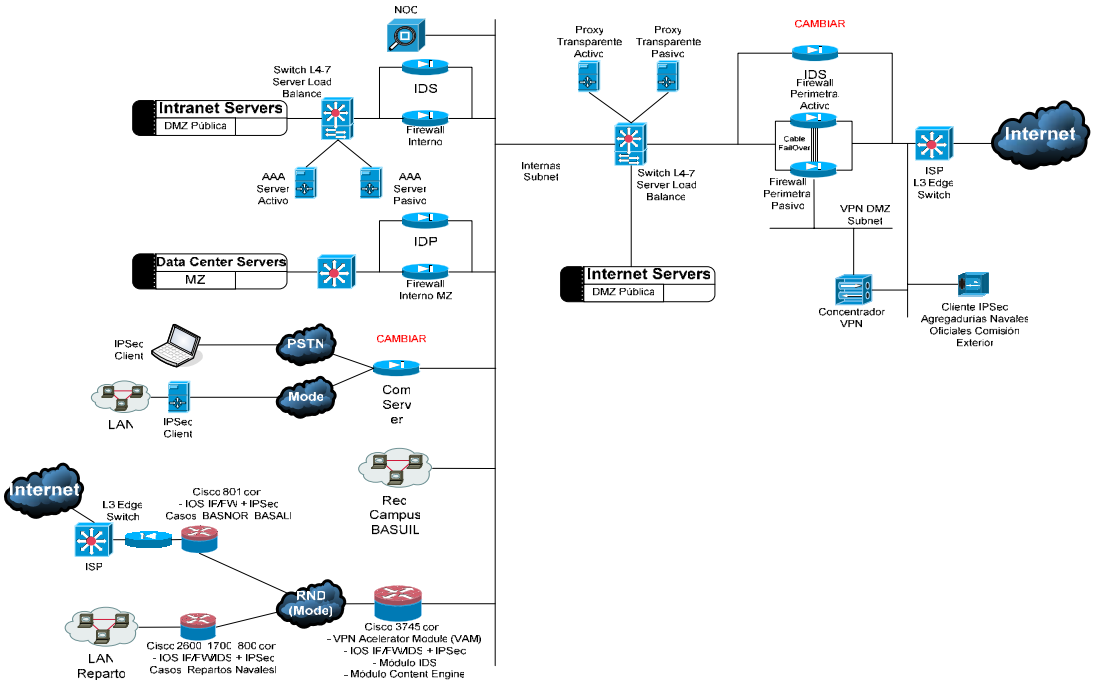


FIGURA 4.58 MODELO FUNCIONAL DE LOS MECANISMOS DE SEGURIDAD DE LA RED NAVAL DE DATOS Y ACCESO AL INTERNET

2. Calidad de Servicio Diferenciada

La Red Naval de Datos debe permitir establecer una Calidad de Servicio (QoS) diferenciada, que considere criterios tales como: usuario, tipo de aplicación y hora. Al ser la **disponibilidad** parte de los aspectos de la Visión Global de Seguridad Informática, es necesario definir las políticas de Calidad de Servicio a

aplicar, para garantizar el ancho de banda requerido por los usuarios que emplean determinada aplicación.

La Calidad de Servicio (QoS) se implementa con un conjunto de tecnologías que permiten a las aplicaciones solicitar y adquirir niveles de servicio predecibles en términos de ancho de banda (throughput), variaciones de latencia (jitter) y retardo (delay). Para lograr esto, no solamente debemos pasar la red de capa 2 a capa 3, sino que además se deben aplicar las políticas de Calidad de Servicio para asignar el ancho de banda limitado a cada usuario/aplicación.

Uno de los recursos con mayor limitación y que por tanto debe ser debidamente controlado, es el acceso al Internet. Por ello es necesario que al momento de asignar ancho de banda, se considere el perfil del usuario. Así mismo, la Armada tiene la intención de establecer aplicaciones de Video Conferencia sobre IP y Voz sobre IP, a través de la Red Naval de Datos; los equipos a emplearse están en plena capacidad de asignar el ancho de banda por el tipo de servicio, considerando las características del tráfico de cada una de éstas aplicaciones. Hay que tener presente que la Voz y el Video son sensibles al

tiempo (retardo), y que la entrega de paquetes para éste tipo de aplicación no puede sufrir retardos. En cambio la transmisión de datos requiere confiabilidad en la entrega, sin ser muy importante el retardo.

El protocolo empleado para establecer Calidad de Servicio (QoS) es el RSVP (Resource Reservation Protocol), el mismo que ofrece tres niveles de servicio:

- ✓ **Best-effort.-** Aplicaciones que requieren entrega confiable (datos tradicionales).

- ✓ **Rate-sensitive.-** Aplicaciones principalmente sensibles a las variaciones del ancho de banda disponible (Videoconferencia sobre IP).

- ✓ **Delay-sensitive.-** Aplicaciones sensibles al retardo (Voz sobre IP).

RSVP traslada la petición de QoS a través de la red, en cada nodo de la red el protocolo intenta reservar recursos para determinada transmisión, por tanto cada nodo luego de comprobar la existencia de recursos suficientes y los permisos

del usuario que hace la reserva, garantizará los niveles requeridos. RSVP es un protocolo de control que emplea los protocolos de enrutamiento.

4.5.11 CENTRO DE OPERACIÓN DE LA RED (NOC)

El NOC (Network Operation Center) implementará las facilidades que permitirá a los administradores de la red controlas los siguientes aspectos (especificaciones FCAPS de la ISO):

- ✓ **F**ault Management.- Detección, aislamiento, reparación y registro de las fallas de un dispositivo en la red.

- ✓ **C**onfiguration Management.- Mantenimiento de la información precisa sobre la configuración de la red (hardware y software) y los parámetros de control del sistema que se relacionan con su operación normal.

- ✓ **A**ccounting Management.- Manejo de usuarios y de tareas de administración, así como contabilización (registro) del uso de los recursos de la red y los servicios.

- ✓ **P**erformance Management.- Maximización del desempeño de la red. Relacionado estrechamente con la Calidad del

Servicio (QoS) y parámetros como utilización de recursos, retardos (delays), variaciones de latencia (jitter) y pérdida de paquetes.

- ✓ **S**ecurity Management.- Seguridad de los datos y operaciones, administración de los diferentes mecanismos de seguridad implementados en sitios críticos y estratégicos, como Firewalls, VPNs e IDS.

En pocas palabras, el NOC es el centro estratégico de control de los dispositivos de la red. Está compuesto por una serie de aplicaciones que le permite conocer a un administrador de la red el estado de ésta en todo momento. En el NOC se habilitan herramientas como NTP Server (para el control y sincronización del tiempo en los dispositivos de la red), SNMP para lectura de variables SNMP y control de ancho de banda, Traps Server para la captura de mensajes de error y alertas de los dispositivos de red, entre otros.

Para tener un control de la red es necesario monitorear cuatro parámetros: el desempeño (throughput), la pérdida de paquetes, el retardo (delay) y las variaciones de latencia (jitter). En el NOC se

emplea una herramienta de administración basada en ICMP o SNMP, la misma que permitirá notificar por varios medios alarmas y enviar mensajes (celular, beeper, email) a un administrador informando que existe algún evento que debe ser atendido de manera urgente (Ej: caída de un servidor, caída de un enlace, alerta grave en un firewall, etc). En el NOC también se implantará un servidor de accesos con puertos asincrónicos, llamado también Out of Band Server (OOB Server). Este equipo se conecta al puerto de consola de los switches, servidores y ruteadores principales de la red de modo que si no es posible accederlos vía TCP/IP, se pueda al menos acceder por consola a estos dispositivos. En el NOC se emplea también herramientas de sniffing que permiten conocer en tiempo real cuales son los parámetros de broadcast/multicast/unicast que mantiene la red en todo momento. En el NOC se debe contar con herramientas que permitan administrar las VLANs, creándolas, borrándolas o añadiendo nuevos usuarios a ellas.

Bajo el NOC están los servidores TACACS que permiten autenticar el acceso a los dispositivos de la red (Ruteadores, switches, servidores). Todos estos dispositivos tendrán acceso

únicamente a través de SSH, se deshabilitarán los accesos vía telnet.

En el NOC se tiene también un servidor Dummy desde el cual a través de TCP Wrappers se establezca que es el único que puede hacer telnet a los dispositivos de red.

Las principales herramientas de administración a emplear serán: CiscoWorks para redes de área local, redes de área extendida, Firewalls y VPNs; y HP Open View para dispositivos SNMP. En la Figura 4.59 se muestra el diagrama esquemático del NOC.

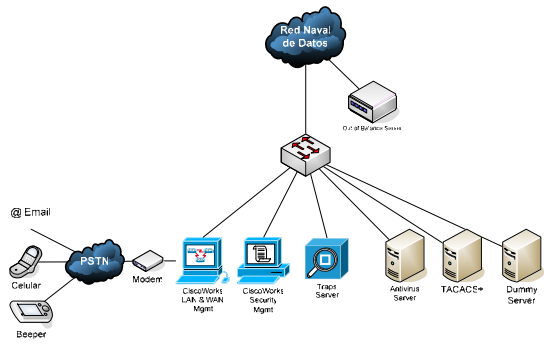


FIGURA 4.59 MODELO ESQUEMÁTICO DEL CENTRO DE OPERACIÓN DE LA RED NAVAL DE DATOS

El detalle de los equipos de conectividad propuestos se muestra en el Apéndice E – Plataforma Tecnológica de Conectividad.

4.5.12 SEGURIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA

Tal como se indicó en el Capítulo 3, Sección 4; estando la definición de políticas de seguridad a nivel institucional, como un marco de trabajo de mucho mayor alcance al pretendido en éste trabajo, nos limitaremos a presentar mecanismos de seguridad tecnológicos básicos que debe tener la infraestructura tecnológica para conseguir el fin superior de contar con una estrategia institucional de seguridad de la información. Se presume en base a las estadísticas recopiladas por el CERT (Computer Emergency Response Team), el CSI (Computer Security Institute) y el FBI; que el 80% de un marco de referencia de seguridad son procesos, entrenamiento y personas, y el 20% es tecnología, puesto que muchas de las organizaciones que han sufrido violaciones a su seguridad de la información contaban con mecanismos tecnológicos [35]. Justamente trataremos de resaltar en ésta sección éste 20% de mecanismos tecnológicos considerados para proteger nuestra infraestructura.

Siendo en general las redes de información, y en particular el Internet, medios de comunicación poderosos y muy difundidos en el mundo actualmente; la dependencia de las instituciones de estos medios tal como ha sido propuesto en éste trabajo, es cada vez mayor. La seguridad de las redes basadas en los estándares de Internet suele ser deficiente, por que los protocolos de comunicación empleados en muchas de las capas carecen de características robustas de seguridad; y generalmente la mayoría de aplicaciones ni siquiera emplean éstas emplean.

La automatización y la velocidad de los ataques está en aumento, siendo una amenaza permanente. Las herramientas empleadas son cada vez más sofisticadas y están la mayoría disponibles para cualquier curiosos en el Internet. Con poca dedicación es posible ponerse al tanto de las múltiples vulnerabilidades existentes en los diferentes sistemas, puesto que la comunidad de hackers tiene una penetración y capacidad de difusión muy parecida al modo de operar de la comunidad de código abierto. La proliferación de virus tipo gusano es una constante a la cual se enfrentan las infraestructuras tecnológicas.

Todos estos aspectos que conforman el entorno y la realidad a la que se exponen las infraestructuras tecnológicas de un mundo interconectado, conforman un medio bastante hostil que para ser mitigado, debe ser tratado con un enfoque integral de seguridad de la información que sobrepasa el alcance de éste trabajo.

Al decir de muchos expertos, la característica de seguridad es algo poco probable de alcanzar, particularmente en sistemas operativos y redes de computadoras, por lo cual se determina que la seguridad debe ser entendida más como un proceso que como un fin. Se pasa entonces a hablar de **fiabilidad** (probabilidad de que un sistema se comporte tal y como se espera de él), entonces el enfoque es conseguir mantener a los sistemas fiables.

En éste punto es necesario recordar la visión global de lo que representa la seguridad informática, que conlleva los elementos a proteger, los tipos de amenazas que contra ellos se presentan y el origen de tales amenazas, y las posibles formas de protección apropiadas para cada caso [17]. En la Figura No. 4.60 se muestra ésta visión global:

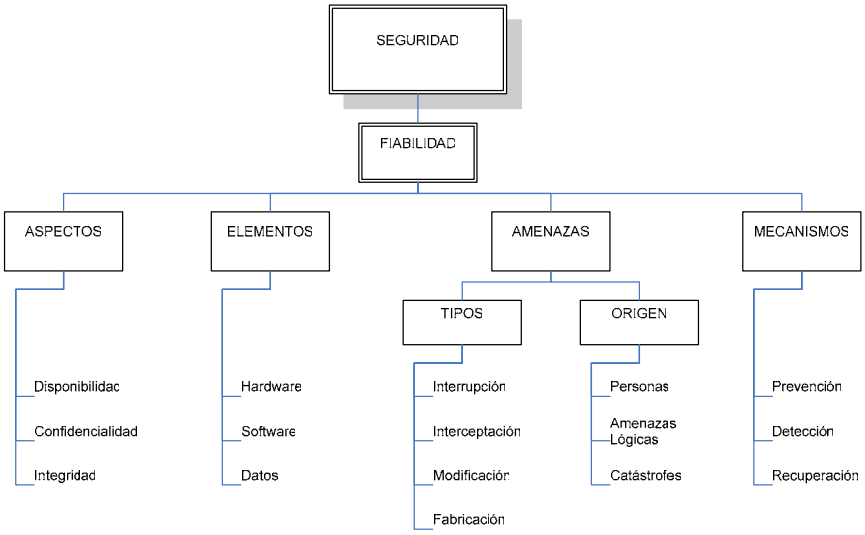


FIGURA 4.60 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

Los mecanismos de prevención más habituales son:

- ✓ Mecanismos de autenticación e identificación.- Permiten identificar entidades del sistema de forma única, y posteriormente una vez identificadas, autenticarlas (comprobar que la entidad es quien dice ser). Son los mecanismos más importantes puesto que forman la base de otros mecanismos que basaran su funcionamiento en la identidad de las entidades que acceden a un objeto. La combinación de esquemas de registro único (Single Sign On)

con autenticación basada en biometría o tokens físicos, integrados en un repositorio único (Directorio LDAP) son un ejemplo adecuado de éste mecanismo.

- ✓ Mecanismos de control de acceso.- Todos los objetos dentro de un sistema deben estar protegidos con mecanismos de control de acceso. Un ejemplo de estos mecanismos son las Listas de Control de Acceso (ACL) disponibles en los sistemas operativos UNIX, IOS, y en las bases de datos ORACLE.

- ✓ Mecanismos de separación.- Un sistema con diferentes niveles de seguridad ha de contar con mecanismos que permitan separar los objetos dentro de cada nivel, evitando el flujo de información entre objetos y entidades de diferentes niveles siempre y cuando no exista autorización expresa del mecanismo de control de acceso. Un ejemplo de éste mecanismo es la implementación de Base Segura de Cómputo (TCB) en UNIX.

- ✓ Mecanismos de seguridad en las comunicaciones.- Es vital mantener la integridad y privacidad de los datos mientras se

transmiten a través de la red, para ello se emplean ciertos mecanismos la mayoría basados en criptografía (cifrado con claves públicas/privadas, claves simétricas, empleo de protocolos seguros como SSH).

Hasta aquí se ha descrito los mecanismos que son requeridos para proteger especialmente los datos mientras son transmitidos a través de la red. En cuanto a la seguridad aplicada a los datos almacenados, tan solo se menciona que la base de datos escogida en éste caso obedece principalmente a las características de seguridad ofrecidas en el producto. El producto seleccionado como ha sido mencionado anteriormente es Oracle en su edición empresarial, incluyendo las características de seguridad avanzadas. Con ello se pretende tener seguridad adicional en la transmisión de datos a través del protocolo de transmisión de Oracle, Oracle Net con encriptamiento, así como también las características de bases de datos privadas virtuales, adecuado para el ambiente consolidado de Data Center presentado; y el etiquetamiento avanzado de objetos que permite mantener un control de acceso de granularidad muy fina.

Para centrarnos en la transmisión de datos, debemos considerar los servicios básicos de red que deben ser administrados de manera controlada en los servidores Linux, tal como consta en el Apéndice F – Seguridad de Redes; sin que esto pretenda ser una guía de instalación segura.

Para garantizar la seguridad que circula entre el cliente y el servidor, cuando se trata de datos sensibles, se requiere cifrar los datos mediante SSL (Security Socket Layer), que trabaja en conjunto con los certificados digitales.

1. Servicios de Firewall o Cortafuegos

Es un sistema o conjunto de sistemas que implementan una política de control de acceso y tráfico entre dos redes. De manera más clara podemos definir a un firewall como cualquier sistema utilizado para separar – en cuanto a seguridades se refiere – una máquina o subred, del resto; protegiéndola así de servicios y protocolos que desde el exterior pueden suponer una amenaza de seguridad. Un Firewall suele tener como mínimo tres interfaces, lo que permite crear las redes que se describen a continuación [36]:

- ✓ **Interior.-** Es el área de confianza de la red. Los dispositivos que están en el interior forman la(s) red(es) privada(s) de la organización. Estos dispositivos comparten directivas de seguridad comunes con respecto a la red exterior. Sin embargo es común también encontrar firewall en el segmento de confianza de la red, para proteger áreas críticas de ataques internos.

- ✓ **Exterior.**- Es el área de no confianza de la red. El firewall protege los dispositivos del interior y de la Zona Desmilitarizada (DMZ), de los dispositivos del exterior. Se suele permitir ciertos accesos desde el exterior a la DMZ de manera selectiva, pero no es recomendado hacerlo a un dispositivo en el interior.

- ✓ **Zona Desmilitarizada (DMZ).**- Es una red aislada a la que pueden acceder usuarios del exterior. Se configura en el firewall los tipos de acceso desde el exterior y desde el interior a la DMZ. Los equipos que residen en la DMZ suelen llamarse **host bastion.** Un servidor host pese a estar generalmente actualizado en cuanto a aplicación de parches de seguridad, es vulnerable a los ataques del

exterior, y solo ejecuta los servicios mínimos necesarios para cumplir sus tareas, los servicios innecesarios son desactivados.

Dicho esto, un Firewall básicamente cumple las siguientes funciones [36]:

- ✓ No permitir el acceso desde el exterior hasta el interior.
- ✓ Permitir un acceso limitado desde el exterior a la DMZ.
- ✓ Permitir todo el acceso desde el interior hasta el exterior (aunque puede ser más restrictivo).
- ✓ Permitir un acceso limitado desde el interior hasta la DMZ.

Si el Firewall tiene mayor cantidad de interfaces, que permita definir más zonas, se emitirán directivas específicas para controlar el flujo entre éstas.

Tipos de Firewall

En términos generales tenemos tres tipos de Firewall:

- ✓ Filtros de paquetes

- ✓ Filtros de proxy
- ✓ Filtros de paquetes con estado

Filtros de paquetes.- Analiza el tráfico en la capa de transporte o en la capa Internet. la información analizada por un filtro de paquetes es la información estática de la cabecera del paquete. El administrador configura reglas que se utilizan como criterios de origen y/o destino específicos. Un filtro de paquetes puede autorizar o negar un paquete en base a uno o más de los siguientes criterios:

- ✓ Dirección IP de origen
- ✓ Dirección IP de destino
- ✓ Protocolo
- ✓ Puerto de origen
- ✓ Puerto de destino

Un ruteador configurado con una lista de control de acceso (ACL) para filtrar tráfico que pasa por él, es un ejemplo de éste

tipo de Firewall. Un Firewall de ése tipo no guarda información de estado, es decir toma una decisión sin que guarde información al respecto.

Filtros de Proxy

Es un dispositivo Firewall que examina los paquetes en las capas superiores del modelo OSI (capas 4-7). Es un filtro efectivo pero afecta el rendimiento. El dispositivo oculta datos valiosos exigiendo que los usuarios se comuniquen con un sistema seguro a través del proxy. Los usuarios obtienen acceso a la red pasando por un proceso que establece el estado de la sesión, la autenticación del usuario y la política autorizada. Esto implica que los usuarios se conectan con servicios externos a través de programas de aplicación (proxies) que se ejecutan en el *gateway* conectado con la zona externa desprotegida.

Filtros de paquetes con estado

Combina lo mejor de las dos metodologías antes mencionadas. Un filtro de paquete con estado mantiene una información completa del estado de sesión para cada sesión

que se construya en el Firewall. Cada vez que se establece una conexión entrante o saliente, la información queda registrada en una tabla de flujo de sesión con estado. Esta tabla contiene las direcciones de origen y de destino, los números de puerto, información de las secuencias TCP e indicadores adicionales para cada conexión TCP/UDP que esté asociada con una determinada sesión. Cuando se inicia una sesión a través del Firewall, se crea un objeto de conexión y, consecuentemente, se comparan todos los paquetes entrantes y salientes con los flujos de sesión de la tabla de flujo de sesión con estado. Solo si hay una conexión apropiada que valide el paso, se autoriza el paso de los datos a través del Firewall.

4.5.13 APLICACIONES FUTURAS DE LA RED

Internet 2

Internet 2 es un esfuerzo de colaboración para desarrollar tecnología y aplicaciones avanzadas en el Internet, vitales para las misiones de investigación y educación de las instituciones de educación superior. Las más importantes

universidades del mundo, trabajando con la industria y los gobiernos, encabezan este proyecto. Internet 2 habilita aplicaciones tales como: aprendizaje remoto, telemedicina, bibliotecas digitales y laboratorios virtuales que no son posibles con la tecnología actual del Internet. Como proyecto de la Corporación Universitaria para el Desarrollo Avanzado del Internet (UCAID), el Internet 2 no es una simple red aparte, sino que une las aplicaciones de la red y los esfuerzos de desarrollo de ingeniería con redes avanzadas de universidades, regionales y nacionales [37].

El Internet que actualmente conocemos tuvo sus inicios como un esfuerzo federal y universitario, y fue concebido con las siguientes características [38]:

- Miles de usuarios.
- Acceso remoto, transferencia de archivos.
- Interconectar Mainframes.
- Creación de aplicaciones con la tecnología existente.

El Internet de hoy desde su comercialización a partir del año 1994, tiene muchas características nuevas. Tanto su tamaño como la tecnología necesaria para soportar nuevas aplicaciones más allá de sus parámetros originales de diseño han cambiado [38]:

- Millones de usuarios.
- Web, email, audio y video de baja calidad.
- Interconecta computadoras personales y servidores.
- Las aplicaciones se adaptan a la tecnología base del Internet.

El Internet de mañana promete satisfacer nuevas demandas, muchos más usuarios y muchas más aplicaciones. Para lograrlo se requieren nuevas capacidades en la red. Tendrá las siguientes características [38]:

- Billones de usuarios y dispositivos.

- Convergencia de las aplicaciones actuales con multimedia (telefonía, videoconferencia, video digital de alta definición.

- Interconectará computadoras personales, servidores y computadoras empotradas.

- Las nuevas tecnologías habilitarán aplicaciones emergentes y creará nuevos retos.

Las capacidades avanzadas de red del Internet 2, incluyen una infraestructura donde los backbone operan desde 2.4 Gbps (OC48) hasta 10 Gbps (OC192, interconectando los GigaPoPs. Para entender lo que representa ésta capacidad, a continuación mostramos una figura comparativa del tiempo que toma descargar la película “The Matrix" en formato DVD a través de diferentes tecnología de acceso al Internet actual, con Internet 2 [38]:

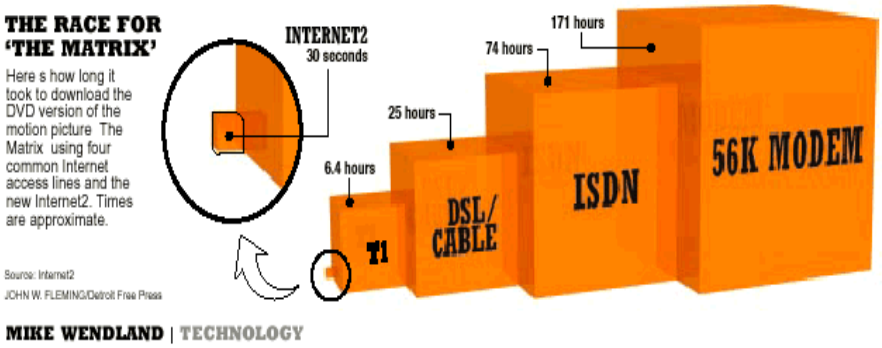


FIGURA 4.61 COMPARACIÓN DE CAPACIDADES ENTRE INTERNET 2 Y DIFERENTES TECNOLOGÍAS DEL INTERNET ACTUAL

Dentro de las iniciativas relacionadas con el proyecto Internet 2 tenemos el desarrollo de Middleware, capa de software entre la red y las aplicaciones, responsable de:

- Autenticación.
- Identificación.
- Autorización.
- Directorios.
- Seguridad.

Otra iniciativa activa y clave es la Ingeniería de la red, en la que se han conformado grupos de trabajo para los siguientes tópicos:

- IPv6.
- Medición.
- Multicast.
- Calidad de Servicio (QoS).
- Ruteo.
- Seguridad.
- Topología.

Las aplicaciones avanzadas son el corazón del Internet 2, e incluyen las siguientes áreas:

- Computación distribuida.
- Laboratorios virtuales.
- Librerías digitales.

- Aprendizaje distribuido.
- Video digital.
- Tele-inmersión.
- Acceso remoto a laboratorios y teleoperación remota de instrumentos avanzados.

Estas aplicaciones se caracterizan por tener una transferencia masiva de datos, ser sensibles al tiempo real, calidad de servicio garantizada, seguridad y alta disponibilidad de la red.

El Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA) es Miembro Internacional del proyecto Internet 2, y en él, la Armada del Ecuador, a través del INOCAR quien es miembro de CEDIA tendría una participación para que los esfuerzos de investigación, desarrollo y transferencia de tecnología de la Institución en diferentes campos, conformen parte de los esfuerzos del país en aspectos de innovación. Las necesidades actuales y futuras de desarrollo tecnológico en la Armada implican que ésta sea parte activa de un sistema de innovación nacional.

La Armada al participar en este proyecto, debe tener presente el impacto estratégico que representará el acceso a aplicaciones como:

- Educación a distancia (Global).
- Bibliotecas digitales.
- Telemedicina.
- Ciencias del mar (Oceanografía, Hidrografía, Biología Marina, etc)
- Colaboratorios.
- Robótica.
- Supercómputo compartido.

Es importante además resaltar que el sistema de telecomunicaciones de las Fuerzas Armadas (Red MODE) tiene una cobertura nacional enlaces de hasta 2 Mbps, en sitios donde por razones comerciales las operadoras y portadores no les resulta atractivo invertir, pudiendo

convertirse en sistema de acceso a la gran red dorsal (Backbone) nacional en un esfuerzo de país por reducir la brecha digital existente, como un posible proyecto de responsabilidad social.

IPv6

El Internet Protocol versión 6 (inicialmente llamado IPng – IP next generation), es la “nueva generación” de protocolos diseñados por el Internet Engineer Task Force (IETF) para reemplazar la versión actual del Internet Protocolo (IPv4). La mayoría de usuarios actuales utilizan IPv4, un protocolo utilizado desde hace aproximadamente 20 años, que ha demostrado mucha confiabilidad, pero ha comenzado a tener problemas. Uno de los más importantes es el agotamiento de direcciones IPv4, las que son ampliamente demandadas por máquina y dispositivos que deben ser añadidos al Internet [40].

IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4,294’967,296).

En cambio IPv6 nos ofrece un espacio de 128 bits, es decir, 2^{128} (340,282,366,920,938,463,374,607,431,768,211,456); un número extremadamente grande (665.570.793.348.866.943.898.599 IP's por cada metro cuadrado de superficie terrestre.

El importante desarrollo de diferentes tecnologías como la telefonía celular, las redes inalámbricas, los modems de cable, xDSL, etc, que requieren direcciones IP fijas ha ocasionado que en muchos de los casos (Japón y algunos países de Europa) la relación de utilización de direcciones IP por parte de los usuarios pase en pocos meses, de 10:1 a 1:1. En un futuro próximo, pronto veremos dispositivos "siempre conectados" lo que invertirá la relación a 1:20, 1:50, 1:100.

Si bien es cierto mecanismos como NAT (Network Address Translation) han solucionado de manera temporal el problema de las direcciones, no es la solución definitiva. Las tablas de ruteo crecen excesivamente, degradando el desempeño y los tiempos de respuesta. Adicionalmente los esquemas NAT han privado a las Intranets de importantes aplicaciones como [41]:

- RTP y RTCP (“Real-time Transport Protocol” y “Real Time Control Protocol”) que utilizan UDP con asignación dinámica de puertos (No soportado por NAT).

- La autenticación Kerberos necesita la dirección fuente, que es modificada por NAT en la cabecera IP.

- IPsec pierde integridad, debido a que NAT cambia la dirección en la cabecera IP.

- El Multicast, aunque es posible, técnicamente su configuración es muy complicada con NAT, que en la práctica no se emplea.

Dentro de las características principales de IPv6 tenemos [41]:

- Mayor espacio de direcciones.

- Autoconfiguración (Plug & Play).

- Seguridad intrínseca en el núcleo del protocolo (IPsec).

- Calidad de Servicio (QoS) y Clase de Servicio (CoS).

- Multicast: envío de UN mismo paquete a un grupo de receptores. Ya no hay broadcast.

- Anycast: envío de UN paquete a UN receptor dentro de UN grupo.

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los ruteadores, alineados a 64 bits (preparados para su procesamiento óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agilita el procesamiento por parte del ruteador.

- Posibilidad de paquetes con carga útil (datos) de más de 65,535 bytes.

- Enrutamiento más eficiente en el backbone de la red, debido a una jerarquía de direccionamiento basada en la agregación.

- Renumeración y “multi-homing”, que facilita el cambio de proveedor de servicios.

- Características de movilidad.

La cabecera en IPv4 tiene una longitud mínima de 20 bytes, a lo que se añade las opciones que depende de cada caso; y tiene 12 campos. En IPv6 la cabecera tiene una longitud fija de 40 bytes, y solo 8 campos. Esto facilita el procesamiento de los procesadores de 64 bits previstos para las nuevas generaciones de ruteadores.

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Estas direcciones se clasifican en tres tipos [41]:

- **Unicast.-** Identificador para una única interfaz. Un paquete enviado a una dirección Unicast es entregado únicamente a la interfaz con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

- **Anycast.-** Identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Un paquete enviado a una dirección Anycast es entregado a **una** (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima según el protocolo de

enrutamiento). Nos permite crear ámbitos de redundancia o clusters con varias máquinas compartiendo la misma dirección.

- **Multicast.-** Identificador para un conjunto de interfaces (generalmente de diferentes nodos). Un paquete enviado a una dirección multicast es entregado a **todas** la interfaces identificadas por dicha dirección. Se emplea en aplicaciones de transmisiones múltiples (broadcast).

Hay algunas diferencias importantes en el direccionamiento IPv4 respecto a IPv6 [41]:

- No hay direcciones broadcast (su función es sustituida por direcciones multicast).

- Los campos de las direcciones reciben nombres específicos; denominados “prefijo” a la parte de la dirección hasta el nombre indicado (incluyéndolo).

- Dicho prefijo nos permite conocer **donde** está conectada determinada dirección, es decir, su ruta de encaminamiento.

- Cualquier campo puede tener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.

- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.

- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).

- Una única interfaz puede también tener varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.

- Una misma dirección o conjunto de direcciones unicast pueden ser asignadas a múltiples interfaces físicas,

siempre que la implementación trate dichas interfaces desde el punto de vista de Internet, como una única, lo que permite el balanceo de carga entre múltiples dispositivos.

- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiple prefijos de subred a un mismo enlace.

La representación de direcciones IPv6 sigue el siguiente esquema:

- x:x: x:x: x:x: x:x, donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:
    - FEDC:BA98:7654:3210:FEDC: BA98:7654:3210
    - 1080:0:0:0:8:800:200C:417A
- Dado que por el direccionamiento definido, podrán existir largas cadenas de bits “cero”, se permite la

escritura de su abreviación, mediante el uso de “::”, que representa múltiples grupos consecutivos de 16 bits “cero”. Este símbolo solo puede aparecer una vez en una dirección IPv6. Ejemplos:

1080:0:0:0:8:800:200C:417A (dirección unicast)	1080::8:800:200C:417A
FF01:0:0:0:0:0:0:101 (dirección multicast)	FF01::101
0:0:0:0:0:0:0:1 (dirección loopback)	::1
0:0:0:0:0:0:0:0 (dirección no especificada)	::

- Una forma alternativa y conveniente cuando nos hallamos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde “x” representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y “d” representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar de IPv4). Ejemplos:

0:0:0:0:0:0:13.1.68.3 ::13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38 ::FFFF: 129.144.52.38

- La representación de los prefijos se realiza de la siguiente forma:

    - dirección-IPv6/longitud-del-prefijo

    Donde la dirección IPv6 se representa en cualquiera de las notaciones válidas explicadas, y la longitud del prefijo es un valor decimal que indica cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo.

    Por tanto para escribir una dirección completa, indicando la subred, podríamos hacerlo como:

    12AB:0:0:CD30:123:4567:89AB:CDEF/60

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones [41]:

- Sus direcciones locales de enlace para cada interfaz.

- Las direcciones unicast asignadas.
- La dirección de loopback.
- Las direcciones multicast de todos los nodos.
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas.
- Las direcciones multicast de todos los grupos a los que dicho host pertenece.

Además en el caso de los ruteadores, tienen que conocer también [41]:

- La dirección anycast del ruteador de la subnet, para las interfaces en las que esta configurado para actuar como ruteador.
- Todas las direcciones anycast con las que el ruteador ha sido configurado.
- Las direcciones multicast de todos los ruteadores.

- Las direcciones multicast de todos los grupos a los que el ruteador pertenece.

Todos los dispositivos con IPv6, deben tener, predefinidos los siguientes prefijos [41]:

- Dirección no especificada.
- Dirección de loopback.
- Prefijo multicast (FF).
- Prefijos de uso local (local de enlace y local de sitio).
- Direcciones multicast predefinidas.
- Prefijos compatibles con IPv4.

Existe una relación interdependiente y vinculante entre el desarrollo de IPv6 y el Internet 2.

El camino de IPv4 a IPv6 no es una cuestión de transición ni de migración, sino de evolución, de integración, una evolución disruptora y al mismo tiempo necesaria. IPv6 permitirá un crecimiento escalable y a la vez simple, principales

limitaciones de IPv4. Se espera que IPv6 reemplace gradualmente a IPv4, con un periodo de coexistencia de ambos por algunos años.

CAPITULO 5

5. IMPLEMENTACIÓN DE LA INTRANET PILOTO DEL INSTITUTO OCEANOGRÁFICO DE LA ARMADA

Nuestra implantación práctica de los conceptos, modelos, diseños y aplicación de tecnología descritas a lo largo de nuestra tesis se concretan en un piloto desarrollado en un reparto de la Armada, el Instituto Oceanográfico. La decisión de seleccionar esta dependencia naval fue porque se logró establecer un compromiso de parte del señor Director del INOCAR para facilitarnos las instalaciones del Centro de Datos con los equipos computacionales y red de datos local que dispone el Instituto, así como la adquisición de las herramientas de software para el desarrollo e implementación del piloto.

5.1 DEFINICIÓN Y APLICACIÓN DEL MARCO DE TRABAJO DENTRO DE LA INTRANET

El valor de la organización es generado en sus operaciones (procesos), y toda la Intranet y la estructura organizacional que soporta la Intranet deben ser capaces de soportar los procesos de la organización. Consecuentemente, los procesos que demandan y producen información para la Intranet deben necesariamente ser integrados en la solución aplicada.

Para el caso del INOCAR se implantó el marco de trabajo de procesos y roles necesarios para administrar la Intranet de la organización para que apoyen efectivamente las tareas principales diarias de los usuarios, técnicos y científicos, dentro de las operaciones de investigación técnica-científica.

Entre las actividades de administración de la Intranet se incluyeron la generación y actualización de contenido, soporte de usuarios, administración de cuentas de usuarios, permisos de acceso y mantenimiento de componentes de hardware y software. Se buscó evitar que las responsabilidades indefinidas y procesos no claros resulten en contenido desactualizado o no accesible, lo que provocaría que la Intranet

no sea atractiva para los usuarios y por tanto resulte en bajos retornos a la inversión efectuada.

Se definió el mapa de procesos de la Figura 5.1 que soporta una eficiente administración de la información en la Intranet. Cada uno de estos procesos agrupa varias tareas para operar la Intranet. Cada tarea es asignada a un rol con responsabilidad de llevarlo a cabo. A su vez este rol es asignado a uno o varios individuos. Con este esquema se logra que al personal se le asignen roles. Puede cambiar el personal asignado a un rol pero las tareas vinculadas permanecen inalterables.

Los procesos se agrupan en dos niveles, el primero a nivel funcional donde interviene el personal de los departamentos que desarrollan las actividades de producción y uso de información que se relacionan a los procesos operativos de la organización; y por otra parte, el nivel técnico que agrupa las actividades de mantenimiento y soporte de la infraestructura tecnológica de la Intranet.

Procesos a nivel funcional

Los procesos que producen información, entre los que están la creación de contenido, mantener el contenido actualizado, remover el contenido desactualizado y distribuir contenido.

Procesos a nivel técnico

Los procesos para la provisión, distribución, mantenimiento y eliminación de información en la Intranet. Estos procesos aseguran que el contenido de la Intranet esté siempre actualizado y reúna estándares de calidad. Los estándares incluyen regulaciones detalladas para autoría, edición, publicación y archivo de contenido del Intranet. Estos procesos son usualmente iniciados por los procesos de producción de información.

Los procesos para mantener operando los componentes de hardware y software pertenecen a la cuarta categoría. Cubren las tareas de instalación, administración y soporte.

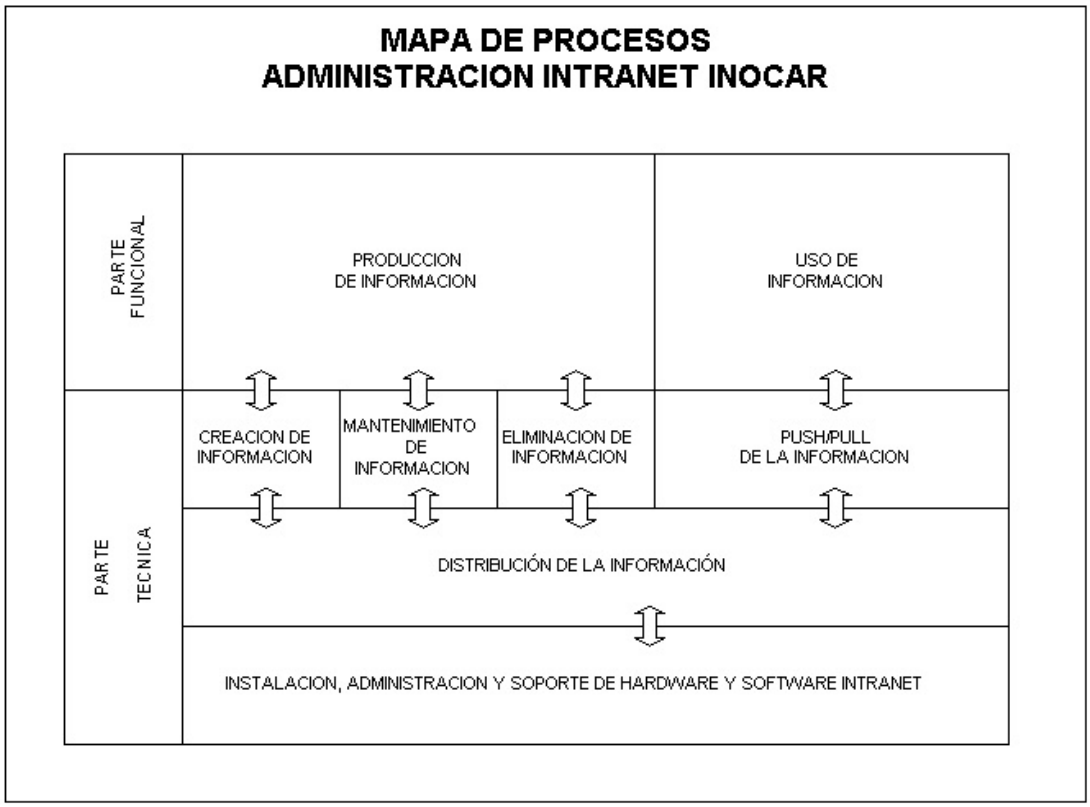


FIGURA 5.1. MAPA DE PROCESOS INTRANET INOCAR

5.2 DEFINICIÓN DE ROLES, ORGANISMOS, PROCEDIMIENTOS Y ESTÁNDARES PARA EL MANEJO DE LA INTRANET

Una organización militar como es el INOCAR se encuentra regulada por múltiples leyes, reglamentos, ordenanzas navales, procedimientos operativos y administrativos para cumplir con sus funciones principales orientadas al apoyo de la Fuerza Naval. Por otra parte el INOCAR es una

organización técnica-científica con personería jurídica, dotada de facultades para ejercer actividades hidrográficas, de mantenimiento a las ayudas a la navegación y oceanográficas en todo el país, y representar al Estado en todas las organizaciones que regulan o promueven normativas en estos campos. Por esta razón se vuelve mandatorio la formalidad en los procesos de investigación técnica-científica. Pero por otro lado, las actividades de coordinación y comunicación de los investigadores generan intercambio de ideas y contenido informal con la intención de crear nuevo conocimiento. Es decir que se requiere soportar el manejo de contenido formal e informal. Para ello tomamos como base la infraestructura para la administración de una Intranet revisada en el capítulo 2 y que a continuación detallamos su implantación en INOCAR.

5.2.1 ROLES PARA ADMINISTRACIÓN DE LA INTRANET

Iniciamos describiendo los roles individuales que fueron establecidos:

5.2.1.1 Usuarios

Aquellos que utilizarán la información digital disponible en la Intranet. En el ambiente Intranet del INOCAR mantenemos

una posición de dejar que los usuarios utilicen cualquiera de los dos clientes universales más comunes que son:

- Netscape Navigator o Comunicator.
- Internet Explorer.

5.2.1.2 Autores

Son responsables de producir y actualizar una porción específica del contenido de la Intranet.

Herramientas de oficina como Microsoft Word, Excel, Power Point, Project y compatibles que les permita generar documentación digital. Aquí lo importante es que no se preocupen en los detalles de diseño de las páginas a publicar y de detalles técnicos de la Intranet sino su compartición de conocimiento que pueda ser utilizado para mejorar los productos de datos y servicios que el INOCAR ofrece en el campo de la investigación oceanográfica, hidrográfica y de las ayudas a la navegación.

Para la creación de contenido optamos por la herramienta tecnológica BeeBox Community Content Manager, un

software desarrollado con el auspicio de la UNESCO, a través de la Comisión Oceanográfica Intergubernamental (COI), que impulsa la creación de sociedades de conocimiento. Es una herramienta de fácil uso y que permite a los autores rápidamente generar sus documentos HTML y almacenarlos en una base de datos MySQL, que luego serán revisados por los editores de contenido quienes decidirán su publicación. El objetivo es que los autores de la información sientan que las herramientas tecnológicas son un apoyo para sus tareas antes que un obstáculo, y que se requiere de su participación para mantener el dinamismo del sitio Intranet.

Todos aquellos funcionarios que dentro de sus procesos formales de trabajo deben generar información resultante de análisis de datos, estudios o investigación se consideran personal idóneo para ser autores. Los jefes de área designan quienes son los autores de contenido para mantener la información departamental en continua actualización.

5.2.1.3 Editores

Coordinan el contenido producido por varios autores, son responsables de asegurar consistencia, de evitar contenidos repetidos, y, sugerir cambios y nuevo contenido a los autores.

En cada departamento del INOCAR: Hidrografía, Ciencias del Mar, Ayudas a la Navegación y Administrativo, el Jefe de Área delegó a un representante para que se encargue de editar y publicar la información formal previamente aprobada.

Utilizan el módulo de administración de la herramienta BeeBox Community Content Manager.

5.2.1.4 Webmaster

Representa la interfaz entre la parte técnica y la parte de contenido en la gestión de la Intranet. La principal responsabilidad del webmaster es mantener las aplicaciones web operativas y consistentes, instalar y administrar la tecnología de información requerida para la Intranet, dar soporte técnico al personal de especialistas de la publicación y planificar e impartir el entrenamiento de los usuarios.

5.2.1.5 Soporte Técnico

Responsable de operar y mantener los componentes de hardware y software. Las principales tareas son: monitoreo, acceso, configuración, instalación de hardware y software, y administración de usuarios.

Este rol se subdivide a su vez en varios roles subordinados:

Administrador de red.- Responsable de hardware y software de red.

Administrador de Servidores.- Responsable de hardware y software de servidores, que incluye sistemas operativos de servidores.

Administrador de Usuarios.- Responsable por el hardware y software de usuarios.

Asistente de usuarios.- Responsable de operar el help desk, dando soporte a los usuarios finales así como a los autores y editores. Problemas que no pueden ser resueltos por el asistente son direccionados a los especialistas competentes.

Instructor.- Responsable de entrenar a los usuarios, autores y editores.

En la Figura 5.2 se presenta la asignación de roles para cada proceso funcional y técnico que da soporte a la administración de la Intranet.

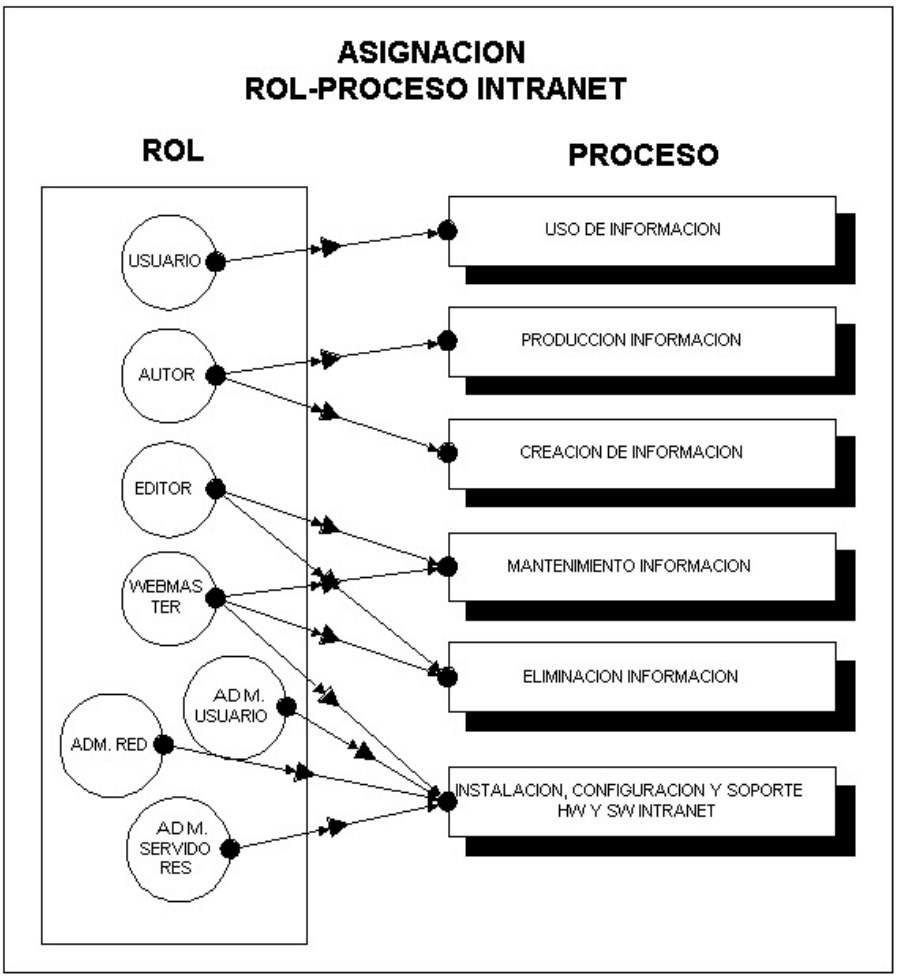


FIGURA 5.2. ASIGNACIÓN DE ROLES A PROCESOS INTRANET

5.2.2 ROLES ORGANIZACIONALES

Las personas que estarán a cargo de los roles del Intranet requieren de entidades que provean el soporte a la comunicación y coordinación. Para llevar a cabo las tareas de aprobación de contenido formal de los sitios web a cargo del INOCAR y el establecimiento de políticas, estándares y procedimientos se definió la creación de un solo organismo rector en el desarrollo, operación y mejora de la Intranet, el Consejo Web; mientras que se definió el Comité Técnico Web para ejecutar las tareas de mantenimiento y soporte tecnológico de la Intranet.

5.2.2.1 Consejo Web

El Consejo Web del INOCAR es el único ente que tratará todos los asuntos relacionados a la Intranet, Extranet e Internet definidos en el Capítulo 2, y que incluye las tareas que le corresponde al Foro Editorial.

Se integró este consejo con la participación del coordinador y editor de la información de los departamentos de Ciencias del Mar, Hidrografía y Ayudas a la Navegación, presidido por el

administrador del Web a cargo del Jefe de CENDO. Es miembro también el Webmaster del INOCAR.

Su función principal es la de:

- Establecer políticas, estándares y guías de estilo al más alto nivel que deberán respetarse en todos los sitios administrados por el INOCAR.

- Supervisar el Mapa de Sitio de la Intranet del INOCAR para verificar actualización y cumplimiento de estándares.

- Identificar oportunidades de mejorar, cambiar o ampliar los servicios web para hacer que la información sea más valiosa y accesible por los usuarios del sitio.

5.2.2.2 Comité Técnico Web

Está integrado por el webmaster del INOCAR, el equipo de desarrollo de aplicaciones web, administrador de servidores, soporte técnico y el administrador web quién lo preside, Su función es establecer estándares técnicos de la Intranet y presentar la planificación anual de requerimientos para dar

soporte efectivo a las actividades de mantenimiento de los sitios.

5.2.3 SERVICIOS DE LA INTRANET

Las personas que estarán a cargo de los roles del Intranet requieren de entidades que provean el soporte a la comunicación y coordinación.

5.2.3.1 A nivel de Sistemas de Administración de la Información

a) Sistema de Información Hidrográfica-Oceanográfica que permita consultar al banco de datos histórico de las diferentes áreas de investigación que el INOCAR mantiene en su Centro de Datos. Este sistema debe permitir que se implementen las consultas a través de menús autoexplicativos y produzcan reportes desde interfaces browsers, actuando como clientes universales, basados en perfiles de usuarios autorizados para tal acción.

b) Desarrollo de una aplicación web para consulta de la Ejecución Presupuestaria del INOCAR, donde se presente la información actualizada de los movimientos de las partidas presupuestarias del Instituto con niveles de porcentaje

ejecutados hasta la fecha. Así se podrá informar a los jefes departamentales de los saldos presupuestarios del área bajo su responsabilidad como herramienta de apoyo para su gestión.

c) Sistema de Información sobre Proyectos en Ejecución donde se pueda mostrar toda la documentación referente al estado de un proyecto, personal responsable, asignación de tareas específicas con plazos comunicados a través de un sistema colaborativo para grupos de trabajo.

d) Resúmenes de las principales sesiones de consejos, comités técnicos o de grupos de trabajo llevadas a cabo en relación a un proyecto para su revisión en línea por todos los empleados interesados.

5.2.3.2 Herramientas colaborativas para trabajo en grupo

Comunicación Interdepartamental

Se aprovechó la potencialidad de la tecnología web para habilitar comunicaciones interactivas dentro del Instituto. Estos incluyen:

a) Grupos de discusión para intercambiar ideas de propuestas de proyectos de investigación, desarrollo de nuevos productos de datos e información científica, mejora de los servicios que el INOCAR oferta actualmente o creación de nuevos.

b) Servidor de noticias relacionadas al tema de investigación hidrográfica y oceanográfica a nivel nacional e internacional.

c) Sitio de publicación de productos de software disponibles en el INOCAR para uso interno, donde se pueda bajar archivos ejecutables y documentación de soporte.

d) Sitios departamentales donde se publique información técnica sobre actividades relacionadas a su área de cobertura, donde los empleados puedan tener acceso en línea a documentación sobre proyectos, objetivos estratégicos a corto, mediano y largo plazo, responsabilidades del personal, proveedores y clientes de los servicios, políticas y directrices, reglamentos y estándares técnicos para desarrollo del trabajo.

e) Encuestas y retroalimentaciones a través de formularios de sugerencias.

f) Distribución de oficios y memos y sus respuestas.

g) Consultas a bases de datos en forma interactiva

5.2.3.3 Documentos y Referencias en línea

a) Políticas de la Armada y del INOCAR, Plan Estratégico Institucional en lo aplicado al sector de desarrollo de los intereses marítimos.

b) Reglamentos internos para empleados civiles.

c) Catálogo de los artículos disponibles para la venta en la mapoteca del INOCAR, así como horario de funciones del planetario y su programación.

d) Procedimientos para aplicación de beneficios del personal en atención médica y seguros contra accidentes.

e) Noticias sobre eventos técnico-científicos organizados en el Instituto o externamente que sean aplicables.

f) Manual de Organización interna y Manual de Procedimientos operativos y administrativos de los departamentos y unidades adscritas subordinadas.

g) Manuales de Calidad

h) Materiales de orientación

i) Guía de usuarios de software

j) Guías de referencia rápida

k) Manuales de entrenamiento y tutoriales

l) Mapas y dibujos esquemáticos

m) Especificaciones de equipos y metodologías para su uso aplicado a la investigación

n) Catálogos de datos y productos de datos

5.3 IMPLEMENTACIÓN DEL SISTEMA DE INFORMACIÓN DE AVISOS A LOS NAVEGANTES, UTILIZANDO EL PARADIGMA ORIENTADO A OBJETOS.

Como parte de los sistemas de administración de información técnica del Instituto, se propuso el desarrollo e implementación de una aplicación bajo el paradigma orientado a objetos que se integre a los servicios de la Intranet y que sistematice la provisión de información sobre las novedades que se presenten en el sistema de ayudas a la navegación del país, las que son requeridos por diferentes usuarios navieros, portuarios, buques navales y mercantes. Se aprobó este

proyecto y se lo desarrollo bajo el marco referencial que se presenta a continuación.

5.3.1 FINALIDAD DEL PROYECTO

Contribuir a que el INOCAR, a través de su departamento de Ayudas a la Navegación, provea un servicio oportuno y eficiente de información sobre el estado del Sistema Nacional de Señalización Marítima como aporte a la seguridad de la navegación en el Ecuador.

5.3.2 PROPÓSITO DEL PROYECTO

Desarrollar un Sistema de Información que permita registrar el estado de las ayudas a la navegación del país a fin de difundirlas automáticamente a los navegantes y usuarios de este servicio por diferentes medios de comunicación.

5.3.3 DEFINICIÓN DEL SISNAV

El proyecto en su fase I contempla la implementación del sistema de difusión de los Avisos a los Navegantes, a cargo del Departamento de Ayudas a la Navegación, donde se podrá registrar en formularios electrónicos los avisos diarios y mensuales, temporales y

permanentes de las novedades presentadas en el sistema nacional de balizamiento y almacenarlas en una base de datos histórica para su consulta posterior. Los avisos podrán ser transmitidos en forma automática por medio de:

a) Páginas web
b) e-mail
c) Fax
d) Beeper

5.3.4 ALCANCE DEL SISNAV

El sistema en esta fase tendrá lo siguiente:

a) Módulo de ingreso de datos por formulario de novedades diarias o mensuales de las ayudas con su respectiva validación y almacenamiento en la base de datos relacional Oracle.

b) Módulo de mantenimiento de los equipos de las ayudas que incluya el registro de las comisiones realizadas para este propósito.

c) Módulo de consultas predefinidas de la base de datos que incluyen estadísticas básicas.

d) Módulo de envió de novedades por diferentes medios de comunicación a usuarios previamente configurados.

5.3.5 SOLUCIÓN TECNOLÓGICA DEL SISNAV

Para este sistema se utilizó la infraestructura tecnológica disponible en INOCAR:

- ✓ Base de Datos Oracle 8i
- ✓ Servidor de Aplicaciones web : Websphere Application Server 3.5 de IBM
- ✓ Herramienta de programación : Visual Age for Java de IBM

Se aplicó la metodología de orientación a objetos para el análisis y desarrollo del sistema y su arquitectura se ajustó al modelo de n-capas: servidor de base de datos, servidor de aplicaciones y clientes ligeros para los usuarios. La implementación se llevó a cabo siguiendo el esquema Model-View-Control aplicando EJB, JSP/Applet y Servlets.

5.3.6 ENTREGABLES DEL SISNAV

Los entregables del SISNAV, como parte del proceso de desarrollo del sistema de información son los siguientes:

- ✓ Procedimientos de Administración del Intranet en INOCAR – Apéndice G.
- ✓ Documentación Técnica del Análisis y Diseño aplicando el paradigma Orientado a Objetos al Sistema Aviso a los Navegantes – Apéndice H.
- ✓ Manual de Usuario del SISNAV – Apéndice I.
- ✓ Documentación Técnica Herramienta BeeBox (Technical Notes for Developers) – Apéndice J.

5.4 INFRAESTRUCTURA TECNOLÓGICA.

La infraestructura tecnológica de procesamiento del Centro de Datos, tiene como finalidad proveer los diferentes servicios tanto dentro como fuera del INOCAR, los que tienen un nivel de criticidad alto, al

soportar fuertemente muchos de los procesos considerados claves dentro del Instituto.

Siguiendo con el esquema propuesto en éste trabajo, a fin de evitar que la infraestructura tecnológica se vuelva compleja, con múltiples soluciones por doquier, se implementó un esquema estandarizado, estructurado y ordenado. Este esquema provee un ambiente con ciertos niveles de disponibilidad, seguridad, escalabilidad y facilidad de administración, considerados adecuados para las necesidades del INOCAR. El esquema consideró además los recursos tecnológicos existentes en el Instituto, a fin de que sean reutilizados.

La **disponibilidad** del esquema está reforzada por ciertas características de redundancia, y, mecanismos de respaldo y restauración que permitan recuperar el sistema en caso de caídas y otros tipos de desastres que pudieran afectar a la información. Hasta donde sea económicamente posible se ha evitado puntos únicos de falla.

La **seguridad** del esquema proviene de una defensa establecida en profundidad con tres zonas: pública (Internet), restringida (Intranet Naval) y privada (Intranet del INOCAR). Las zonas están controladas

a través de un Firewall basado en software, listas de control de acceso en servidores pasarela (“gateways” con Proxy) y segmentación de la red a través de Redes Locales Virtuales (VLANs).

La **escalabilidad** está garantizada por el empleo de tecnología abierta comercial, que permita el aumento de la capacidad de procesamiento aumentando nodos en el sentido horizontal a los cluster o aglomerados de servidores. De igual manera la división de la infraestructura de procesamiento en: presentación, procesamiento de reglas de negocio y almacenamiento de datos; brinda la facilidad para escalar en la medida que las necesidades aumenten.

La infraestructura tecnológica de procesamiento está organizada en zonas de confianza o seguridad. Estas zonas son redes de servidores limitadas por firewalls, mediante los cuales se limitan los protocolos de comunicaciones y se regula el tráfico entre una red y otra. Básicamente tenemos tres zonas de confianza:

- **Zona Desmilitarizada Pública (DMZ Pública).-** Infraestructura que soporta los servicios que son accesibles desde el Internet por cualquier usuario.

- **Zona Desmilitarizada Privada (DMZ Privada).-** Infraestructura que soporta los servicios que son accesibles desde el Intranet Naval, incluyendo el segmento privado del Instituto.

- **Zona Militarizada (MZ).-** Infraestructura que únicamente es accesible por determinadas personas o recursos debidamente autorizados.

En la Figura 5.3, 5.4 y 5.5, se muestra el esquemático de la infraestructura tecnológica de procesamiento del Instituto:

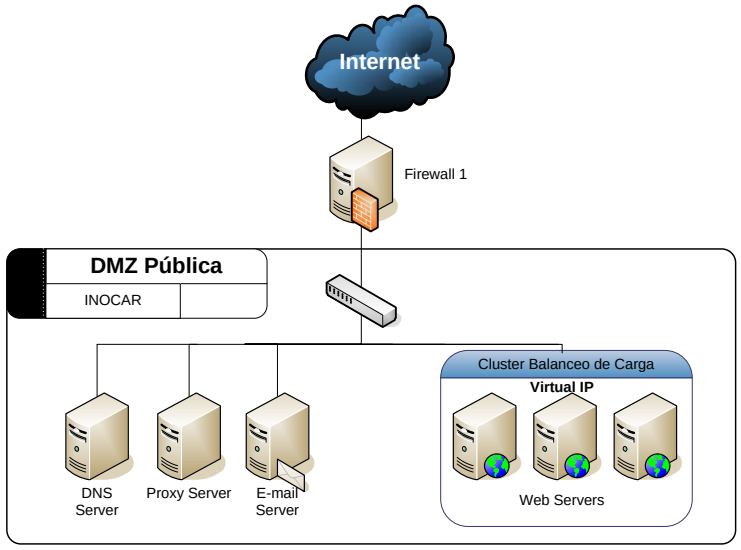


FIGURA 5.3. INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO DE LA DMZ PÚBLICA DEL INOCAR

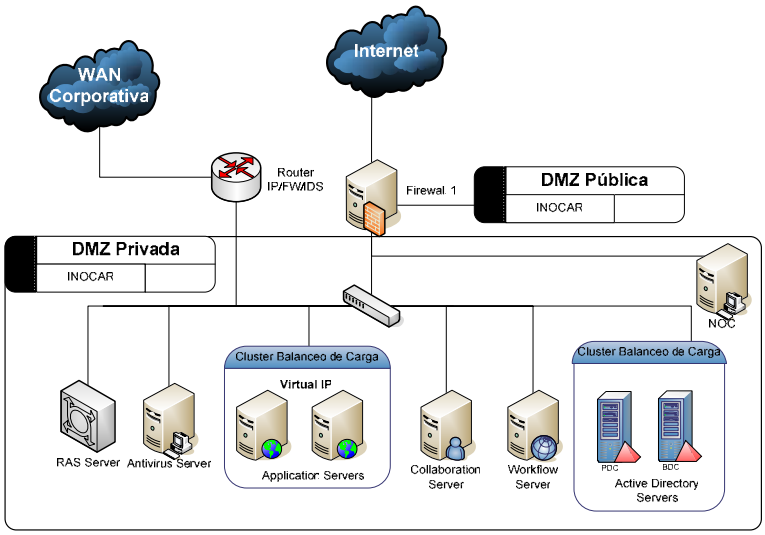


FIGURA 5.4. INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO DE LA DMZ PRIVADA DEL INOCAR

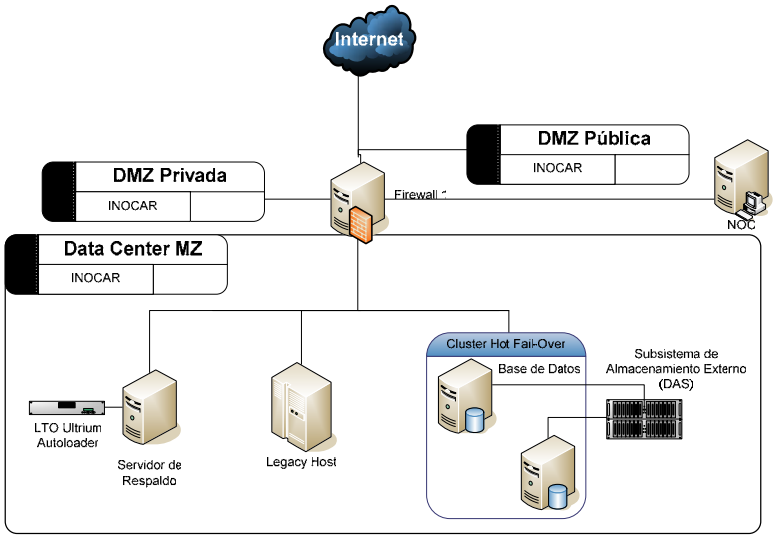


FIGURA 5.5. INFRAESTRUCTURA TECNOLÓGICA DE PROCESAMIENTO DE LA ZONA MILITARIZADA DEL INOCAR

Red de Datos

La red de datos del INOCAR está basada en una combinación de varios elementos y tecnologías de networking, conforme a la realidad física de la distribución de las áreas funcionales en varios edificios, tal como se muestra en la Figura 5.6:

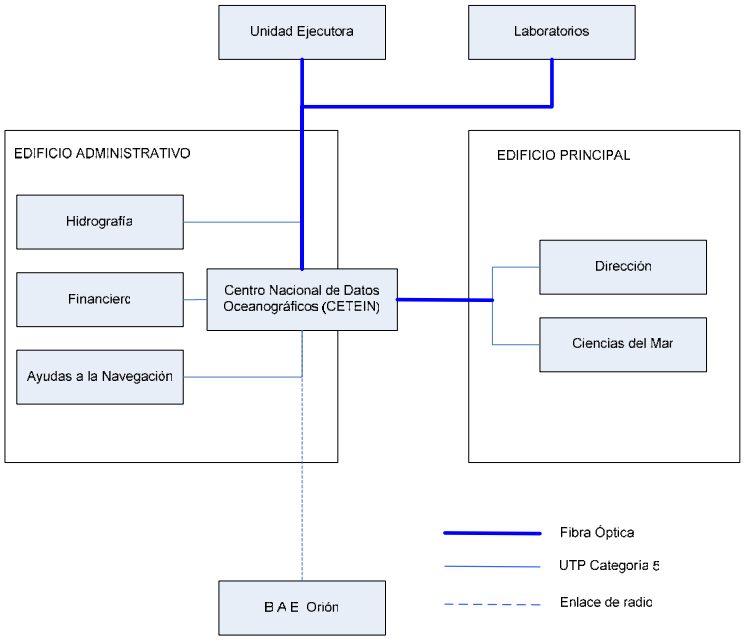


FIGURA 5.6. DISTRIBUCIÓN ORGANIZACIONAL Y DE EDIFICIOS DEL INOCAR

Para cubrir las necesidades de los usuarios de los servicios informáticos ofrecidos en el INOCAR, se ha implementado una red de datos basada principalmente en tecnología Fast Ethernet, con

segmentos que tienen tecnología Gigabit Ethernet. En cada edificio la red es de cableado estructurado UTP categoría 5, con una topología tipo estrella. Los segmentos de red de cada edificio son interconectados en el switch principal a través de enlaces de fibra óptica que colapsan en un switch central. El Buque Hidrográfico – Oceanográfico “ORION” se enlaza a la red a través de una radio enlace de espectro ensanchado. Así mismo, se cuenta con un servidor de accesos para la interconexión bien sea a través de la red telefónica privada del sistema de telecomunicaciones de las Fuerzas Armadas (Red MODE), redes telefónicas públicas o redes celulares, de las estaciones de sensoramiento remoto a lo largo del litoral ecuatoriano. En la Figura 5.7 se muestra el modelo esquemático de la solución implantada.

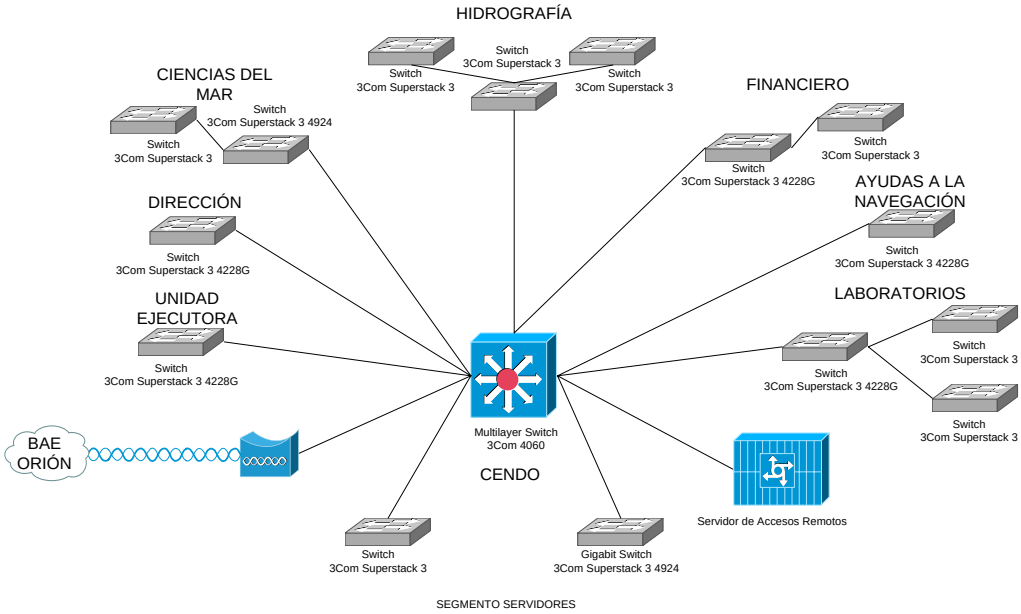


FIGURA 5.7 DIAGRAMA ESQUEMÁTICO DE LA RED DE DATOS IMPLEMENTADA EN EL INOCAR

En la Tabla XVI se describe con mayor detalle la infraestructura de tecnológica de procesamiento implementada para la solución informática del INOCAR.

TABLA XVI

EQUIPOS DE LA INFRAESTRUCTURA INFORMÁTICA DE PROCESAMIENTO DEL INOCAR

Dependencia de Servicios	**Detalles Específico del Servicio**	
Servicios de Mensajería Electrónica	Provee los servicios de mensajería electrónica a todos los usuarios del Instito a través de los estándares POP3, IMAPv4, SMTP. **Software.-** Código abierto: Linux, SendMail y Squirrel para proveer WebMail. Soporte e-mail relay Server.	
	Hardware.- Plataforma Intel / Linux	
	CPU	(2) Xeon 2.4 Ghz, 512 Kb Caché L2
	RAM	2 Gb / 4 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio mail. (3 x 72 Gb) Internos en RAID 5 para las cuotas de almacenamiento de los usuarios.
Servicios Web y HTTP	Para páginas HTML/XML, soporte de Servlets y JavaServer Pages (JSPs) y soporte a servicios web; a través del servidor Web HTTP. **Software.-** Código abierto: Linux, Apache y Tomcat.	
	Hardware.- Plataforma Intel / Linux; Servidores típicamente con buenas capacidades de procesamiento y memoria RAM.	
	Cluster	3 Nodos
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	2 Gb / 4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio http.
Consola Antivirus	Servidor de actualizaciones de definiciones de virus informáticos para actualización interna del software antivirus. **Software.-** Mc Affe.	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb Caché L2

Dependencia de Servicios	**Detalles Específico del Servicio**	
	RAM	512 Mb/ 4 Gb
	NIC	(2) 10/100 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1
Servidor Proxy	Configuración Proxy para caching de páginas web externas, y autenticación, autorización y accountability (rendición de cuentas) de usuarios. **Software.-** Código abierto: Linux, SQUID, ARP.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(3 x 72 Gb) Internos en RAID 5 para sistema operativo y servicios Proxy.
Servidor DNS	Servicio de resolución de nombres de dominio. **Software.-** Código abierto: Linux, SQUID.	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	1 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicios.
Firewall	Mecanismo de control de flujo entre dos redes, normalmente una protegida y otra no confiable. Firewall 1 de Checkpoint	
	Arquitectura	Basado en Software
	ACL	Creación de Listas de Control de Acceso
	Análisis	Inspección de paquetes en tiempo real
	NAT	Network Address Translation
	Otras:	Reporte automático de actividades, SNMP, VPN, prevención ataques DoS, Mail Relay y filtrado de URL.
Servidor de Aplicaciones	Cluster de balanceo de carga, para ejecutar el servidor J2EE. **Software.-** IBM Websphere Application Server Enterprise Edition.	
	Hardware.- Plataforma Intel Itanium 2 / Linux AS	
	Cluster	2 Nodos

Dependencia de Servicios	**Detalles Específico del Servicio**	
	CPU	(2) Itanium 2 1.3 Ghz, 256 Kb Caché L2, 3 Mb. Caché L3.
	RAM	8 Gb / 16 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo, servidor de aplicación y aplicaciones implantadas.
Servidor Colaborativo	Servidor de Gestión de Contenidos. **Software.-** Linux AS / BeeBox.	
	Hardware.- Plataforma Intel Xeon / Linux AS	
	CPU	(2) Xeon 3.0 Ghz, 512 Kb Caché L2.
	RAM	4 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación. (3 x 72 Gb) Internos en RAID 5 para datos.
Servidor Workflow	Servidor de Workflow para automatización de la gestión administrativa. **Software.-** Windows 2003 Server / Domino Workflow.	
	Hardware.- Plataforma Intel Xeon	
	CPU	(2) Xeon 3.0 Ghz, 512 Kb Caché L2.
	RAM	4 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación. (3 x 72 Gb) Internos en RAID 5 para datos.
Servidor de Directorio	Servidor de Directorio y Dominios. **Software.-** Windows 2003 Server con Active Directory.	
	Hardware.- Plataforma Intel Xeon	
	CPU	(2) Xeon 3.0 Ghz, 512 Kb Caché L2.
	RAM	2 Gb

Dependencia de Servicios	**Detalles Específico del Servicio**	
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y datos.
Servicio de Administración de Infraestructura	Administración de los dispositivos de la infraestructura tecnológica, basado en SNMP, para captura y presentación de variables SNMP de los diferentes dispositivos de procesamiento y red de la infraestructura; captura de mensajes de error / advertencias de los dispositivos de red y control de dispositivos de tiempo de la red. Verificación en tiempo real de parámetros de broadcast / multicast / unicast de la red. Autenticación a dispositivos críticos de la red a través de RADIUS/TACACS. Servidor de acceso a dispositivos de red vía SSH. Servidor de monitoreo de servicios. **Software.- (W2K-AS) – Software Unicenter de Computer Associates**.	
	Hardware.- Plataforma Intel Xeon	
	CPU	(2) Xeon 3.0 Ghz, 512 Kb Caché L2.
	RAM	1 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 72 Gb) Internos en RAID 1 para sistema operativo y aplicación.
	Servidor de sniffing de la red (W2KAS – LAN Explorer)	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb L2
	RAM	512 Mb
	NIC	(2) 10/100/1000 Mbps
	HD	(2 x 36) Internos en RAID 1 para sistema operativo y aplicación
	Monitoreo de servicios: RADIUS/TACACS/NTP/MRTG/SSH – Linux	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb L2
	RAM	512 Mb
	NIC	(2) 10/100/1000 Mbps
	HD	(2 x 36) Internos en RAID 1 para sistema operativo y aplicación
Servicios de Gestión de Datos	Servidores de base de datos. **Software.-** Oracle 9i DB Enterprise Edition.	
	Hardware.- Plataforma Intel Itanium 2 / Linux AS	

Dependencia de Servicios	**Detalles Específico del Servicio**	
	CPU	(2) Itanium 2 1.3 Ghz, 256 Kb Caché L2, 3 Mb. Caché L3
	RAM	8 Gb / 16 Gb.
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y motor de base de datos.
Servidor de Almacenamiento	Dispositivo de almacenamiento conectado a los servidores de base de datos directamente (Direct Attachment Storage – DAS) para lectura / escritura de bloques de datos. **Software.-** Software de gestión del almacenamiento, configuración de arreglo, control de acceso, replicación, snapshots, snapclones, expansión en línea y cambio del nivel de RAID.	
	Capacidad de almacenamiento real inicial instalada	0,5 Tb
	Capacidad de almacenamiento real máxima	3 Tb
	Controlador	Doble controlador SCSI Ultra 320 independientes.
	Fuente de Poder	Redundante
Servicios de Respaldo	Servicios de Respaldo/Restauración de Información para los distintos servidores del Data Center, de alto desempeño, con características de calendarización para respaldar en línea base de datos y archivos abiertos. **Software.-** Windows 2000 Server y HP OpenView Data Guard	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	1 Gb
	NIC	(1) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación de respaldo.
	Unidad de Respaldo en Cinta	
	Drives	1 / 2
	Tecnología	LTO Ultrium 2

Dependencia de Servicios	**Detalles Específico del Servicio**	
	Capacidad nativa	3 Tb
	Autoloader	Mínimo 8 cartuchos
	Desempeño	30 Mb/seg
	MCBF	> 250.000 horas
	MTBF	> 100.000 horas
Servicios de Gestión de Datos Legado	Servidor de base de datos del Sistema Administrativo Financiero. **Software.-** Informix Enterprise Dinamic Server.	
	Hardware.- Plataforma RISC / AIX	
	CPU	(2) PowerPC II 160 Mhz
	RAM	512 Mb
	NIC	(2) 10 / 100 Mbps
	Fuente de Poder	Redundante
	HD	(5 x 2,2 Gb) Internos en RAID 5 para sistema operativo, motor de base de datos y datos. Incluye CD Óptico para respaldo.

CONCLUSIONES Y RECOMENDACIONES

A continuación se presentan las conclusiones obtenidas al realizar éste trabajo:

1. CON RELACIÓN A LAS PREGUNTAS FORMULADAS:

Éste Trabajo aportó a la resolución de las interrogantes planteadas al inicio de su desarrollo, especialmente en el Capítulo 1, dentro del contexto de cómo la “Era de la Información” representa tanto retos como oportunidades para una Organización en búsqueda de su excelencia. El impacto de las TIC (Tecnologías de la Información y Comunicación) como medio evolutivo, son inductores de revoluciones organizacionales.

¿Qué es el Intranet?

Apartándose del rigor estricto de una definición técnica del Intranet como una infraestructura tecnológica de comunicaciones, basadas en los estándares globales de comunicación y los protocolos del Internet; podemos concluir que desde el punto de vista del contenido, una Intranet

es el conjunto de información compartido por una comunidad de usuarios dentro de la Organización. El Intranet guarda similitud con la electrónica de estado sólido, facilitando el surgimiento de arquitecturas de software para ambientes distribuidos, que explotan las capacidades de procesamiento del lado del servidor y favorecen la reutilización de código. Al igual que los circuitos integrados, que permiten pensar en funciones y no en detalles de implementación, estas arquitecturas de software han permitido el surgimiento de un mercado de componentes de uso comercial (COTS) para una gran variedad de problemas comunes.

¿Cómo voy a acceder a la información?

Siendo consecuentes con los hechos y realidades analizadas en el presente trabajo, el principal habilitador de la “Era de la Información” es el Web. Es la nueva imprenta de Gutenberg para el siglo XXI. El Web rompe las barreras para que la persona común pueda publicar y leer la información en el mundo de la información digital sin depender de un programador. Esta información soportada por una infraestructura de procesamiento, a través de las redes y un adecuado esquema organizacional conforman el Intranet. El Intranet aumenta la velocidad y el alcance de la producción y consumo de información de modo que ésta fluya por toda la organización. El empleo del navegador web, y la adecuada implementación de la Intranet conforme a lo propuesto,

permitirán a la Armada eliminar la información del tipo “por sí acaso” reduciendo la sobrecarga de información. En vez de empujar la información desde la producción al consumo, se promueve el consumo de información “bajo demanda” o “justo a tiempo”. Para esto se habilita y/o construye los sistemas de información bajo una arquitectura distribuida centrada en el Web, empleando al navegador como cliente universal que es relativamente fácil de utilizar. Este modelo de arquitectura soporta el control distribuido, la publicación, el acceso y el manejo de la información en múltiples formatos, sin depender de la complejidad de los grandes sistemas de información centralizados; siendo transparente para el usuario que tipo de aplicación, sistema o plataforma es la fuente que atiende su demanda; y facilitando el mantenimiento y sostenimiento de los sistemas.

¿Cómo voy a controlar el acceso a la información?

Las características propias en cuanto a la restricción y control de acceso a la información en una organización militar, implica que sea necesario contar con mecanismos tecnológicos a nivel de los diferentes elementos de hardware (procesamiento y transmisión), software y datos; que permitan mitigar los riesgos y las amenazas a las que se ven expuestas las infraestructuras informáticas actuales, de modo que se garantice la disponibilidad, confidencialidad e integridad de la información en el Intranet, tendiendo a que el sistema tenga alta fiabilidad.

Los mecanismos propuestos permiten mantener un control centralizado de la seguridad a nivel de almacenamiento y transmisión. Al no contar aún con una doctrina adecuada para la información digital, emitida por la Dirección de Inteligencia como organismo competente en cuanto a recomendaciones de seguridad, se han propuesto esquemas muy generales que permitan considerar herramientas para la confidencialidad, como son el empleo de claves asimétricas; herramientas de autentificación, como son las claves de una sola vida; herramientas de no repudio, como son las firmas digitales; herramientas de control de flujo en redes, como son los Firewall; y otras herramientas tendientes a mitigar los riesgos asociados a la infraestructura propuesta.

¿Quién decide que información debe ser controlada?

El enfoque que se ha cubierto en el presente trabajo, al referirse al Intranet, está basado más allá de la infraestructura tecnológica, en una infraestructura organizacional. El marco de trabajo propuesto, es eminentemente una transformación organizacional de roles y funciones, es una conversión de trabajadores funcionales en trabajadores del conocimiento. Los roles propuestos como parte de éste marco de trabajo: Administrador del Web, Webmaster, Publicadores, Editores y Autores; así como los roles organizacionales: Consejo Organizacional del Web, Comité Técnico del Web, y el Foro Editorial; en conjunto permiten habilitar una

organización funcional con capacidad de toma de decisiones distribuidas y control y coordinación centralizado. Aplicando la política de seguridad a establecerse, existirán tanto mecanismos tecnológicos, como entes funcionales capaces de determinar que información debe ser controlada dentro de cada grado de libertad, sin mermar la capacidad de compartir información como inductor del cambio requerido para habilitar la innovación.

¿Cómo voy a saber que calidad de información tiene el web de la Organización?

Como principio básico en que se basa la cultura de la calidad total, el primer mecanismo es el control en la fuente. Esto se logra con la aplicación de la metodología propuesta para el desarrollo de la información para el Web, reconociéndolo como un medio de comunicación diferente a los tradicionales, ya que reconoce la naturaleza de la información como un algo dinámico y no estático; y tiene además alta interactividad. La metodología hace un estudio de la audiencia pretendida, como eje central para el desarrollo de la información. A partir de ello, se plantea un propósito, se definen los objetivos, se estudia la información disponible de la audiencia pretendida, y la información del dominio.

Por otro lado la existencia de un Foro Editorial, habilita a la Organización con una estructura funcional capaz de impedir que se publique cualquier

cosa, de modo que a diferencia de lo que sucede en el Internet, el Intranet mantiene una calidad de la información para que ésta sea una verdadera base de conocimientos.

¿Cómo voy a mantener la explosión de generación de la información?

Uno de los problemas centrales a resolver, es la complejidad de la Organización cuyo modelo de gestión ha sufrido los efectos de la latencia organizacional, la inercia y la deformación. Los paradigmas de mando y control centralizado, y las prácticas burocráticas poco saludables, degradan la capacidad de adaptación de la organización a un entorno globalizado, altamente dinámico, volátil y complejo. Para ello se requiere adoptar una visión sistémica del problema, y permitir que la Organización tienda a reordenarse en subsistemas autorregulados menos complejos, descentralizando así la toma de decisiones, habilitando mejores canales de comunicación, promoviendo una infraestructura con enorme capacidad coordinadora, sin que esto represente la pérdida de control gracias a la centralización de la coordinación y comunicación. La innovación adaptiva adecua las capacidades organizacionales para que exista un desempeño diario conducido por propósitos. Bajo éste esquema habilitador, y la enorme capacidad de compartir información de manera simple, sencilla y de bajo costo, la revolución se iniciará y la cantidad de conocimiento

organizacional reconocido, capitalizado, gestionado y compartido irá en aumento cada día más.

¿Cuáles son las características de las aplicaciones empresariales de la próxima generación? ¿Cómo las puedo hacer útiles para mí?

Los sistemas de información empresariales, deben ser capaces de explotar la velocidad, desempeño, seguridad y confiabilidad de la computación centrada del lado del servidor. Los modelos de despliegue orientados a la consolidación de servidores en un Data Center, se ajustan a resolver las principales necesidades de la Armada. Considerando las alternativas existentes en cuanto a arquitectura de software, en modelos o marcos de referencia de computación distribuida, es decir la plataforma J2EE y Microsoft .Net; la decisión se ve condicionada a ofrecer un ambiente de cómputo seguro. En el análisis podemos determinar que la plataforma Microsoft al no ser portable, está basada en el sistema operativo Windows, el cual como es públicamente conocido adolece de problemas de seguridad. Los principales virus informáticos y vulnerabilidades son descubiertos en Windows. Siendo la disponibilidad un factor importante a considerar, y buscando siempre la posibilidad de no depender de una plataforma específica, la decisión se inclina a una combinación de los procesadores Intel Itanium 2, como alternativa de alto poder de procesamiento, con una clara tendencia a ser un estándar de la

industria comercial y por tanto de bajo costo. Esto combinado con el sistema operativo Linux como una opción de Unix válida y probada ampliamente en los diferentes roles: base de datos, servidor de aplicaciones, servidores web, servidores de archivos, etc. Independiente de tecnología propietaria como son otras opciones comerciales de Unix: AIX, HP-UX y Solaris. Finalmente la plataforma J2EE es una opción madura, un compromiso de la industria con amplia participación de los principales fabricantes de software del mundo, que en cuanto a aplicaciones distribuidas tiene apego a estándares derivados de CORBA, es interoperable con otros ambientes, incluyendo sistemas de información empresariales como ERPs, y esencialmente portable al ser independiente de plataforma. La plataforma J2EE está basada en componentes, lo que facilita la reutilización para aumentar la efectividad de los equipos de desarrollo, y provee a través de los contenedores servicios de sistema cuya complejidad es abstraída permitiendo a los equipos de desarrollo concentrar su esfuerzo en la resolución del problema desde el punto de vista de las reglas del negocio. El portafolio ofrecido como parte de la plataforma J2EE incluye la implantación de servicios web, así como también soporte a equipos de próxima generación o móviles a través de J2ME (Java 2 Micro Edition).

¿Qué es seguridad en una red?

En términos prácticos, al hablar de seguridad no podemos considerar ésta como un hecho, un resultado, un estado, un fin. La seguridad es un proceso, es un “que hacer” permanente que busca que la información que se transmite en la red esté donde y en el momento que uno la requiera. Que sea confiable y precisa, que no esté al alcance de personas no autorizadas y que estemos seguros de que no ha sido alterada. Las características actuales de un mundo interconectado, trae ventajas y desventajas. La realidad de éste entorno exponen de manera continua nuestras infraestructuras tecnológicas a un medio bastante hostil, en donde la seguridad tiene que basarse en análisis que permitan mitigar los riesgos más probables y críticos, puesto que no es posible ni factible dedicar recursos para el todo. Podemos concluir que el enfoque general, macro y teórico de una política de seguridad debe obedecer a una implantación conforme a la norma ISO 17799, pero que en la práctica debe estar orientada a mantener la fiabilidad de la Intranet.

¿Cómo una organización puede soportar efectivamente la dirección de actividades hacia sus metas sin alguien a cargo?

El cambio de paradigma hacia una toma de decisiones distribuida, descentralizando el mando y control, tiene un cuerpo en teoría. La centralización de las comunicaciones mantiene la coordinación, sin

depender de un flujo de información vertical que induce prácticas burocráticas poco saludables. El Intranet facilita la implantación de procesos horizontales y estructuras “funcionales” planas, reduciendo las barreras interdepartamentales. En el caso de la Armada como organización militar, la estructura jerárquica no puede ser omitida ni reemplazada, pero podemos concluir que existen al menos dos roles funcionales a nivel de la Institución: un rol de gestión y un rol operacional. El rol operacional tiene que ver con el cumplimiento de la misión básica relacionada con la defensa nacional, el que obedece a la doctrina y al entrenamiento de la Armada en operaciones militares, donde prima la estructura jerárquica, la organización por tareas y la cadena de mando. El rol de gestión en cambio es el que se ve favorecido tremendamente por el Intranet, puesto que es en la gestión de la institución donde tenemos las mayores reservas de mejoramiento, donde se pueden reducir drásticamente tiempos y costos innecesarios, facilitando un funcionamiento ordenado y coordinado, soportado en la visión general de la información.

¿Cómo podemos tener una organización que aprende, si basamos nuestros procesos en una estructura rígida? ¿Cómo podemos aprender algo nuevo? ¿Cómo podemos aprender de manera radical nuevas cosas?

La mayoría de hechos trascendentales en la historia de la humanidad están relacionados con un cambio radical de paradigma, una especie de salto cuántico que rompe las reglas hasta entonces vigentes, para instaurar una nuevas. Por tanto la clave de los grandes logros no está sencillamente en modificar el comportamiento, ni modificar la actitud, sino que es necesario cambiar la manera de "ver" al mundo, cambiar de paradigma, dejar de lado los supuestos. Un medio como una Intranet permite compartir ideas y difundir información, someter a consultas y trabajar colaborativamente, dejando de lado las barreras del tiempo y del espacio, que han limitado a otros medios, especialmente los basados en papel. La cantidad de ideas compartidas a su vez son fuente de surgimiento de nuevos paradigmas. Estos nuevos paradigmas no pueden ser explorados cada tres años (vigencia típica de un plan estratégico), ni siquiera cada año. Deben ser explorados permanentemente a fin de garantizar la sobre vivencia de las organizaciones y la prosperidad en un mundo turbulento como el que vivimos en la actualidad. Cada día enfrentamos un nuevo desafío, el cual exige una respuesta que esté a su altura. En la Armada cuando la respuesta es igual o superior al desafío,

nos estaremos acercando al éxito. El problema común es que cuando surge un desafío nuevo y más grande, la tendencia natural es recurrir a los patrones, a los procesos y a las prácticas que han concluido en éxito en el pasado. Sin embargo, difícilmente estos patrones, procesos y prácticas vuelven a ser igual de útiles, no solo por la dinámica de las variables que configuran una determinada situación, sino por la sinergia de éstas, jamás una situación es igual a otra. Lo más radical es que mientras en el pasado la información alguna vez fue autocrática y prerrogativa de unos pocos privilegiados, hoy en día se ha democratizado a nivel universal y hay una demanda irreprimible de sistemas participativos y democráticos en todos los sectores de la sociedad, incluyendo Fuerzas Armadas. Para gestionar el conocimiento de la organización, debemos concienciar que el aprendizaje es una actividad individual. Debemos ser capaces de aprovechar la mente, el cuerpo, el corazón y el espíritu de las personas, y demostrar que nuestro liderazgo es reconocido como arte de facultar y comunicar a las personas su valor y potencial de modo que inspiren comportamientos. En esencia, el hecho es que el capital humano, intelectual y social, es el activo más valioso de la Armada. La aplicación de paradigmas que permitan mayor participación liberará este potencial en los nuevos trabajadores del conocimiento, ávidos de aprender algo nuevo, de encontrar nuevos paradigmas, de mejorar.

¿Qué camino nos llevará al éxito en la nueva economía digital?

El Internet ha cambiado definitivamente la forma de competir, la velocidad de las acciones, la naturaleza del liderazgo y la forma de interactuar en la sociedad. Si el Internet afecta a un macro mundo inmerso en una economía globalizada afectada principalmente por los adelantos tecnológicos, el Intranet incide en la capacidad de las organizaciones, sean éstas empresariales, gubernamentales o sin fines de lucro, para interactuar e integrarse con más ventajas que desventajas. El empleo adecuado de las TIC deben ser la base de la innovación de una Organización. El contar con buena información es un Factor Diferenciador básico para la innovación. Una Fortaleza Organizacional basada en un Factor Diferenciador, genera una Ventaja Comparativa (para organizaciones sin fines de lucro o gubernamentales) ó Competitiva (para organizaciones empresariales).

2. CON RELACIÓN A LA OBSERVANCIA DE PRINCIPIOS:

Latencia organizacional – descentralizar la organización.

Resulta claro que una organización piramidal, adolece de prácticas burocráticas poco saludables, no adecuadas para un entorno dinámico, volátil e impredecible (Ejemplo: Qué pasó el 11 de Septiembre, porqué pese a contar con indicios de una amenaza, la enorme estructura del

gobierno federal de Estados Unidos no fue capaz de reaccionar oportunamente). Una organización que se mantenga aferrada a un modelo de gestión con toma de decisiones centralizadas no tiene capacidad de adaptación, no se puede anticipar a los cambios y tendrá grandes problemas para sobrevivir. Por otro lado, una organización militar a pesar de tener doctrina, política y procedimientos que permiten la toma de decisiones en los diferentes niveles; no se la concibe desde el punto de vista de intentarla transformar para hacerla plana, horizontal. Esto atenta contra la integridad de la cadena de mando y la jerarquización propia de una organización militar. El Intranet al proponer una toma de decisiones distribuida, con una capacidad de comunicar, coordinar y por ende controlar, centralizada; permite mantener una visión íntegra de las decisiones que se toman en los diferentes niveles, en tiempo real. Permite aerodinamizar la gestión sin perder la autoridad.

La información conduce las funciones vs. las funciones generan información.

Se busca un cambio cultural. Cuando nos centramos en la información que generan las funciones, estamos hablando de analizar el pasado y de tener una actitud principalmente reactiva. Cuando nos concentramos en las funciones que podemos emprender basados en la información disponible, estamos hablando de anticiparse al futuro, anticipar el cambio, ser

proactivos. El rol de los administradores ahora no está directamente relacionado con la capacidad de producción de las personas y de los equipos a su cargo. Está principalmente relacionado con la capacidad de generar y gestionar el conocimiento. Si la contribución más importante de la gerencia en el siglo XX fue incrementar la productividad del “trabajador manual” en las plantas de producción; la contribución más importante que deberá hacer la gerencia del siglo XXI será incrementar en igual proporción la productividad del “trabajador del conocimiento”.

Empujar información (push) vs. halar información (pull).

En términos generales podemos concluir que para la publicación de la información empleamos el principio de halar la información (pull), y para la notificación el principio de empujar la información (push).

Empujamos información cuando necesitamos que ésta sea conocida al instante y/o cuando la información tiene un tiempo de vida útil corto.

Halamos la información cuando se trata de información que será importante y por tanto referenciada en el futuro, o que puede tener un acceso concurrente elevado.

Siempre que se emplee el principio de empujar la información, el usuario o destinatario debe mantener el control del mecanismo. Esto implica el uso de agentes, o la capacidad de suscribir y anular suscripción a la distribución.

Soporte al auto – servicio vs. soporte al hágalo por mí.

El modelo de comunicaciones tiene mucha influencia en la actitud personal, y a partir de ésta en el comportamiento organizacional. El principio de empujar o halar información, determinan en gran parte la actitud de los usuarios respecto a los sistemas de información. En el esquema de empujar, el usuario espera ser servido, confía en que alguien determinó sus necesidades de información y se centra en cumplir con las tareas y responsabilidades expresamente determinadas para él. En el esquema de halar, el usuario determina por sí mismo que información necesita y la consigue; puede en base a ésta información disponible, normalmente incrementar su conocimiento y modificar sus tareas y responsabilidades, buscando siempre un mejoramiento continuo, lo que implica a su vez la necesidad de buscar más y nueva información.

Comunicación y coordinación vs. comando y control; Tomas de decisiones distribuidas vs. control central.

La comunicación y coordinación se enriquece, aumenta su utilidad cuando está centralizada; se degrada cuando no está integrada. El Intranet integra la comunicación de las diferentes áreas de la Organización, a través de medios normalmente más económicos que los tradicionales; por otro lado tiene la gracia de basarse en un modelo de comunicación y coordinación centralizada.

El comando y control se enriquece, cuando es efectivo; esto implica ser eficiente y eficaz; implica hacerlo con poco esfuerzo y recursos, pero logrando los resultados deseados. En una toma de decisiones distribuida se tiene mejor oportunidad de hacer las cosas bien, porque los niveles operativos están cerca de los problemas y perciben probablemente mejor las soluciones. El comando y control se degrada sino cuenta con una capacidad de distribuir la toma de decisiones y controlarla. La Intranet se presta para facilitar la toma de decisiones descentralizada y brindar capacidad de control centralizado a cualquier punto de acceso a la red.

Acceso a la información vs. calidad de la información.

Al emplear los estándares de comunicación y de contenido del Internet, el acceso a la información en una Intranet es relativamente fácil y sencillo. Cualquier usuario con acceso a un navegador Web como cliente universal, y suficientes derechos de acceso es capaz de acceder a la información. La diferencia sustancial entre el Internet y la Intranet, como bases de conocimiento, radica justamente en la calidad de la información. En el Intranet los roles para la administración y los roles organizacionales, en conjunto con la metodología propuesta para la creación de contenido en los sitios Web, y los mecanismos de seguridad adecuados, garantizan la calidad de la información disponible.

Contexto de la información vs. contenido de la información.

El empleo de palabras clave, o tecnología que permita la autodescripción del contenido, permite gestionar la información por contextos. A pesar de que máquinas de búsqueda como google, utilizan algoritmos de redes neuronales, e inteligencia artificial para tratar los contextos de la información, es un área que aún ofrece expectativas y no está al alcance real de su empleo en una Organización. Los mecanismos autodescriptibles al estar siendo adoptados por las bases de datos, permitirán que la metadata disponible en los repositorios de contenido, sirva como medio para habilitar la gestión de contenido por contextos.

Estandarización del conocimiento.

La principal utilidad del Intranet como medio para establecer una base de conocimientos corporativos, es el reconocer que el conocimiento organizacional depende del conocimiento de los individuos, es decir, si los individuos se van, el conocimiento se pierde. Al estandarizar el contenido de información relacionado con los trabajadores “del conocimiento”, se provee un mecanismo de estandarización flexible que permitirá identificar, capitalizar y gestionar el conocimiento organizacional.

Explotación de lo desconocido.

Mediante la propuesta hecha en éste trabajo, probablemente podemos concluir que fue predecible el esfuerzo para determinar que infraestructura tecnológica es necesaria para el Intranet; así como también el marco de trabajo de gestión del Intranet. Pero estos son los medios provistos, son las herramientas evolutivas para que la organización enfrente la “Era de la Información”. Pero resulta totalmente desconocido saber que revolución se desencadenará. Sin embargo la capacidad de compartir ideas y conocimiento en el Intranet, casi con seguridad permitirá explotar las oportunidades que se presenten al momento de todos éstos cambios.

3. CON RELACIÓN A LOS OBJETIVOS:

A continuación reflexionaremos como éste trabajo logró cumplir con los objetivos planteados:

Definir las necesidades para la organización y administración de la información formal de la Armada justificando el uso de la tecnología de Intranet.

Se consiguió realizar un análisis de cómo el modelo de gestión actual de la Armada como causa raíz, limita sus posibilidades de cumplir satisfactoriamente cada vez más funciones encargadas, con menos recursos. Si no se actúa de manera frontal logrando el cambio de paradigmas propuesto, no se podrá eliminar la causa que genera las limitaciones propias de una organización burocrática en un entorno tan cambiante y volátil como el que define la economía global actual

dependiente en gran parte del empleo adecuado de las TICs. Este cambio de paradigmas permite contar a la Institución con un marco de trabajo que surge como parte de un enfoque sistémico que considera especialmente a las personas como capital intelectual de la organización, a los procesos como hilos conductores del cambio, a la estructura en donde sin alterar la jerarquización ni la línea de comando, se propone como artificio una estructura funcional plenamente vigente para el rol de gestión de la Institución separado del rol operacional, y finalmente a la tecnología de información, considerando los aspectos de procesamiento, conectividad, software base, arquitectura y demás elementos que son parte de la propuesta basada en Intranet.

Definir las políticas, estándares y arquitectura para la elaboración de sistemas de información basados en el Web a nivel de la Armada en un plan estratégico que contemple el marco de futuros desarrollos informáticos.

Se formuló un modelo de computación a nivel institucional que considera las políticas adecuadas y convenientes que permitan mantener un ambiente confiable, seguro, centralizado, para reducir los costos de tenencia de la solución, donde la consolidación del ambiente de procesamiento y desarrollo, permitirá optimizar el uso de los recursos humanos y materiales disponibles. La solución basada en una arquitectura definida que emplea la plataforma J2EE, en un modelo de computación distribuida son los componentes tecnológicos que se emplearán para las soluciones de los sistemas de información propuestos como parte del Plan Estratégico de Sistemas de Información. Este Plan Estratégico de Sistemas es una reacción al Plan Estratégico Institucional, y contempla los principales sistemas de información requeridos por los diferentes sectores en base al análisis funcional realizado a la Institución.
En concreto, teniendo al Plan Estratégico Institucional como finalidad; y las

personas, los procesos, la estructura organizacional y la tecnología de información, como un todo; conformamos el gran sistema de información organizacional.

Definir los requerimientos básicos de infraestructura tecnológica, seguridad y disponibilidad que permitan un control centralizado sobre los sistemas de información.

Se determinó una infraestructura tecnológica de procesamiento y conectividad, consolidada en un Data Center, basada en la realidad de los medios de transmisión disponibles y conforme a su topología física. Ésta infraestructura considera las mejores prácticas para minimizar los riesgos asociados, considerando los mecanismos de seguridad que permitan garantizar una alta fiabilidad de la infraestructura. Además considera una administración totalmente centralizada con capacidad de satisfacer niveles de servicio superiores a los disponibles actualmente de manera local en cada reparto. En el modelo propuesto, el Centro de Tecnología de Información es el responsable de proveer los servicios informáticos requeridos por los diferentes repartos, estando a su cargo los segmentos de procesamiento central y conectividad; el reparto mantiene el segmento de usuario final, en lo referente a hardware y soporte a usuario. Las aplicaciones conforme a la arquitectura propuesta están basadas en los servidores centrales, permitiendo incluso simplificar el ambiente del segmento usuario final a terminales gráficos.

Analizar, diseñar e implementar un Sistema de Información Oceanográfico basado en la tecnología de Intranet.

El Sistema de Ayudas a la Navegación está implementado y puesto en producción. Para su desarrollo se empleó como metodología de desarrollo el paradigma orientado a objetos, documentando durante su proceso de desarrollo bajo la nomenclatura UML. El ambiente de producción está

sobre la plataforma Oracle en la capa de datos, IBM WebSphere en la capa de servidor J2EE, y el navegador web como cliente universal. Se utilizó la plataforma J2EE e incluye el empleo intensivo de EJBs.

El SISNAV es un piloto que permitió realizar la prueba del concepto propuesto; el sitio web del INOCAR (www.inocar.mil.ec) ha sido reconocido dentro de los cinco mejores sitios por la calidad de los servicios que presta, gracias al desarrollo de su Intranet, lo que ha permitido potenciar la capacidad de producción de servicios e información de sus funcionarios al servicio de la comunidad oceanográfica.

4. REFLEXIONES:

Es poco probable que alguien tenga duda de la dependencia de las TIC que tiene una Organización en búsqueda del éxito en los tiempos actuales. Pero insertar la tecnología de información en una Organización no es tarea simple, la tecnología “por sí sola” no aporta ningún valor. La tecnología de información pasa a través de los integrantes de una Organización, y por tanto ellos deben querer utilizarla, lo que demanda motivación y capacitación.

Si no se cuenta con una estrategia organizacional que facilite la adopción de la tecnología de información propuesta; si ésta en sí no es fácil de utilizar; si ésta no es fácil de controlar y si no es capaz de ser predecible en costos, las posibilidades de su adopción se reducen.

La información no depende de la tecnología de información. Ésta solo facilita su captura, procesamiento, almacenamiento y distribución.

La tecnología de información debe ser propuesta e implantada conforme a los Objetivos Estratégicos de la Organización, buscando mantener el alineamiento Estratégico adecuado y sobre todo apoyar los Factores

Diferenciadores de las Fortalezas Organizacionales, para soportar una Ventaja Comparativa.

Cuando la tecnología de información apoya una Ventaja Comparativa, coherente con la Estrategia adoptada, su sostenibilidad se vuelve un esfuerzo de la Organización y no solo del área de Sistemas. Por ello se debe empezar implantando tecnología de información en las áreas en que tenemos Fortalezas, y no para eliminar Debilidades Organizacionales.

4. SUGERENCIAS Y TRABAJOS FUTUROS:

- ✓ Extender el marco de trabajo y la aplicación de los conceptos probados descritos en el Capítulo 5, cuyo alcance tuvo únicamente el Instituto Oceanográfico de la Armada; al resto de repartos navales conforme a lo propuesto en el Plan de Sistemas de Información.
- ✓ Implantar las soluciones de infraestructura tecnológica de procesamiento, conectividad y software base; adaptando los recursos actuales, al esquema propuesto en el presente trabajo.
- ✓ Analizar, proponer e implantar un Proceso de Software Ligero en la Armada del Ecuador, tanto para desarrollo interno, como desarrollo compartido o tercerizado. El Proceso de Software debe establecer claramente “que se hace” en cada paso, para garantizar el éxito en una Unidad Técnica de Desarrollo de Sistemas de Información de Gestión en la Armada, considerando la presión existente actualmente para reducir los ciclos de desarrollo debido al denominado “tiempo Internet”. Esto implica considerar la adopción de métodos ágiles pero con un enfoque ingenieril, especialmente considerando las “buenas prácticas” descritas en la Programación

Extrema (XP), de una manera ordenada, gestionada y menos riesgosa, de modo que se pueda obtener productos de software de alta calidad, en ambientes de riesgo controlados, y resolviendo los requerimientos de manera oportuna.

- ✓ Definir estándares Institucionales para todos los aspectos relacionados con la tecnología de información; a nivel de hardware de procesamiento, almacenamiento, conectividad; a nivel de software base en sistemas operativos, sistemas operativos de red, bases de datos, servidor de aplicaciones, y demás servicios de sistema; arquitectura de software, marcos de referencia, modelos de desarrollo y lenguajes de programación.
- ✓ Analizar, proponer y emplear patrones de diseño de software, como mecanismo que permita a la Unidad Técnica de Desarrollo, aumentar la productividad, gestionar el conocimiento y mejorar la calidad de los productos desarrollados.
- ✓ Formalizar una política de seguridad de la información a nivel institucional, conforme a lo establecido en la norma ISO 17799; implementando los mecanismos tecnológicos que permitan satisfacer los requerimientos de seguridad establecidos en la política, conformando un equipo de administración de la seguridad, un equipo de reacción a incidentes (CERT) y definiendo la normativa interna que permita aplicar el marco legal vigente en el Ecuador (Ley de Comercio Electrónico y Firmas Digitales; y Ley de Transparencia de la Información).
- ✓ Establecer y ejecutar un Plan de Fortalecimiento del Recurso Humano especializado en el área de la tecnología de información tendiente a institucionalizar en los Centros de Formación Tecnológicos de la Institución, academias especializadas avaladas por los fabricantes de tecnología de información en: Cisco para el área de redes; Red Hat para el área de sistema operativo; Oracle

para el área de bases de datos; Java para el área de lenguajes de programación y desarrollo de sistemas; UML y RUP, para el área de arquitectura de software.

- ✓ Analizar e implementar una solución urgente de manejo de identidades a través de mecanismos tecnológicos a nivel Institucional, para implementar servicios de firma digital y certificados digitales de uso interno, estableciendo un directorio corporativo unificado.

BIBLIOGRAFÍA

No	Referencia	Autor; Titulo obra; Editorial; Fecha edición.
1.	[SINGER, 03]	Andrew, Singer, Vicealmirante; Network Centric Warfare; Navy League of USA, Sea Power; Septiembre 2003
2.	[ARMADA, 90]	Armada del Ecuador; Manual de Procedimientos Tácticos; 1990
3.	[ROTHSCHILD, 95]	Michael, Rothschild; Bionimics: Economy as Ecosystem; Henry Holt & Company, Inc.; 1995 <http://www.bionomics.org/text/resource/biobook.html>
4.	[TELLEEN, 96]	Steven, Telleen; Intranet Organization: Strategies for managing change; Amdahl Corporation; 1996.
5.	[BERTALANFFY, 67]	Ludwig von, Bertalanffy; General Theory of Systems; Social Science Information; 1967.
6.	[SIMON, 62]	Herbert, Simon; The Architecture of Complexity; Proceedings of American Philosophical Association; 1962 <http://cepa.newschool.edu/het/profiles/simon.htm>
7.	[DECEMBER, 97]	John, December; World Wide Web 1997 Unleashed; Fourth Edition, Sams.net; 1997
8.	[DRUCKER, 94]	Peter, Drucker; The Age of Social Transformation; 1994 <http://www.theatlantic.com/politics/ecbig/soctrans.htm>

9. [GALBRAITH, 00] Jonathan, Galbraith; Designing the Global Corporation; John Wiley and Sons Ltd; 2000
10. [FERNANDEZ, 98] Juan, Fernández; Curso de Dirección Estratégica; Universidad de Especialidades Espíritu Santo; 1998.
11. [TITTEL, 97] Ed, Tittel; y James Michael, Stewart; Intranet Bible; IDG Books Worldwide, Inc.; 1997
12. [TODT, 01] Ron, Todt; Defend the RNC 420; Associated Press; 2001. <http://www.r2kphilly.org/media/ap-030901.html>
13. [LINDORFF, 00] Dave, Lindorff; The Battle of Philadelphia; InTheseTimes.com, Independent News and Views; 2000. <http://www.inthesetimes.com/issue/24/20/lindorff2420.html>
14. [MIDENA, 99] RT-3-IV Reglamento para la elaboración, manejo, custodia y seguridad de la documentación militar calificada; Ministerio de Defensa Nacional; 1999.
15. [MAZZARI, 98] Geovanny, Mazzari; Tesis sobre Seguridad de Redes para la ESPOL; Escuela Superior Politécnica del Litoral; 1998.
16. [DoD 5200.28 STD] Department of Defense, USA; Orange Book DoD 5200.28 STD.
17. [VILLALÓN, 00] Antonio, Villalón Huerta; Seguridad en UNIX y Redes; Universidad Politécnica de Valencia; 2000.
18. [CONTRERAS, 03] José Contreras; Seguridad de la Información; Universidad Técnica Federico Santa María; 2003.
19. [ISO 17799] Information Security Management Standard; International Standard Organization; 2000.
20. [ARMADA, 00] Plan Estratégico Institucional de la Armada; 2000.
21. [ARMADA, 02] Manual de Organización de la Armada; 2002.
22. [KAPLAN, 96] Robert, Kaplan; y David, Norton; Cuadro de Mando

Integral; Harvard Business School Press; 1996.

23. [ORACLE-1, 02] Oracle Collaboration Suite, Technical Overview; 2002; <http://otn.oracle.com/products/cs/index.html>
24. [ORACLE-2, 02] Oracle Portal Center, Product Information; 2002; <http://portalstudio.oracle.com/servlet/page?_pageid=478&_dad=ops&_schema=OPSTUDIO>
25. [AGUENA, 03] Military Review; Guerra Conjunta; Academia de Guerra Naval; 2003.
26. [VANDERBURG, 98] Glenn, Vanderburg; Tricks of the Java Programming Gurus; Segunda Edición; Sams.net Publishing; 1998.
27. [NETSCAPE, 98] DevEdge Online Documentation, Introduction to Developing Applications for the Netscape ONE Platform; 1998; <http://developer.netscape.com/docs/manuals/tools/intro/index.html>
28. [MICROSOFT, 98] Introducing DNA Architecture; Microsoft, Inc; 1998.
29. [ORACLE, 03] Introducing the 9i Application Server Architecture; Oracle, Inc.; Oracle World 2003; 2003.
30. [MORRISON, 96] Michael, Morrison; Java Unleashed; First Edition, Sams.net Publishing; 1996.
31. [CORBA, 98] CORBA Services: Common Object Services Specification; Object Management Group (OMG); 1998 <http://www.omg.org/technology/documents/formal/corbaservices.htm>
32. [SUN, 02] SUN Microsystems; Designing Enterprise Applications with the J2EE Platform; Second Edition; 2002 <http://java.sun.com/blueprints/guidelines/designing_enterprise_applications_2e/introduction/introduction.html>
33. [SUN, 04] SUN Microsystems; The J2EE 1.4 Tutorial; 2004

<http://java.sun.com/j2ee/1.4/docs/tutorial/doc/index.html>

34. [MICROSOFT, 02] Reference Architecture Guide; Microsoft System Architecture (MSA); Microsoft; 2002.
35. [POWER, 02] Richard, Power; Computer Security Issues & Trends, Vol. VIII, No.1; Computer Security Institute; 2002
36. [CHAPMAN, 02] David, Chapman; y Andy, Fox; Firewalls PIX de Cisco Secure; CiscoPress; 2002
37. [CEUDI 1, 02] Preguntas frecuentes de Internet 2; Consorcio Ecuatoriano de Universidades para el Desarrollo de Internet; 2002.
38. [INTERNET 2, 04] Internet 2 Overview, Presentación; Internet 2 Consortium; 2004.
39 [CEDIA, 04] Red Académica Avanzada (I2) – Ecuador, Presentación; Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado; 2004.
40. [IPV6, 03] The Next Generation Internet; IPv6 Information Page; 2003
<http://www.ipv6.org>
41. [PALET, 00] Jordi, Palet; Tutorial de IPv6; Foro Español IPv6; 2000.

APÉNDICE A

DESCRIPCIÓN DE LOS ROLES PARA EL DESARROLLO Y MANTENIMIENTO DE LA INTRANET

1. **Administrador del proyecto.**
   - Proveer la dirección estratégica del proyecto.
   - Auspiciar y promover el proyecto ante el Comando o Alta Dirección y la organización.
   - Asesorar al Comando en cuestiones estratégicas relacionadas con el empleo de la tecnología.
   - Liderar el equipo de especialistas internos y externos en tecnología, línea de acción de la organización y administración.
   - Administrar el proyecto en términos de: planificación, programación, presupuesto, personal, entrenamiento, control de gastos y reportes de estado del proyecto.

2. **Arquitecto de la red.**
   - Diseñar la arquitectura para la infraestructura de la red TCP/IP para el Intranet, tanto para la cobertura institucional como para los sitios específicos.
   - Seleccionar y desarrollar los estándares para la infraestructura a implementar.

3. **Arquitecto de la mensajería electrónica.**
   - Planificar el rol de la mensajería electrónica en la organización.
   - Administrar el grupo técnico responsable de la operación diaria de la mensajería.
   - Proveer la dirección estratégica para la mensajería electrónica.

4. **Diseñadores de interfaces (artistas gráficos).**
   - Diseñar los estándares de la páginas web, estilos y directrices.
   - Desarrollar plantillas para las páginas.
   - Crear librerías para los estándares de contenido con relación al texto, gráficos, audio y video.
   - Diseñar formularios en HTML, tablas, etc.
   - Diseñar interfaces de usuario en Java/JavaScript, Flash, PHP, etc.

5. **Administrador del sistema.**
   - Instalar, configurar, calibrar, reparar y administrar el software de intranet (server y clientes, aplicaciones y contenido web en cuanto al file system).
   - Efectúar tareas rutinarias de administración tales como control de acceso, respaldo, monitoreo y demás.

6. **Administradores de las base de datos.**
   - Proveer accesos autenticados a los datos de la base de datos vía logins.

- Mantener las estructuras de datos, transacciones, consultas, reglas del negocio y autenticación de usuarios.

7. **Desarrolladores de aplicaciones / programadores.**
   - Escribir programas utilizando herramientas basadas en estándares abiertos (Java, JavaScript, HTML, XML).
   - Escribir formularios en HTML.
   - Escribir scripts tipo CGI.
   - Interactuar contra la base de datos vía SQL, JDBC y herramientas middleware.
   - Verificar y probar las aplicaciones.
   - Administrar el control de versiones y la verificación de código.

8. **Desarrolladores de contenido web/webmaster.**
   - Coordinar con los proveedores de contenido web la información a ser publicada.
   - Desarrollar la arquitectura lógica del sitio y el diseño de páginas.
   - Crear páginas HTML utilizando las herramientas adecuadas, plantillas y administradores de estilos.
   - Incorporar texto, gráficas, audio, video, flash, scripts, applets o aplicaciones según sea necesario.
   - Crear y probar los vínculos entre las páginas para verificar su consistencia.

- Administrar el contenido del sitio, incluyendo actualizaciones, control de versiones, hipervínculos rotos, etc.

9. Usuarios del navegador web.

- Aprender como utilizar el navegador web para navegar por los sitios de información autorizados.
- Aprender a utilizar aplicaciones específicas tales como mensajería, grupos de discusión o aplicaciones personalizadas.

APÉNDICE B

ELEMENTOS Y PROCESOS DE LA METODOLOGÍA DE DESARROLLO DE SITIOS WEB

1. ELEMENTOS DE LA METODOLOGÍA

1.a) Información de la audiencia del sitio web.- Se refiere al conocimiento que se obtiene de la audiencia pretendida, lo que puede incluir a los usuarios actuales del tipo de información a ser publicada. El conocimiento que debemos tratar de obtener es: perfil de la audiencia, interés, inclinación a que tipo de información, y todo detalle que sea útil para moldear la información que se incluirá en el sitio web de modo que se satisfaga sus necesidades. Normalmente, esta información no llega a estar completa en el ciclo de vida del sitio web, puesto que en la medida que pasa el tiempo, ésta se puede volver obsoleta, lo que obliga a mantener un esquema de retroalimentación en el sitio que ayude a mejorar este elemento.

1.b) Declaración del propósito del sitio web.- Es una descripción de la razón y el alcance de la existencia del sitio web. Esta declaración puede realizarse en términos generales, o específicos; y deberá ser observada durante el desarrollo del sitio en los diferentes procesos de la metodología. La declaración del propósito del sitio web, es dinámica, cambia a lo largo del tiempo.

1.c) Declaración de los objetivos del sito web.- Se obtiene a partir de la declaración del propósito, y define que metas específicas el sitio web deberá alcanzar. Esta declaración también es dinámica, y no solo cambia porque el propósito del sitio web cambia, sino posiblemente porque cambia la información de la audiencia pretendida.

1.d) Información de dominio del sitio web.- Es la colección de conocimiento e información acerca del tópico que el sitio web cubre, tanto en términos de lo que se pondrá al alcance de los usuarios, como lo que estará al alcance de los desarrolladores del sitio. No toda la información que los desarrolladores conozcan acerca del tópico del sitio, se pondrá disponible para los usuarios, pero puede resultar útil para que su tarea logre alcanzar los objetivos del sitio.

1.e) Especificación del sitio web.- Incluye una descripción detallada de las restricciones y elementos que deberán ser considerados en el sitio web. En esta especificación, se lista la información que será presentada, indicando cualquier consideración que podría ser una limitación para la presentación del sitio. Esta especificación es totalmente dinámica, puesto que el sitio web debe mostrar cambios a su audiencia.

1.f) Presentación del sitio web.- Aquí se indica que información será entregada al usuario. La presentación es el resultado de los procesos de diseño e implementación. Aquí se plasman alternativas creativas y técnicas de presentación pretendidas para cumplir con las especificaciones del sitio. Pueden además incluir consideraciones de eficiencia, estética y patrones de usabilidad.

2. PROCESOS DE LA METODOLOGÍA.

2.a) Planificación.- Es el proceso de escoger entre varias posibilidades, la más idónea, de modo que se garantice alcanzar las metas del sito web. Estas metas incluyen: la definición de la audiencia pretendida, la declaración del propósito y de los objetivos. Además, los desarrolladores deberán planificar la información de dominio, definiendo y especificando la información que deberá ser recolectada, cómo será recolectada y cómo esta información posteriormente será actualizada. Al planificar el sitio web, se debe definir las habilidades necesarias para cumplir con las especificaciones del sitio web. Así

también, se puede definir la necesidad de ciertos recursos como por ejemplo un programa de control de estadísticas del sitio.

2.b) Análisis.- Es el proceso de recolección y comparación de información del sitio web y su operación, de modo que se pueda mejorar su calidad. Un proceso importante en el análisis, es la recolección de información del nivel técnico de la audiencia pretendida, puesto que esto puede tener un gran impacto en el cómo se debe proveer la información del sitio.

2.c) Diseño.- Es el proceso en el que el diseñador del sitio web, en base a las especificaciones del sitio, toma decisiones acerca de qué componentes se utilizarán para la construcción del sitio. Para esto se debe tomar en cuenta la declaración del propósito del sitio, los objetivos, la audiencia y la información de dominio.

2.d) Implementación.- Es el proceso de construir el sitio en sí, siguiendo las especificaciones del sitio, y las guías provenientes del proceso de diseño.

2.e) Promoción.- Es el proceso de hacer público la existencia del sitio web, se pueden utilizar estrategias de mercadeo para garantizar que la audiencia pretendida para el sitio se entere de su existencia.

2.f) Innovación.- Es el proceso de asegurarse que se inició otro ciclo del proceso de desarrollo del sitio, buscando mejoras en cada uno de los procesos. Se debe considerar el uso de tecnologías emergentes que podrían ser apropiadas para el sitio, incluyendo elementos que aseguren atraer la atención con éxito de la audiencia pretendida. Es una forma permanente de considerar la retroalimentación de los usuarios para mejorar la usabilidad y calidad del sitio de modo que incluso se supere las expectativas de la audiencia.

3. PLANIFICACIÓN DE UN SITIO WEB

El proceso de planificación de un sitio web es dinámico, un constante balance entre oportunidades y recursos.

3.a) Información de la audiencia

Para crear una comunicación efectiva, los desarrolladores deberán primero establecer qué quieren comunicar y a quién. La información acerca de la audiencia pretendida es por tanto fundamental. Para obtener esta información se deben seguir dos pasos:

1. Definir la audiencia pretendida.- Escriba una declaración de la audiencia pretendida para el sitio web. Ejemplo: "Personas interesadas en conocer sobre el estado de las mareas de las costas ecuatorianas".

2. Definir la información que es crítica sobre esta audiencia.- Esto dependerá mucho del propósito del sitio web. En todo caso se trata de descubrir qué características de esta audiencia son importantes, las mismas que pueden ser refinadas una vez establecido el propósito del sitio, descartando aquellas características que sean irrelevantes.

3.b) Declaración del propósito

La declaración del propósito del sitio es lo que conduce el proceso de desarrollo. Esto ayuda a los desarrolladores a escoger qué información acerca de la audiencia debe ser obtenida y como ésta influye en la presentación del sitio una vez terminado.

Para definir el propósito del sitio web, el desarrollador necesita establecer qué es lo que el sitio deberá hacer, contemplando los siguientes elementos:

- ✓ El tópico de la información del sitio.- ¿Qué área del conocimiento sirve como contexto de lo que el sitio deberá comunicar?

- ✓ La audiencia.- La declaración del propósito del sitio, incluye una identificación de la audiencia.

- ✓ El nivel del detalle con el cual la información será presentada.- Esto influye en cuanta información del dominio debe ser obtenida para ser publicada.

- ✓ Las expectativas de los usuarios.- Puede incluirse en la declaración una frase como: "con el propósito de...."

Esto ayuda a definir bien cual es el mensaje que el sitio web desea transmitir, por lo tanto a veces resulta muy práctico incluir esta declaración en la página principal del sitio web.

3.c) Declaración de los objetivos

Luego de que los desarrolladores del sitio web, han planificado el propósito del sitio, quién es la audiencia del sitio y qué necesitan los desarrolladores conocer acerca de la audiencia, el siguiente paso es combinar toda esta información, para definir los objetivos del sitio web. Una declaración de objetivos define claramente resultados en términos de información, que implementarán el propósito declarado para el sitio web.

Los objetivos del sitio, no deberán constar en la página principal del sitio web, es información que detrás de la escena, guía el desarrollo de los otros elementos del sitio web.

3.d) Información de dominio

La información de dominio tiene que ver con el conocimiento acerca del tópico definido para el sitio web, tanto la información que será puesta en línea como la que no, aquella que permitirá que los desarrolladores simplemente hagan mejor su trabajo. Para planificar la información de dominio se deberá hacer lo siguiente:

1. Definir qué información de dominio necesitan conocer los desarrolladores y qué información del dominio será puesta al alcance de los usuarios. Deberá establecerse si los usuarios tendrán acceso a alguna base de datos, si hay alguna información digital que puede servir de base para ser publicada en línea, qué información analógica deberá ser digitalizada para ser publicada en línea.

2. Planificar la adquisición de la información determinada, cómo se van a crear las interfaces con la base de datos, cómo se van a convertir los formatos digitales existentes en formato HTML, cómo se va a digitalizar la información analógica, etc.

3. Planificar la actualización y el mantenimiento de la información, puesto que no es suficiente definir las fuentes de información y el proceso de adquisición de esa información. Hay que determinar si cada pedazo de información es dependiente del tiempo, es decir cambia en la medida que éste transcurre, si es así, se debe definir quién deberá actualizar la información, y cual será el costo de esta actualización. Estas son tareas que tanto los dueños de la información, como el administrador del sitio, deberán tener presentes, creando "una lista de cosas por hacer..."

3.e) Especificación del sitio web

La especificación del sitio web, es un refinamiento de los objetivos del sitio en términos más específicos, añadiendo limitaciones y otros requerimientos. Estas especificaciones sirven como libro guía para los diseñadores e implementadores, en las especificaciones se deben considerar todos los recursos necesarios que debe utilizar el sitio web, como por ejemplo: hiperenlaces, componentes como mapas sensitivos, sonido, imágenes, videos, etc.

La meta principal en el proceso de planificación, en cuanto a la especificación del sitio, es asegurarse de que los desarrolladores tengan todos los recursos, herramientas, entrenamiento y tiempo necesario para cumplir con estas especificaciones.

3.f) Presentación del sitio web

Al planificar la presentación del sitio web, se puede considerar lo siguiente:

- ✓ Generar páginas de muestra que incluyan la mayoría de las especificaciones establecidas.
- ✓ Crear y mantener un conjunto de componentes web, definidos en las especificaciones.
- ✓ Crear una imitación del sitio basado en las especificaciones iniciales.

4. ANÁLISIS DE UN SITIO WEB

El proceso de análisis tiene como propósito, verificar que un sitio web, ya sea que se lo esté planificando o ya esté operativo, este cumpliendo debidamente los objetivos planteados, es decir validar que el sitio cumple el propósito para

el que fue creado. El proceso cubre la validación técnica, así como de su contenido y diseño, incluyendo su usabilidad y estilo.

La meta del análisis es asegurarse de que el sitio trabaja en la siguiente manera:

- ✓ Retóricamente, ¿Está el sitio web cumpliendo con el propósito declarado, para la audiencia pretendida?

- ✓ Técnicamente, ¿Es el sitio web funcionalmente operacional y de una implementación consistente con las especificaciones determinadas?

- ✓ Semánticamente, ¿Es la información del sitio correcta, relevante y completa?

Así, el analista del sitio web, actúa como un verificador, evaluador y auditor, para un sitio en desarrollo, sin embargo, de ser posible, si el sitio ya está implementado, el analista deberá ser tan independiente como sea posible del grupo de desarrollo.

4.a) Principios para el análisis del sitio web

Durante el análisis, se debe poner mucha atención al evaluar, como el sitio es consistente con los siguientes principios:

- ✓ Esforzarse para garantizar un servicio continuo y global.- Dentro de los límites de la aplicación del sitio, si es un Intranet, en que horarios se ha garantizado el uso de la información.

- ✓ Verificación de los hiperenlaces, tanto semánticamente como técnicamente.- Debe ser aprovechada la ventaja de que el web, a través de los hiperenlaces puede aumentar y extender el significado de la

información, se debe hacer un análisis retórico y semántico de los hiperenlaces establecidos, para verificar de que estos contribuyan en la aclaración del contenido del sitio. La verificación técnica, lo que asegura es la operación y disponibilidad al mayor grado posible.

- ✓ Asegurar la porosidad.- El contenido de un sitio, tiene múltiples entradas, dado que al construirlo, se debió haber observado una porosidad adecuada. Desde este punto de vista, el análisis debe verificar cómo cada una de las posibles entradas, ofrecen a los usuarios el suficiente nivel de información.

- ✓ Trabajar con dinamismo.- El sitio web opera en un ambiente de continuo cambio en términos de información y tecnología. El analista, deberá estar al tanto de los cambios, que podrían favorecer la eficiencia del sitio.

4.b) Análisis de la información

El analista puede evaluar los aspectos retóricos y técnicos del sitio, analizando los elementos del sitio: información de la audiencia, declaración del propósito y objetivos, información del dominio, especificación del sitio y presentación, y el desempeño: obteniendo información de cómo los usuarios utilizan o esperan utilizar el sitio.

El proceso de análisis de la información busca respuestas a las siguientes preguntas:

- ✓ ¿Está el sitio cumpliendo el propósito establecido y alcanzando los objetivos declarados?

- ✓ ¿Está el sitio operando eficientemente?

✓ ¿Se están obteniendo los beneficios y resultados esperados?

El analista del sitio, puede obtener información acerca de los elementos para el sitio, de la planificación del sitio, y puede obtener información del desempeño, examinando las estadísticas del sitio.

El resultado del análisis del sitio, es utilizado para mejorar la calidad de éste, así si se determina que la información del dominio del sitio está usualmente desactualizada, entonces se recomendará modificar lo establecido en la planificación del sitio, disminuyendo el lapso entre las actualizaciones, observaciones que deberán ser consideradas tanto por los administradores del sitio, como por los diferentes consejos de la intranet.

Tal como se muestra en la Figura B.1, el proceso de análisis de la información, se lo lleva a cabo siguiendo los siguientes puntos de verificación:

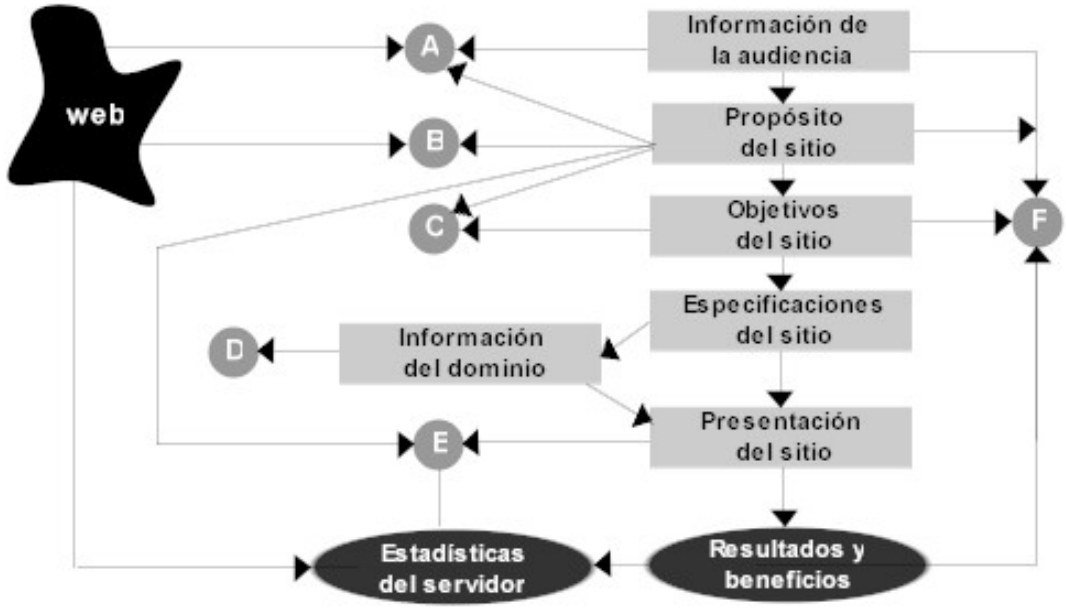


FIGURA B.1. PUNTOS DE VERIFICACIÓN PARA EL PROCESO DE ANÁLISIS

Punto A: ¿Existe la audiencia pretendida para el sitio web, según el propósito dado?

Lo primero que debe analizarse, es que la audiencia pretendida, tiene acceso al web, a pesar de que resulta muy difícil establecer con exactitud la población demográfica de usuarios del web, es necesario de alguna forma obtener una aproximación estimada. Si estamos analizando un sitio de dominio público en el Internet, lo mejor será buscar por el tópico que el sitio busca cubrir, si existen grupos de discusión o sitios relacionados que puedan tener interés en lo que el sitio les puede ofrecer, el analista puede obtener dos resultados: que no exista nada relacionado, por lo cual puede haber una muy buena oportunidad de éxito para el sitio; o a su vez, que la audiencia pretendida no tiene interés en las comunicaciones en línea. Para establecer cual de los dos casos es el más preciso, se deberá entrevistar a un grupo representativo de la audiencia pretendida.

Otro aspecto del análisis, es determinar si el propósito establecido para el sitio, cubre las necesidades de información de la audiencia pretendida, y que está incluido en sus patrones de comunicación

A través de esta verificación de la audiencia pretendida, el propósito del sitio y los patrones de comunicación de la audiencia identificada, se pueden detectar rápidamente problemas lógicos, que pueden impedir que el sitio tenga éxito, lo que permitirá replantear el sitio, o a su vez, optar por otro medio de comunicación.

Punto B: ¿Existe algún sitio en el web (interno o externo) que cumpla ya con el propósito establecido para el sitio?

Cómo parte de un proceso de la metodología, el análisis se lo llevará a cabo a sitios web en planificación, así como a los que están en producción. Con esto

en mente, es necesario considerar que en el análisis de la información, se verificará este punto para cuando existan ya sitios web desarrollados en la Intranet.

La idea es no duplicar la tarea de algo que está cumpliendo exitosamente con su propósito. El objetivo es revisar si alguien más ha desarrollado un sitio con el mismo propósito que cumplir, para la misma audiencia, para lo cual se deberán utilizar métodos de búsqueda sean estos públicos, como Altavista, o privados provistos por la Intranet.

Como resultado de esta búsqueda, se puede llegar a determinar que existen sitios con el mismo propósito, pero provistos para una audiencia diferente, esto puede dar al analista ideas acerca de la clase de información que le puede ser útil para la audiencia pretendida; si se determina la misma audiencia pero con otro propósito, lo que puede resultar útil para aumentar el conocimiento de los intereses de la audiencia pretendida, incluyendo en el sitio hiperenlaces hacia esta información, que provean valor agregado al sitio, permitiendo la colaboración entre diferentes fuentes de información.

Punto C: ¿El propósito, los objetivos y las especificaciones, son consistentes entre sí?

Uno de los elementos más importantes de integridad, es la triada propósito/objetivos/especificaciones, esta triada deletrea el porqué el sitio web existe, y que es lo que ofrece.

La verificación de esta triada, sirve para asegurarse de que nada queda suelto al momento de interpretarla desde el propósito (descripción general de porque el sitio existe), a los objetivos (una descripción más específica de que es lo que el sitio va a hacer), hasta las especificaciones (una enumeración detallada de la información que el sitio presentará y como lo hará)

Una forma de hacer esto, es dibujando un diagrama similar al de la Figura B.2, que enlace la declaración del propósito del sitio, con los objetivos establecidos, y estos con las especificaciones. Así, cada una de las especificaciones, deberá estar enlazada con un objetivo, y cada objetivo deberá contribuir a la consecución del propósito. El diagrama también puede incluir una lista de las direcciones URL que contienen los elementos y la información a ser utilizada en el sitio.

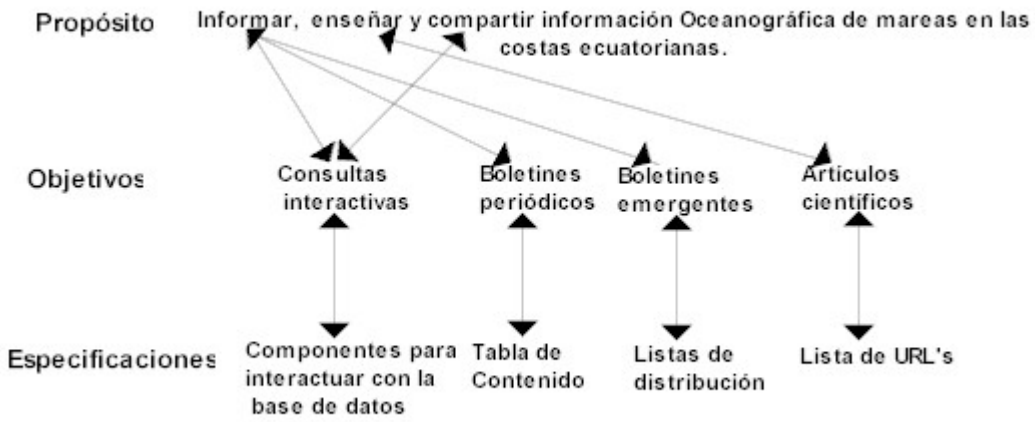


FIGURA B.2. VERIFICACIÓN DE LA INTEGRIDAD DEL PROPÓSITO, OBJETIVOS Y ESPECIFICACIONES PARA UN SITIO WEB

Punto D: ¿Es la información de dominio del sitio exacta?

La calidad de la información de dominio que provee el sitio web, afecta a la percepción del usuario sobre la calidad en general de éste. Por tanto, esta información debe ser chequeada, para asegurar su precisión, actualidad y sobre todo que esté completa. Según la naturaleza de la información de dominio, deberá establecerse la frecuencia de los chequeos periódicos de la misma.

La siguiente lista, ayuda a verificar los puntos principales que se deben verificar aquí:

- ✓ Verificar la operatividad de los hiperenlaces, para garantizar que la información a la que hacen referencia, no ha sido eliminada o movida.
- ✓ Verificar la exactitud de la información.
- ✓ Utilice siempre fuentes de información confiables y representativas para el área de información provista.
- ✓ Si hay interacción con alguna base de datos, asegurarse de que esté tan actualizada como sea posible.
- ✓ Si utiliza hiperenlaces externo, verificar la disponibilidad de la información y del enlace de comunicación.
- ✓ Verificar que la información proporcione el nivel de detalle adecuado.
- ✓ Verificar que no haya información no apropiada para los usuarios desde el punto de vista ético, legal u obsceno.

Punto E: La presentación del sitio web, ¿Está proporcionando resultados consistentes con lo planificado?

La meta en este punto de chequeo, es determinar si el sitio web, basado en las estadísticas del servidor, o en caso de no contar con ello, en la retroalimentación de los usuarios, es accesado consistentemente. El administrador del servidor web, debe tener la capacidad de obtener una lista de los archivos del sitio, con el número de accesos en un lapso de tiempo

determinado. Esto permite determinar ciertos patrones de acceso por parte de los usuarios.

Para interpretar estas estadísticas, se deben buscar respuesta a las siguientes preguntas:

- ✓ El patrón general de accesos al sitio, ¿Refleja que se cumple con el propósito del sitio?

- ✓ El patrón general de acceso, ¿Indica un balance en la forma de presentar el sitio, o hay páginas que tienen un acceso desproporcionado? ¿Puede esto indicar un problema de diseño? ¿Existe falta de información de acceso en las páginas de acceso, o en la página principal?

Punto F: ¿Son congruentes las necesidades de la audiencia, los objetivos del sitio, y los resultados del uso del sitio?

Es muy importante determinar que las necesidades de la audiencia son satisfechas por el sitio, para hacerlo, debemos comparar la información obtenida de la audiencia, esto es: sus necesidades e intereses, con los objetivos establecidos para el sitio, y los beneficios y resultados obtenidos en el sitio. Aunque esto último no es muy fácil de determinar, se puede hacer lo siguiente:

- ✓ Preguntar a los usuarios, capture información de retroalimentación a través de formularios o con el correo electrónico, para lo cual incluya preguntas sobre la satisfacción de los usuarios, como ¿Qué más les gustaría que se incluya en el sitio web?

- ✓ Haga una encuesta sobre su sitio, haga un estudio para determinar la reputación de su sitio en la comunidad interesada en el tópico de la

información provista. Trate de determinar si alguien recomienda su sitio como una buena fuente de información.

- ✓ Determine si el proceso de análisis cumplió bien su propósito

El punto F trata de asegurar que el resto de puntos garanticen en conjunto que el sitio ofrece los resultados deseados.

5. ANÁLISIS DE DESEMPEÑO Y DISEÑO

No basta con realizar un análisis de la información nada más, también es necesario determinar la calidad del diseño del sitio y su desempeño.

5.a) Desempeño

Uno de los aspectos que más deja huella en los usuarios, es cuánto les cuesta a ellos recuperar la información del sitio. El costo está dado en términos de tiempo para obtener la información, el mismo que crece en la medida que la información incluya imágenes, videos, audios, etc, y dependiendo del tamaño de las páginas accesadas.

Este tipo de análisis se lo puede hacer en términos generales, verificando la siguiente lista:

- ✓ Tiempo de recuperación.- Cuánto toma al usuario obtener la información desde el sitio, para lo cual el analista deberá efectuar accesos al sitio con una cuenta de acceso, un computador y un navegador web, lo más parecido a la media de la mayoría de usuarios. Si este tiempo de recuperación de la información, es muy alto, debe ser proporcionado a los diseñadores, para que mejoren el sitio, sin embargo es bueno preguntarse si el tipo de audiencia está dispuesta a pagar el tiempo de espera, por obtener la información.

- ✓ Legibilidad.- Se busca determinar si el usuario puede o no, leer el texto de las páginas, esto debido al uso de tramas y colores de fondo que se usan comúnmente en los sitios web, al tamaño del texto y efectos de animación como texto intermitente.

- ✓ Rendimiento.- La idea es determinar el rendimiento del sitio, para varios tipos de navegadores web, incluyendo aquellos que no soportan extensiones de diseño o tecnologías más avanzadas.

5.b) Estética

La estética tiene un efecto subjetivo acerca de la apreciación de la calidad del sitio web. Algunas de las guías a seguirse son:

- ✓ El sitio web, ¿Exhibe un diseño coherente y balanceado, que ayude a los usuarios a enfocarse en el contenido? No se debe ir al extremo de utilizar toda extensión disponible tan solo por el hecho de tener un sitio sofisticado y actualizado, en el análisis se debe determinar si el diseño de las páginas cae fuera del propósito del sitio o de las necesidades de la audiencia pretendida.

- ✓ El sitio web, ¿Exhibe repetitivamente patrones de diseño consistentes, así como metáforas de navegación, que ayuden al acceso a la información a ser más consistente? Trate de utilizar elementos gráficos repetitivos que sean consistentes con el propósito de ilustrar

- ✓ ¿Cómo está siendo utilizado el color? El color puede ser utilizado muy eficientemente para codificar la información, o para enfocar la atención del usuario. El uso arbitrario del color puede afectar al sitio.

5.c) Usabilidad

Siga la siguiente lista de chequeo para verificar la usabilidad del sitio web:

- ✓ Lleve a cabo recorridos simples del sitio web, y con el propósito del sitio y la definición de la audiencia en mente, verifique si la mayoría de los objetivos se cumplen con un recorrido breve.

- ✓ Chequee las tareas más comunes de los usuarios, basado en el propósito del sitio y en el conocimiento de la audiencia, tratando de descubrir problemas para cumplir con estas tareas.

- ✓ Pruebe las tareas de los usuarios más representativos del sitio, observando directamente como ellas son llevadas a cabo, pidiendo a los usuarios que narren en voz alta lo que ellos piensan cuando interactuan con el sitio.

5.d) Semántica

Aquí semántica se refiere al sentido transmitido por las páginas del sitio web. En este análisis se determina como el sitio transmite ese significado. Para esto, se lleva a cabo la siguiente lista de verificación:

- ✓ Verifique metáforas de navegación o acceso a la información no apropiadas, normalmente, los diseñadores incluyen iconos o flechas para permitir moverse hacia delante o hacia atrás, así como también a la página principal; pero debido a la porosidad del sitio web, uno debe pensar que un usuario que hizo un acceso directo a una página determinada, tal vez como resultado de una consulta a una máquina de búsqueda, no tiene idea de lo que podrá encontrar en la página siguiente o la anterior, las flechas por sí solas no dicen nada. En la tecnología de hipertexto, no tiene sentido hablar de patrones de acceso lineales. En lugar de esas metáforas, utilice pistas

como hiperenlaces que describan brevemente lo que encontrará en el destino de ese enlace.

- ✓ Verifique el contexto de las pistas, el uso de las pistas en un medio de comunicación no lineal como el web, es lo que lo hace poderoso. Las pistas utilizadas como hiperenlaces, ayudan a los usuarios a entender como la información provista en las páginas del sitio, encaja en un sistema más general o universal de información y conocimiento.

- ✓ Verifique el significado de los gráficos y símbolos utilizados.

5.e) Preguntas que un analista de un sitio web deberá hacerse

- ✓ ¿Porqué utilizar imágenes grandes? Está seguro de que el usuario del sitio está dispuesto a pagar el alto precio de la espera por ver esas imágenes.

- ✓ ¿Porqué utilizar palabras dibujadas? A menos de que sea un logotipo o texto artístico que tiene algún propósito en especial, no debe utilizar palabras dibujadas.

- ✓ ¿Porqué tener diferentes logos en las páginas? Trate de reflejar una imagen consistente, un solo logotipo ayuda en esto y ahorra el tiempo de espera en los usuarios.

- ✓ ¿Porqué tener diferentes colores y tramas de fondo en cada página? Utilice una metáfora y un patrón de diseño consistente, no pierda el beneficio de utilizar una apariencia familiar en todas sus páginas.

- ✓ ¿Porqué utilizar viejas metáforas? Utilice hiperenlaces asociativos, utilice las pistas, no utilice flechas o palabras como siguiente.

- ✓ ¿Porqué no ir directamente al punto? No se olvide que hay un propósito establecido para el sitio web, entonces porque no enfocar al sitio para alcanzar ese propósito, utilice esquemas de acceso a la información relacionada dando la libertad siempre al usuario de que si él lo desea la revise.

- ✓ ¿Porqué no enfocarse en su única contribución? Vaya directo hacia la fortaleza de su sitio, provea información detallada y profunda de lo que usted ha establecido como propósito del sitio.

- ✓ ¿Porqué utilizar términos bulliciosos con sus usuarios? A ellos no les interesa saber que su sitio es interactivo o inteligente, tan solo les interesa la información que en él obtengan.

- ✓ ¿Porqué ser muy pegajoso? Si su sitio tiene una audiencia adulta, de la impresión de que usted espera de ella que sea inteligente, no trate de ser muy detalloso, puede resultar no adecuado para los usuarios.

- ✓ ¿Porqué no identificar la fuente física de la información que usted está proveyendo? Proporcione en el pie de cada página, información de contacto tanto vía correo electrónico, como dirección geográfica de su sitio.

6. DISEÑO DE UN SITIO WEB

Durante el diseño de un sitio, debe existir un balance permanente entre las necesidades de la audiencia pretendida, y el desempeño, la estética y la usabilidad.

Los diseñadores del sitio, deben ser sensitivos con la experiencia de los usuarios del sitio, su disponibilidad de tiempo y su nivel cultural para entender las pistas y metáforas utilizadas. Toda esta información es obtenida de la

descripción de la audiencia pretendida, proporcionada en el proceso de planificación, y posteriormente verificada en el proceso de análisis.

6.a) Principios para un buen diseño de un sitio web

La mejor manera de manipular la experiencia de los usuarios del sitio, es empacando juiciosamente la información en la cantidad adecuada de páginas y de secciones dentro de ellas, enlazando estas páginas para cubrir las necesidades del usuario y proporcionar las pistas suficientes para que estos descubran el contexto de las piezas de conocimiento propuestas y puedan navegar adecuadamente.

Basados en esto, durante el diseño se deben contemplar los siguientes principios:

- ✓ **Construya un significado asociativo.-** Explotando el poder del hipertexto para enlazar información relacionada.

- ✓ **Mantenga el sitio competitivo.-** El diseño del sitio deberá garantizar el mínimo costo para el usuario al momento de encontrar a la información, accesarla y entenderla.

- ✓ **Haga un uso eficiente de los recursos.-** Seleccione las características que mejor cubran las necesidades de los usuarios, con el mínimo uso de espacio, tiempo de acceso, grandes gráficos y requerimientos muy difíciles de ser mantenidos. Utilice características para el sitio que sean eficientes de operar, elegantes de utilizar y fáciles de mantener.

- ✓ **Enfóquese en las necesidades del usuario.-** Conociendo sobre la audiencia pretendida, satisfacer sus necesidades es la primera prioridad, utilice la declaración del propósito del sitio y la información de la audiencia

para tomar decisiones sobre la organización de las páginas y su esquema de diseño.

- ✓ **Reconozca la porosidad.-** No utilice metáforas no adecuadas para esta característica, como siguiente, anterior, arriba, página principal, etc. el usuario puede hacer accesos al sitio en forma no lineal.

- ✓ **Cree una apariencia consistente, agradable y eficiente.-** De al usuario una idea común de diseño para todas las páginas, sea coherente y organizado y utilice metáforas visuales adecuadas. Cada página por sí sola debe ser una pista de lo que el usuario encontrará en ella, la apariencia del sitio debe ayudar al usuario a satisfacer sus necesidades de información.

- ✓ **Soporte la interactividad.-** Por lo menos provea una forma de que los usuarios contacten a los desarrolladores del sitio, para plantear preguntas o informar problemas relacionados con el sitio. Basados en el propósito del sitio, puede desarrollarse mayores niveles de interactividad que vayan desde interfaces de formularios hacia aplicaciones interactivas.

- ✓ **Proporcione un soporte a la navegación del usuario.-** A pesar de que los navegadores web, incluyen funciones para desplazarse hacia atrás o hacia delante del sitio explorado, proporcione un esquema de diseño que soporte la navegación por la estructura del sitio, que explote la asociación de la información.

6.b) Técnicas de diseño

Empacar la información en paquetes de tamaño adecuado

La idea es que estos paquetes de información, no sobrecarguen al usuario. Como guía general, el ser humano puede mantener la atención simultaneamente a cinco más/menos dos elementos.

Los paquetes de información, cuando se crean alrededor de ideas, conceptos o maneras de pensar familiares al usuario, ayuda a estos e enfocarse en un tópico a la vez y a desarrollar en ello el conocimiento en forma incremental.

Para agrupar la información en paquetes, el diseñador debe primero agrupar los documentos que representan la información que se presentará en el sitio. Esta información deberá estar listada en detalle en las especificaciones del sitio, y reflejada en los objetivos propuestos. La siguiente es una técnica que ayuda a obtener los paquetes de información para el sitio web:

1. Primero escriba el propósito del sitio web y sus objetivos. Encierre con un círculo los sustantivos de esas declaraciones.

2. Luego agrupe los sustantivos relacionados, y defina esas relaciones en términos de la perspectiva de la audiencia. Establezca primero si el usuario pensará en términos de tópicos (categorización de los sustantivos), o en términos de procesos (¿Qué es lo que el diseñador debe hacer con los sustantivos?) Intente ambos arreglos y muéstrelos a un usuario representativo, preguntando, ¿Cuál de los dos arreglos parece ser más útil para el trabajo que usted espera que el sitio haga?

3. Los sustantivos relacionados, deberán ser graficados en un diagrama de agrupación, dibujando círculos alrededor de las palabras relacionadas. En el agrupamiento orientado por el tópico, se puede hacer una

descomposición jerárquica del mismo. En el agrupamiento orientado por los procesos, se puede agrupar los nombres que actúan en el mismo proceso.

Un diagrama de este tipo, muestra una posible organización del sitio. Así, a partir de este diagrama, se pueden crear los diferentes paquetes. Un paquete, es una o más páginas web relacionadas de acuerdo a la elaboración del diagrama.

El siguiente paso será transformar las páginas web en documentos HTML. Para asegurarse de que las páginas no estén sobrecargadas, se puede revisar el número de hiperenlaces que éstas tienen apuntando a los otros paquetes.

Enlazar las páginas

Lo siguiente será especificar, cómo las páginas están enlazadas entre sí. Para ello se utiliza nuevamente el diagrama de agrupación, en una de las siguientes maneras:

- ✓ Enlace las páginas siguiendo la jerarquía determinada en el diagrama de agrupación, y enlazando además cada una de las páginas en forma secuencial dentro de cada paquete. La ventaja de esta técnica, es que la organización jerárquica de las páginas ayudan a los usuarios a moverse a través de los paquetes rápidamente, y luego dentro de cada paquete si se desea más detalle de la información. La desventaja es que se establece un patrón predefinido de navegación por el sitio, lo que no siempre es adecuado para todos los usuarios, especialmente aquellos más experimentados en el sitio, los que para accesar a una información revisada con anterioridad, tendrán que eventualmente volver a hacer el recorrido pre - establecido.

- ✓ La otra técnica, es enlazar todas las páginas, unas con otras. Esto es conveniente si el sitio no contiene una cantidad excesiva de páginas, caso contrario mantener un sitio así, puede ser una tarea muy complicada.

- ✓ Otros métodos de enlace de páginas son: por necesidad, en el que se trata de hacer rutas de enlaces basados en las necesidades de los usuarios; y otro es por asociación, en el que se enlazan las páginas que están más relacionadas unas con otras.

7. PRESENTACIÓN DEL SITIO WEB

7.a) Técnicas de promocionamiento

La meta principal al momento de promover el sitio, es mantener informado al público en general y a la audiencia pretendida en particular, acerca del propósito del sitio y lo que este puede ofrecer. Dadas las características de este medio de comunicación, se requiere de un constante promocionamiento, informando acerca de nueva información ofrecida, nuevos recursos y nuevos foros que el sitio a creado.

Un promocionador del sitio web, deberá desarrollar ciertas estrategias para publicitar el sitio. Esta publicidad tiene entre otras las siguientes metas:

- ✓ Informar al público en general, la existencia del sitio web y que es lo que este ofrece.

- ✓ Atraer el interés de la audiencia pretendida, permitiendo que descubran como el sitio cubre sus necesidades de información.

- ✓ Mantener informados a los usuarios actuales del sitio, sobre las nuevas innovaciones.

La promoción del sitio web, debe basarse fundamentalmente en el propósito establecido y los objetivos propuestos, así como en la información disponible de la audiencia pretendida, especialmente este último elemento para tomar decisiones sobre donde colocar la publicidad del sitio.

Las técnicas que pueden resultar útiles para la promoción del sitio web, se describen en la Figura B.3.

FIGURA B.3. TÉCNICAS DE PROMOCIONAMIENTO DE UN SITIO WEB

La idea general es distribuir información acerca del sitio en tres niveles: A todo el web en sí, a la audiencia pretendida y a los usuarios actualmente reconocidos.

Para el primer nivel, lo que se debe buscar es un sitio que ofrezca un servicio de indexamiento o catalogación, un sitio dedicado a la búsqueda de la información en la Intranet. Para el segundo nivel, en base a la información de la audiencia, se pueden descubrir foros de discusión concurridos por la audiencia, listas de distribución u otros sitios visitados, en donde resultaría útil promocionar el sitio. Para el tercer nivel, se utilizan listas de distribución en base a información captada de los usuarios que visitan nuestro sitio, a través

de formularios o libros de visitas, o a su vez, se puede utilizar una página de anuncios o novedades con una sección de promocionamiento en la página principal.

APÉNDICE C

ARQUITECTURA JAVA 2 ENTERPRISE EDITION

1. Tecnologías de Servicios

a) JDBC

Permite invocar comandos SQL desde los métodos programados con Java. En los componentes CMP las operaciones de acceso a la base de datos, es gestionada por el contenedor, y la implementación del EJB no contiene ni código JDBC, ni código SQL.

Sin embargo se puede tener acceso a una base de datos desde un Servlet o una página JSP utilizando JDBC sin pasar por un componente EJB.

El API JDBC tiene dos partes:

- ✓ Una interfaz a nivel de aplicación utilizada por los componentes de aplicación para acceder a la base de datos.
- ✓ Una interfaz de provisión de servicios para montar un driver JDBC para la plataforma J2EE.

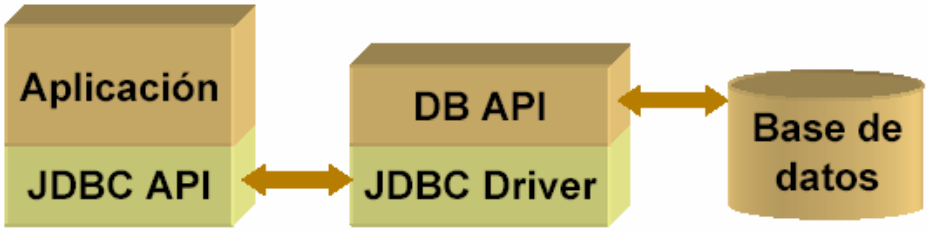


FIGURA No. C.1. Modelo de Operación de JDBC

b) Java Transaction API (JTA)

Es una interfaz estándar utilizada para demarcar transacciones. La arquitectura J2EE provee por defecto un auto commit para la gestión del commit y roll back de transacciones. Un auto commit significa que cualquier otra aplicación viendo los datos, verán su actualización después de cada operación de lectura – escritura. Sin embargo si la aplicación ejecuta dos operaciones de acceso a la base de datos que sean dependientes, será necesario utilizar JTA para demarcar donde la transacción entera, incluyendo ambas operaciones, comienza, se reversan o se comprometen. JTA funciona soportado con los servicios de Java Transaction Services (JTS). JTS es un conjunto de interfazs de bajo nivel utilizada detrás de escena por los componentes EJB. El código cliente nunca interactúa directamente con éstas interfazs. JTS permite que se pueda implementar el soporte a transacciones en un ambiente distribuido y heterogéneo. JTS está basado en la

especificación Object Transaction Service (OTS), que es parte de CORBA.

c) Java Naming and Directory Interfaz (JNDI)

Provee la funcionalidad de nombramiento y directorio, prestando a las aplicaciones métodos para llevar a cabo operaciones estándar de directorio, como asociar atributos con objetos y búsqueda de objetos en base de atributos.

A través de JNDI una aplicación puede almacenar y recuperar cualquier tipo de objeto Java nombrado. Puede utilizarse para múltiples servicios de directorio como: LDAP, NDS, DNS y NIS. JNDI es una interfaz no una implementación.

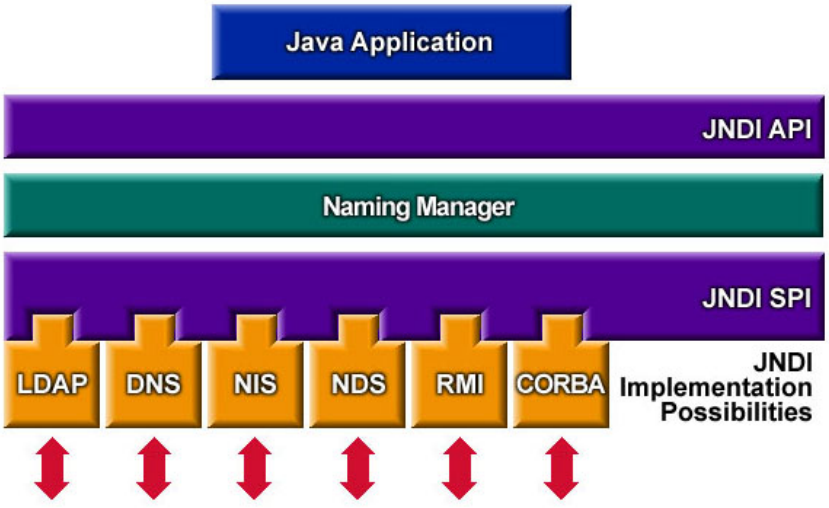


FIGURA No. C.2. Modelo de Operación de JNDI

d) Servicio de Autenticación y Autorización de Java (JAAS)

JAAS provee un mecanismo para que una aplicación J2EE autentique y autorice a un usuario específico o a un grupo de usuarios. JAAS es la versión en Java del framework PAM (Pluggable Authentication Module) que hereda la arquitectura de seguridad de J2EE para soportar la autorización basada en usuario.

e) Arquitectura de conectores (JCA)

Utilizada por los fabricantes de herramientas J2EE e integradores de sistemas para adaptadores de recursos que soporten el acceso a sistemas de información empresarial que puedan ser conectados a un producto J2EE. Un adaptador de recursos es un componente de software que permite a los componentes de una aplicación J2EE acceder e interactuar con el administrador de recursos de capas inferiores.

f) API para el procesamiento XML

JAXP soporta el procesamiento de documentos XML utilizando DOM, SAX (Simple API for parsing XML), y el lenguaje de transformación de hojas de estilo XML (XSLT). JAXP permite a las aplicaciones hacer un análisis sintáctico de documentos XML y transformarlos de manera

independiente de una implementación de procesamiento XML en particular. Soporta además namespaces, lo que permite trabajar con esquemas que de otra manera podrían tener conflictos de nombramiento. JAXP fue diseñado para ser flexible, le permite utilizar cualquier procesador XSL compatible con parser XML y soporte al esquema W3C.

g) API para el registro XML

JAXR le permite acceder a registros de negocio y propósito general en el web. Soporta los estándares de registro y repositorio ebXML y las especificaciones emergentes UDDI.

h) API Java para RPC basado en XML

JAX-RPC utiliza los estándares SOAP y HTTP de modo que los clientes se puedan hacer invocaciones RPC basados en XML sobre el Internet. JAX-RPC soporta WSDL de modo que se puede importar y exportar documentos WSDL.

Con JAX-RPC se puede operar entre aplicaciones y servidores corriendo sobre plataformas Java y no Java.

i) API SOAP para adjuntos Java

SAAJ es un API de bajo nivel de la cual JAX/RPC depende. Permite la producción y consumo de mensajes conforme a la especificación SOAP 1.1 y con la nota SOAP con adjuntos.

2. Tecnologías de Comunicación

a) Java Message Server (JMS)

Estándar de mensajería que permite a componentes de la aplicación J2EE, crear, enviar, recibir y leer mensajes. Permite una comunicación distribuida con bajo acoplamiento, confiable y asíncrona.

b) JavaMail

Se puede utilizar el API JavaMail para enviar notificaciones vía e-mail. El API tiene dos partes:

- ✓ Una interfaz a nivel de aplicación utilizada por los componentes de aplicación para enviar e-mails.
- ✓ Una interfaz del proveedor del servicio.

3. Tecnología EJB

La tecnología EJB es la piedra angular de la especificación J2EE, y se encuentra establecida desde hace ya algún tiempo. EJB es una tecnología de componentes del lado del servidor, que facilitan el desarrollo de aplicaciones en Java, provistas de calidad empresarial, lo que significa que sean transaccionales, distribuidas, múltiple capa, portables, seguras, escalables y confiables. Los componentes al estar alojados dentro del contenedor EJB del servidor J2EE, son provistos de servicios tales como: gestión de recursos (pool de conexiones a la base de datos), coordinación de transacciones (gestionadas por el contenedor) y gestión de la persistencia. El desarrollador al estar liberado de la responsabilidad de escribir código de sistema de bajo nivel, centra su esfuerzo en la implementación de las reglas de negocio demandadas. Los componentes son portables entre cualquier servidor J2EE compatible con la especificación, y se logra esta adaptación a diferentes ambientes operacionales, en donde pueden haber diferentes políticas de seguridad, diferentes bases de datos y diferentes modelos transaccionales, gracias al descriptor de implantación. El descriptor de implantación es un archivo XML que especifica las características del comportamiento de los componentes en tiempo de ejecución. De ésta

manera se modifica el comportamiento de los componentes de manera declarativa sin topar el código.

Un desarrollador de componentes empresariales EJB, tiene que escribir tres archivos en Java. Primero, la interfaz Home EJB, la cual define los métodos que serán utilizados por los clientes para crear y ubicar su componente. Segundo, tiene que escribir la interfaz remota EJB, la cual define los métodos de negocio del componente. Finalmente, se construye el componente que implementa todos los métodos. En el contenedor, al momento de implantar los componentes, se crean dos objetos internos, el objeto EJB Home y EJB Remote. Estos objetos son implementaciones de las interfazs ya definidas por el desarrollador, de modo que cuando el cliente quiera invocar alguno de los métodos de negocio de los componentes empresariales, hablará con estos dos objetos intermediarios. Esto permite un manejo adecuado de la concurrencia por parte del contenedor, así como también la interceptación de las invocaciones de modo que se pueda proveer los servicios de sistema como seguridad, transaccionalidad, persistencia, gestión de recursos y gestión del ciclo de vida. En la siguiente figura se muestra de manera bastante simplificada la tecnología EJB.

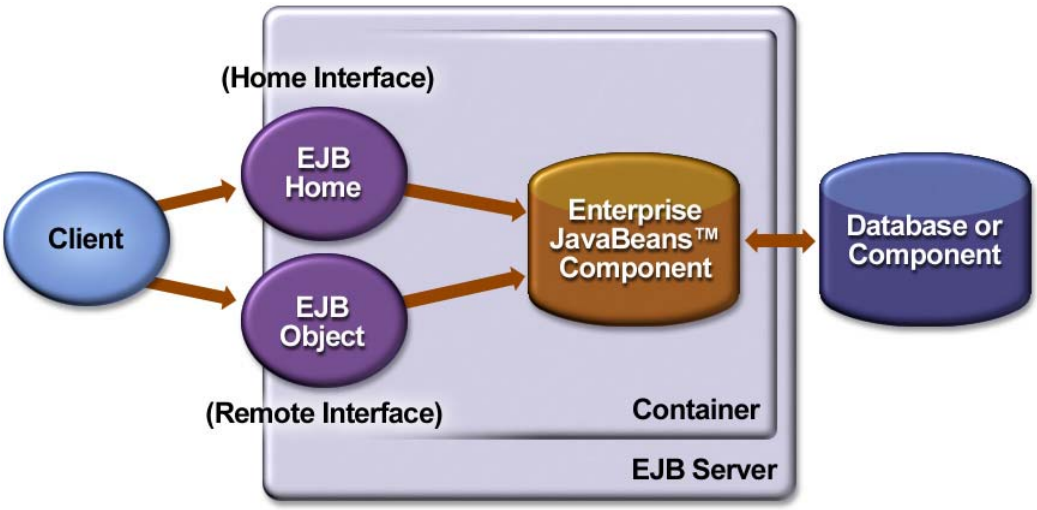


FIGURA No. C.3. Modelo de Operación de la Tecnología EJB

Los componentes EJB son código que a través de la implementación de campos y métodos en las clases, instrumentan los módulos de la lógica de negocio. Existen tres clases de componentes EJB: entity bean, session bean, y message-driven bean. Al ser la tecnología EJB la más importante dentro de todas las tecnologías que implementan la especificación J2EE, es necesario dar una breve descripción de cada una de éstas clases de componentes.

a) Session Bean

Un Session Bean representa trabajo en ejecución por parte del código cliente que lo invoca. Son objetos de procesos de negocio. Implementan lógica de negocio, reglas de negocio y flujos de trabajo. Son componentes reutilizables que contienen lógica para los procesos

de negocio. Ejemplos de session beans tenemos: cotización de precios, ingreso de orden, compresión de video, transacción bancaria, mercado de valores, etc. Se puede ver en los ejemplos que representan procesos.

Un session bean se llama así porque “viven” tanto como la sesión del cliente cuyo código invocó al session bean. Por ejemplo, si el código cliente contacta al session bean para ejecutar una lógica de ingreso de órdenes, el servidor de aplicaciones es responsable de crear una instancia de tal componente session bean. Cuando el cliente se desconecte, el servidor de aplicaciones tendrá que destruir la instancia del session bean.

Un session bean es utilizado por un cliente a la vez, es decir no son compartidos entre clientes. Esto es un severo contraste con los Entity Beans que son compartidos entre muchos clientes como se verá más adelante.

El servidor de aplicaciones es el responsable de administrar el ciclo de vida del componente. Esto quiere decir que el cliente no instancia directamente un session bean, el contenedor lo hace automáticamente. Así mismo el servidor de aplicaciones destruye al componente cuando

es adecuado hacerlo. Esto permite que se pueda tener un consorcio de componentes para que sean reutilizados por múltiples clientes.

Para ponerlo en mayor detalle, es necesario también indicar que hay dos tipos de session beans:

- ✓ **Stateful Session Beans.-** Dijimos antes que los componentes session bean representan procesos de negocio. Algunos de éstos procesos pueden ejecutarse en una sola petición, como el cálculo de precio de un bien, o la verificación de una cuenta de una tarjeta de crédito. Otros métodos pueden ser más detallosos y requerir múltiples peticiones y transacciones. El típico ejemplo de éste tipo de procesos es el carro de compras de una tienda en línea. El cliente cada vez añadirá uno a uno los productos que desea, por ende tal proceso de negocio debe controlar el estado del usuario (el carro de compras) de petición en petición. Un componente Stateful Session Bean está diseñado para procesos de negocio que se dividen en múltiples peticiones y transacciones. Para hacer esto, el componente *retiene el estado* de un cliente individual. Si el estado del Stateful Session Bean es cambiado durante una invocación de algún método, ese mismo estado estará disponible para el mismo cliente hasta la siguiente invocación.

- ✓ **Stateless Session Bean.-** Algunos procesos de negocio se prestan para el paradigma de una sola petición. Un proceso de negocio de una sola petición, es aquel que no requiere que se mantenga el estado entre diferentes invocaciones de métodos. Los Stateless Session Bean son los más adecuados para este tipo de situación. Son proveedores anónimos de métodos, porque no están pendientes ni concientes de la historia del cliente. Ejemplo de un Stateless Session Bean puede ser un motor de alto desempeño que resuelve operaciones matemáticas complejas dada una determinada entrada, tal como una compresión de video o audio. El cliente puede pasar un buffer de datos sin comprimir, así como el factor de compresión. El componente retornará un buffer comprimido y luego estará disponible para servir a otro cliente. El proceso de negocio sigue el paradigma de una sola petición y por lo tanto no necesita retener el estado de la sesión previa.

b) Entity Bean

Otra parte fundamental de los negocios son los datos permanentes que los procesos de negocio utilizan. En casi todos los procesos de negocio, los componentes requieren manipular datos de algún almacén persistente, como una base de datos relacional. Un Entity Bean es un componente que representa tales datos persistentes. Ejemplos de

modelamiento con Entity Beans son: cuenta bancaria, orden, item de una orden, etc. Los Entity Bean representan objetos del mundo real, tales como clientes, productos o empleados.

Los Entity Bean no contienen lógica de procesos de negocio – solo modelan datos. Los Session Bean como vimos ya, son los encargados de modelar procesos de negocio. Los Session Bean pueden utilizar Entity Beans para representar los datos que utilizan.

El valor que un Entity Bean provee, es una representación orientada a objetos en memoria de los datos almacenados en un almacén de datos. La forma tradicional en que las aplicaciones tratan con datos, es trabajar con tablas relacionales de una base de datos, leyendo y escribiendo los datos en la medida que son necesarios. Los Entity Beans en cambio, son objetos de representación de tales datos. Se puede tratar a datos almacenados en un almacén relacional, como objetos reales. Se puede leer un conjunto completo de datos de una base de datos y sacarlos a memoria en un componente Entity Bean. Puede luego manipular este Entity Bean en memoria invocando sus métodos. Los Entity Bean permiten combinar la funcionalidad de datos persistentes con la conveniencia de la encapsulación de los objetos. En

esencia, un Entity Bean implementa la lógica de acceso a la capa de datos en una arquitectura múltiple capa.

Debido a que modelan datos permanentes, los Entity Beans tienen larga vida. Sobreviven a fallas críticas del sistema, ya que representan datos almacenados de manera permanente en algún tipo de medio persistente, a partir del cual pueden ser reconstruidos. Esta es la gran diferencia entre Session Beans y Entity Beans, los Entity Beans tienen un ciclo de vida mucho más prolongado que una sesión de cliente, quizás duren años, dependiendo que tanto tiempo estén los datos en la base de datos. En la siguiente Figura tenemos una representación de los Entity Bean.

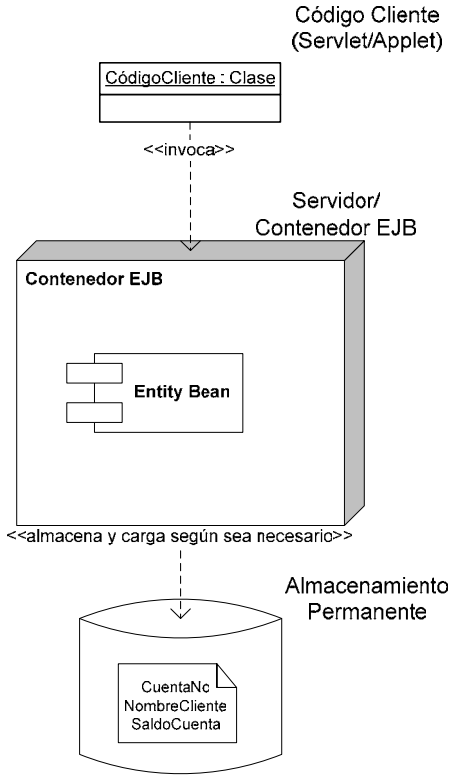


FIGURA No. C.4. Representación de un Componente Entity Bean

Un Entity Bean es distinto de un Session Bean en otro aspecto. Múltiples clientes pueden utilizar los componentes Entity Bean simultáneamente. Es decir de hecho, múltiples clientes estarán manipulando los datos sobre una base de datos de manera simultánea. Uno puede aislar estos clientes de otros utilizando transacciones. Cuando se utiliza de manera adecuada, las transacciones garantizan que múltiples clientes que ejecutan operaciones sobre datos persistentes actúen de manera completamente independiente unos de otros.

Los Entity Beans son muy útiles cuando existen ya bases de datos legadas con datos almacenados por años, ya que permiten tener acceso a tales datos. De hecho los registros de la base de datos pueden haber existido mucho tiempo antes de que la organización anticipe una implementación de un sistema empresarial con tecnología Java.

Hay dos tipos de Entity Beans:

- ✓ **Bean-Managed Persistent Entity Beans (BMP).-** Los Entity Beans son componentes persistentes porque sus estados son almacenados en almacenamiento secundario tal como una base de datos. Un BMP es un componente cuya persistencia es manejada a mano. Es decir, el desarrollador del componente escribe el código para traducir los campos en memoria de su objeto en un almacén de datos de bajo nivel, tal como una base de datos relacional o una base de datos de objetos. El desarrollador se encarga por sí mismo de las operaciones de persistencia – incluyendo el almacenar, cargar, y encontrar datos – dentro del Entity Bean. Para el efecto el desarrollador debe utilizar un API de persistencia como JDBC o SQL/J.

- ✓ **Container-Managed Persistent Entity Beans (CMP).-** Pero la Tecnología Java puede ahorrar a los desarrolladores la preocupación

de codificar la lógica de persistencia. La especificación incluye persistencia automática para los Entity Beans. El contenedor ejecuta toda función que su componente requiere, incluyendo almacenar, cargar y encontrar datos del componente. Como desarrollador en éste esquema no necesita tratar con las APIs de persistencia lo que significa menos tiempo y esfuerzo. En vez de ello, uno describe que desea persistencia gestionada por el contenedor, y el contenedor se encarga de todas las operaciones y funciones por usted. Esto permite tener una independencia teórica de la base de datos.

c) Message-driven Bean (MDB)

Antes del aparecimiento de los MDB en la especificación EJB 2.0, solo se podía soportar el paso de mensajes asíncronos, escribiendo un programa externo en Java que actúa como listener. Un listener es un programa cuyo único propósito es esperar el arribo de datos, por ejemplo, un programa socket servidor que “escucha” en un socket y ejecuta alguna acción cuando detecta la conexión con el cliente. El listener entonces puede invocar métodos en componentes del tipo session bean o entity bean. Todas las invocaciones de métodos en componentes EJB tenían que ser síncronas e iniciadas por el cliente. Este enfoque tenía la desventaja, de que el mensajes sería recibido

fuera del servidor, por lo tanto no podía ser parte de una transacción EJB.

Con la entrega de J2EE 1.3, se pueden utilizar Message-driven beans para combinar la funcionalidad de los componentes EJB con los servicios Java Message Service (JMS).

Dentro de las principales características de JMS, tenemos:

- ✓ JMS es el API de Java que especifican como las aplicaciones pueden crear, enviar, recibir y leer mensajes.
- ✓ JMS permite la comunicación tanto asíncrona como confiable, minimizando la cantidad de conocimiento requerido para su programación.

La implementación del API JMS fue provista por varios fabricantes de software que son conocidos como proveedores de JMS.

Las colas de mensajes, están asociadas con el dominio de mensajes de extremo a extremo. Un mensaje en cola no es persistente; son enviados inmediatamente a todos los suscriptores existentes.

Un MDB generalmente se construye para consumir mensajes, a pesar de que puede crear y enviar mensajes, exactamente igual que cualquier

otro componente EJB. Un MDB vive dentro del contenedor, y no tiene un contexto de seguridad por sí solo. Cuando el componente se implanta, se asocia con una cola o tópico en particular, y es invocado por el contenedor cuando el mensaje arriba en dicha cola o tópico.

Las siguientes son las características del Message-driven Bean:

- ✓ Es anónimo; es decir, no es visible al cliente. No se mantiene ningún estado por parte del cliente.
- ✓ Todas las instancias de un Message-driven Bean en particular, son equivalentes.
- ✓ El contenedor puede crear un consorcio de instancias.
- ✓ No tiene interfaz remota ni local.
- ✓ Es invocado asíncronamente por el contenedor.
- ✓ Los componentes viven en el contenedor; el contenedor gestiona su ciclo de vida y el entorno.

Para los clientes que generan mensajes JMS, el MDB es tan solo un consumidor de mensajes anónimo. El cliente no necesita saber que el consumidor del mensaje es un MDB. El cliente simplemente envía sus

mensajes a sus destinatarios, bien sea una cola o un tópico, y el componente gestiona el mensaje a su arribo. Por tanto, la construcción de un mensaje debe es seguir la especificación JMS y el destinatario debe tener un nombre registrado en JNDI. A parte de ello, el mensaje no tiene que corresponder a ningún formato en particular.

No es necesario que el cliente sea una aplicación Java u otro componente EJB, puede ser un componente JSP o una aplicación no escrita en J2EE.

En algunos aspectos, el MDB es parecido a un componente Stateless Session Bean. Es un componente EJB completo que encapsula lógica de negocio. La ventaja es que el contenedor es el responsable de proveer seguridad, concurrencia, transacciones y demás. Como un Session Bean, un Message-driven Bean tiene una clase y un archivo XML descriptor de implantación.

La principal diferencia de otros componentes EJB, es que el MDB no puede ser invocado directamente por el cliente. Por tal razón, no tiene interfazs Home, Remote o Local, esto hace que sea menos propenso el mal uso por parte del cliente.

En el patrón de diseño de arquitectura de software, el Model se implementa normalmente con EJBs.

4. Tecnología Java Servlet

Permite definir clases servlet HTTP específicas, que heredan las capacidades de aplicaciones alojadas en los servidores con el modelo de aplicación petición – respuesta. A pesar de que pueden responder a cualquier tipo de petición, se utilizan comúnmente para extender las aplicaciones alojadas en los servidores web, generando contenido dinámico. En el patrón de diseño de arquitectura de software, el Controller se implementa normalmente con Servlets.

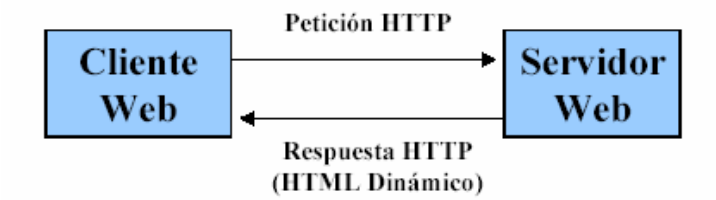


FIGURA No. C.5. Modelo de Operación de los Servlets

5. Tecnología JavaServer Pages (JSP)

Permiten poner pequeñas partes de código de un servlet, directamente en una página basada en un documento. Una página JSP tiene dos tipos de texto:

- ✓ Una plantilla de datos estáticos, expresada en cualquier formato basado en texto, como HTML, XML ó WML.

- ✓ Elementos JSP, que determinan como se construye el contenido dinámico de la página.

JavaBeans Activation Framework (JAF)

JAF está incluida en la plataforma porque JavaMail lo utiliza. Provee servicios estándar para determinar el tipo de una pieza arbitraria de datos, encapsular el acceso a ellos, descubrir las operaciones disponibles sobre ellos, y crear los componentes JavaBeans apropiados para llevar a cabo esas operaciones.

6. Otras tecnologías a mencionar

a) Java Remote Method Invocation (RMI) y RMI-IIOP

Los componentes EJB dependen de casi todo el resto de API de la especificación J2EE, pero fundamentalmente de RMI. RMI es un mecanismo que permite la comunición interprocesos y la invocación de métodos ubicados en otras máquinas remotamente. Los componentes EJB confían en RMI para la comunicación entre los componentes y sus clientes. RMI abstrae al programador de los detalles de codificación de

aspectos como el soporte a redes, parámetros de bajo nivel, orden de bytes entre máquinas, etc. RMI soporta otras características como descargar dinámicamente clases, activación automática de objetos remotos, y un recolector de basura distribuido para eliminar objetos remotos que ya no están en uso.

RMI-IIOP es una extensión portable de RMI que utiliza el protocolo Internet Inter-ORB (IIOP) desarrollado de manera conjunta por SUN Microsystems, IBM y otros fabricantes miembros de OMG (Object Management Group). Es más portable que RMI porque soporta a IIOP como protocolo de comunicación. IIOP es un protocolo de comunicación muy robusto que añade calidad de servicio a RMI. IIOP es además necesario para la integración de J2EE con CORBA.

b) Java IDL

Es la implementación de CORBA basada en Java de SUN Microsystems. Java IDL permite la integración con otros lenguajes de programación. Java IDL también permite que sus objetos distribuidos puedan aprovechar los servicios disponibles de CORBA. Gracias a Java IDL es que J2EE es totalmente compatible con CORBA.

c) XML

XML es un lenguaje de marcado basado en texto que rápidamente se ha vuelto en el estándar de intercambio de datos en el web. Igual que HTML utiliza etiquetas para identificar los datos (<etiqueta>). Pero a diferencia de HTML, XML identifica datos en vez de indicar como éstos datos deben ser mostrados. Una etiqueta XML actúa como el nombre de un campo en un programa. Al ser posible la identificación de los datos, se puede lograr entender lo que éstos datos “significan”, permitiendo entender como interpretarlos y que hacer con ellos. Dicho de manera simplificada, XML es un mecanismo para especificar la “semántica” (significado) de los datos.

Las etiquetas permiten darle sentido a la estructura de datos de una aplicación. Pero para que múltiples aplicaciones puedan utilizar los mismos datos, deben ponerse de alguna manera de acuerdo con el nombre de las etiquetas que van a utilizar.

Un archivo XML siempre comienza con un prólogo, el que contiene una declaración que identifica el archivo como un documento XML de la siguiente manera:

<?xml version=”1.0”?>

Puede contener información adicional como:

<?xml version=”1.0” encoding=”ISO-8859-1” standalone=”yes”?>

La declaración puede incluir los siguientes atributos:

- ✓ **version.-** Identifica la versión de XML utilizada en los datos. Este atributo no es opciional.

- ✓ **encoding.-** Identifica el conjunto de caracteres para codificar los datos. “ISO-8859-1” es “Latin 1” el conjunto de caracteres del idioma inglés y del oeste de Europa. Por defecto es el Unicode comprimido: UTF-8.

- ✓ **standalone.-** Indica si se referencia o no desde éste documento una entidad externa o una especificación de tipos de datos externos. Si no hay referencias externas el valor es “yes”.

El prólogo puede también contener definición de entidades (ítems que son insertados cuando se los referencia dentro del documento) y especificaciones que indican que etiquetas son válidas dentro del documento, tanto declaradas en un DTD (Document Type Definition) o que pueden estar declaradas directamente en el prólogo, o con punteros a especificaciones en un archivo externo. A pesar de ser

opcional, es recomendable incluir al menos en el prólogo la versión utilizada y la encodificación, de modo que se pueda simplificar la estandarización en el futuro y los datos puedan ser localizados en cualquier momento y lugar.

Luego del prólogo un documento XML tiene las instrucciones de procesamiento, las que dan disposiciones o instrucciones a una aplicación que está procesando los datos XML. Las instrucciones de procesamiento tienen el siguiente formato:

<?target instructions?>

Donde target es el nombre de la aplicación que se espera realice el procesamiento, e instructions es una cadena de caracteres que constituye la información o comandos para que la aplicación procese.

Al ser las instrucciones específicas de la aplicación, se pueden tener múltiples instrucciones de procesamiento que indiquen a diferentes aplicaciones como hacer cosas similares, pero de manera distinta. Por ejemplo, un archivo XML para una presentación de diapositivas, puede incluir instrucciones de procesamiento que le permitan al expositor definir si la presentación que se realizará es de nivel técnico o gerencial.

Por qué XML es tan importante?

- ✓ **Texto plano.-** XML ya no es formato binario, se puede crear y editar archivos con cualquier editor de texto o ambiente de desarrollo visual. Por otro lado un front end XML de una base de datos le permite almacenar de manera eficiente grandes cantidades de datos. XML provee así una escalabilidad desde pequeñas configuraciones de archivos hasta enormes repositorios de datos corporativos.

- ✓ **Identificación de datos.-** XML indica que clase de datos tiene y no como mostrarlos. Ya que las etiquetas identifican la información y dividen la data en partes, un programa e-mail puede procesarlos, un programa de búsqueda puede realizar búsqueda de mensajes enviados a una persona en particular, y una libreta de direcciones puede extraer la información de dirección desde el resto del mensaje. Es decir como las diferentes partes de la información se encuentra identificada, puede ser utilizada de maneras diferentes por diferentes aplicaciones.

- ✓ **Capacidad de estilos (stylability).-** Cuando el despliegue es importante, el estándar de estilos XSL, le indica como mostrar los datos. Por ejemplo, la hoja de estilo para:

  <to>destino@destino.com</to>

Puede disponer:

Comience en línea nueva.

Muestre “To:” en negrita, seguido de un espacio en blanco.

Muestre los datos de destino.

Lo que produce la siguiente salida:

To: destino@destino.com

Al ser XML libre de estilo, se pueden utilizar distintas hojas de estilo para producir diferentes salidas: texto, postcipt, TEX, pdf, etc.

- ✓ **Reutilización en línea.-** Una de las mejores características de XML es que puede estar compuesto de entidades separadas. En HTML se puede hacer esto pero vinculando otros documentos, en cambio en XML las diferentes entidades pueden ser incluidas en línea en un mismo documento, así uno puede realizar búsquedas en todo el documento y descargarlo de una sola vez. Esto permite la modularización del documento, sin tener que emplear vínculos. Uno puede tener una fuente única por cada sección, de modo que la edición sobre ésta sección se refleja en cualquier parte que la sección

sea utilizada, y los documentos compuestos con ésta pieza lucirán como piezas únicas en todo el mundo.

- ✓ **Capacidad de vinculación (linkability).-** Gracias a HTML, la necesidad de definir vínculos ahora es una necesidad. Se pueden definir dos tipos de vínculos, vínculos de múltiples objetivo o “expandibles”, que al hacer clic permiten que la información del objetivo se muestre en línea; y vínculos entre dos documentos, definidos en un tercero.

- ✓ **Facilidad de procesamiento.-** Una notación regular y consistente, hace que sea fácil construir un programa que procese datos XML. Las fuertes restricciones aplicadas para garantizar que un documento XML esté bien formado, permite que los programas analizadores sintácticos (parser) sean capaces de leer los datos. Al ser XML un estándar neutro de fabricante, se puede escoger cualquier analizador sintáctico, cualquiera de ellos será capaz de procesar datos XML.

- ✓ **Jerárquico.-** Los documentos XML se benefician de su estructura jerárquica. Las estructuras jerárquicas de documentos son más rápidas de acceder porque se puede taladrar hasta el nivel que se requiera, tal como si se recorriera una tabla de contenidos. Son

también fáciles de reordenar puesto que cada pieza de información está delimitada.

XML y las especificaciones relacionadas

Es importante presentar una revisión de los acrónimos relacionados con XML y lo que éstos significan. La presente revisión no pretende ser completa ni exhaustiva, puesto que existen significativos esfuerzos de desarrollo relacionados con XML en la industria del software.

Los APIs para acceder a documentos XML bien sea de manera serial o randómicamente, son SAX y DOM.

La especificación para asegurar la validez de un documento XML es DTD (mecanismo original definido como parte de la especificación XML), y hay además varios estándares propuestos (mecanismos nuevos que utilizan la sintaxis XML para hacer el trabajo de describir nuevos esquemas de validación).

Existen estándares que están por completarse, como XSL, que es un mecanismo para establecer la traducción de documentos XML (por ejemplo a HTML u otro XML), y para indicar como el documento es renderizado. La parte de transformación de éste estándar XSLT y +XPATH está en su fase de revisión final.

Existe otro esfuerzo casi terminado para la especificación del lenguaje de vinculación XML (XML Linking), que permite definir vinculación entre documentos XML.

Existen otros esquemas relacionados con XML como XHTML, RDF, Xlink y XPointer. Así como también aplicaciones puntuales como SMIL, MathML, etc.

Estándares básicos de XML

SAX (Simple API for XML).- Es más el resultado de un grupo de discusión y colaboración, que del consorcio W3C. Define el acceso serial a un documento XML. Es el mecanismo más rápido de ejecución que se puede utilizar para escribir o leer datos XML. También es llamado protocolo para manejo de eventos, porque registra el manejador con un programa analizador sintáctico XML, luego de lo cual éste programa invoca los métodos de retorno cada que ve una nueva etiqueta XML.

DOM (Document Object Model).- El protocolo DOM convierte un documento XML en una colección de objetos en el programa. Luego se puede manipular estos objetos por parte de una aplicación. Este mecanismo también se conoce como acceso randómico, porque

permite tener acceso a cualquier parte de los datos en cualquier momento. Se puede modificar los datos, eliminarlos o insertar nuevos datos.

JDOM y dom4j.- DOM provee suficiente poder para el procesamiento orientado a documentos, pero no provee mucho para la programación orientada a objetos. Los APIs JDOM y dom4j son útiles para el procesamiento de estructuras de datos definidas en XML. Las principales diferencias entre ambas APIs son:

- ✓ JDOM es más limpio y pequeño, cuando el estilo de codificación es importante, JDOM es una buena alternativa.

  JDOM es una iniciativa del Java Community Proccess (JCP). Cuando esté terminado será un estándar.

- ✓ dom4j es una implementación más pequeña y rápida ya utilizada durante algunos años. Es una implementación basada en el patrón Factory. Esto facilita la modificación para aplicaciones complejas de propósito especial.

DTD (Document Type Definition).- Es parte de la especificación XML, sin embargo es opcional, es decir se puede escribir un documento XML sin un DTD. Hay varios esquemas de estándares propuestos más

flexibles que DTD, por lo que se lo trata a menudo como una especificación separada. El DTD indica que tipo de etiquetas puede incluirse en el documento, y los arreglos básicos de dichas etiquetas. Se utiliza DTD para asegurarse que no se construya una estructura XML no válida. Desafortunadamente es difícil especificar un DTD para un documento complejo de modo que prevenga todas las combinaciones no válidas y permita las válidas. El DTD puede existir en el mismo documento como parte del prólogo. Puede existir también como una entidad separada, o puede ser dividido en el prólogo y una o más entidades adicionales.

Namespaces.- Éste estándar permite escribir documentos XML que utilizan dos o más conjuntos de etiquetas de manera modular. Define mecanismos para calificar los nombres de modo que se elimine la ambigüedad, permitiendo que los programas utilicen información de otras fuentes y hacer las cosas correctas con ello.

XSL (Extensible Stylesheet Language).- El estándar XML específica como identificar los datos, no como mostrarlos. HTML indica como mostrar los datos sin indicar lo que son. El estándar XSL tiene dos partes: XSLT (estándar de transformación) y el XSL-FO (encargada del formato de los objetos, llamado a veces flujo de objetos). Con XSL-FO

se puede tener la habilidad de definir múltiples áreas en la página y luego vincularlas todas juntas.

XSLT (+PATH) (Extensible Stylesheet Languaje for Transformation).- Es un mecanismo de traducción que le permite especificar en que convertir una etiqueta XML de modo que pueda ser mostrada en un formato definido, por ejemplo HTML. Se puede tener distintos formatos para mostrar los mismos datos de manera diferente para diferentes usos. +XPATH es un mecanismo de direccionamiento que se utiliza cuando se construye instrucciones de transformación, para especificar que partes de la estructura XML se quiere transformar.

Los servicios Web

Son aplicaciones empresariales basadas en el web, que utilizan estándares abiertos XML y protocolos de transporte para intercambiar datos en respuesta a invocaciones de clientes.

Al permitir Java portabilidad de código de las aplicaciones, y XML portabilidad de datos; la traducción de datos a cadenas de datos estandarizadas basadas en XML es lo que hace que los servicios web y los clientes escritos en Java con los API Java XML sean totalmente interoperables.

Los servicios web son importantes por dos razones fundamentales:

- ✓ **Ubicuidad.-** Es un término frecuente empleado por las dos plataformas líderes de implementación de aplicaciones empresariales: J2EE y Microsoft .Net.

- ✓ **Facilidad de uso.-** Requiere mucho menos habilidades técnicas para su implementación. La tecnología de servicios web está orientada hacia una comunidad menos técnica, emplea herramientas más simples que por lo tanto facilitará su adopción.

La necesidad de integración entre dos enfoques diferentes de desarrollo de aplicaciones empresariales, hace que los servicios web sean una palabra de moda. Definitivamente, es la forma más simple y fácil de integrar J2EE, CORBA y Microsoft .Net.

Los servicios web son tecnología complementaria a otras tecnologías como J2EE, CORBA y Microsoft .Net; no las reemplaza.

Algunas definiciones previas

WSDL

Es un formato XML estandarizado que permite describir un servicio web. La descripción incluye la siguiente información:

- ✓ Nombre del servicio,
- ✓ Ubicación del servicio, y,
- ✓ Indicaciones de cómo comunicarse con el servicio.

Las definiciones WSDL (Web Services Description Language) se almacenan en registros UDDI publicados en el web.

SOAP/UDDI

Son una propuesta desarrollada en conjunto por Microsoft e IBM. SOAP (Simple Object Access Protocol) fue escrito por IBM y ofrecido a la fundación Apache, por lo que la plataforma Apache AXIS es la referencia para la norma SOAP en el W3C. SOAP es un protocolo de comunicación para servicios web, utilizado para intercomunicar aplicaciones. Dentro de las principales problemáticas de SOAP, es que todavía se siguen experimentando entre los desarrolladores, no resuelve completamente el problema de autenticación y no está totalmente soportado en ambientes de desarrollo ampliamente difundidos en el web, como PHP.

SOAP es la alternativa de interoperabilidad de los servicios web implantados tanto en la plataforma J2EE como en la plataforma Microsoft .Net.

UDDI (Universal Description, Discovery and Integration) es un sistema de registro que permite a las organizaciones publicar interna o externamente sus servicios web, y es donde la información puede ser leída y consultada, y globalmente accedida por los clientes. En términos corrientes, funciona a manera de páginas amarillas.

Los servicios web se basan en un modelo de petición – respuesta, donde existe un cliente que solicita un servicio, y existe un proveedor del servicio; ambos interactúan a través los estándares plenamente definidos. En la Figura No. E.8 se muestra un modelo conceptual de la arquitectura para servicios web SOAP/UDDI/WSDL:

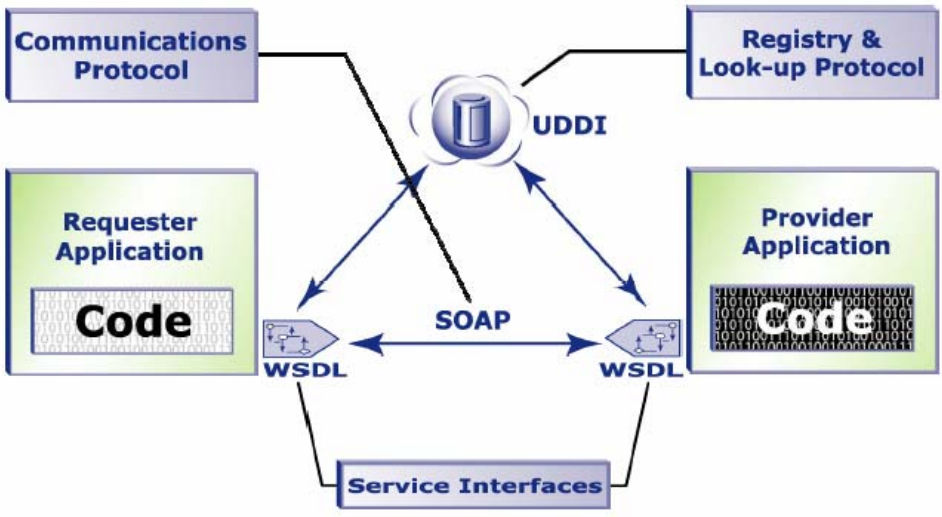


FIGURA No. E.8. Modelo de Operación de SOAP/UDDI/WSDL

ebXML es un estándar global para definir un marco de referencia (framework) propuesto por las Naciones Unidas en OASIS, que trata de resolver la problemática de las comunicaciones entre empresas, con énfasis a proveer un esquema que permita conducir transacciones del tipo B2B, basado en XML.

ebXML utiliza SOAP como medio de transporte, y se dice que es el sucesor de EDI (Electronic Data Interchange). El cliente invoca un servicio web de mensajería enviando un documento completo con un conjunto de parámetros. El servicio web, acepta el documento y retorna una respuesta, la misma que puede ser asíncrona.

ebXML es una colaboración entre servicios web a través de XML. En ebXML tenemos los siguientes componentes:

- ✓ **Registro.-** Provee un "contenedor" para los modelos de procesos, vocabularios y perfiles.
- ✓ **Procesos de negocio.-** Definidos como modelos, expresados en XML.
- ✓ **Acuerdos entre socios colaborativos.-** Expresados en XML, donde se especifican los parámetros para la colaboración.

- ✓ **Componentes centrales.-** Pequeños bits de información que se emplean generalmente para proveer “semántica” al contenido.

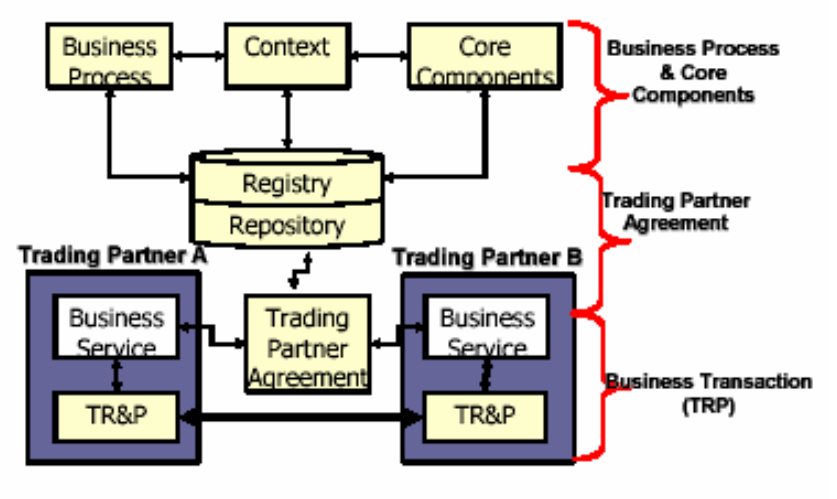


FIGURA No. E.9. Modelo de Operación de ebXML

Ciclo de vida de un servicio web en J2EE desde el punto de vista del proveedor

El desarrollador de un servicio web implementado e implantado en la plataforma J2EE, lo primero que debe hacer es definir la interfaz del servicio web en WSDL, que es el estándar de facto. Una vez definido el servicio, se lo puede implementar, para posteriormente ser implantado. Finalmente, el servicio web debe ser publicado.

La definición del servicio web en WSDL es muy importante porque hace las veces de contrato entre el proveedor del servicio y el cliente del servicio.

Las características de la arquitectura J2EE, de implantar la lógica del negocio como componentes, que se ejecutan en un contenedor, son las que sirven de base para implementar e implantar un servicio web. El contenedor de servicios web, de manera similar a los otros contenedores en J2EE, proveyendo un ambiente de alojamiento de los front end de los servicios web para su ejecución. En éste ambiente de ejecución se provee una vinculación a un transporte y a un puerto. El front end de un servicio web, puede ser el manejador de mensajes SOAP que invoca las funciones de negocio de los componentes J2EE.

Ciclo de vida de un servicio web en J2EE desde el punto de vista del cliente

Como un cliente descubre e invoca un servicio web en la plataforma J2EE. El proceso de invocación más sencillo es en la forma de invocación RPC (Remote Procedure Call), o enviando un mensaje. Típicamente el cliente utilizará un talonario el cual tendrá toda la lógica necesaria para comunicarse con el servicio web.

El proceso de descubrimiento involucra encontrar el documento WSDL o encontrar el talonario cliente cuando esté disponible, el mismo que puede ser generado dinámicamente desde el documento WSDL durante la implantación del cliente o en tiempo de ejecución. El API empleado es JAXR utilizado para servicios de registro como UDDI y ebXML.

El talonario cliente contiene todo el código necesario para la invocación del servicio web, es decir que se conoce el transporte que se necesita y a que punto terminal (puerto) debe conectarse ese transporte para la invocación del servicio web.

En la Figura No. E.10. se muestra la representación del enfoque dado por la plataforma J2EE, para la provisión de servicios web.

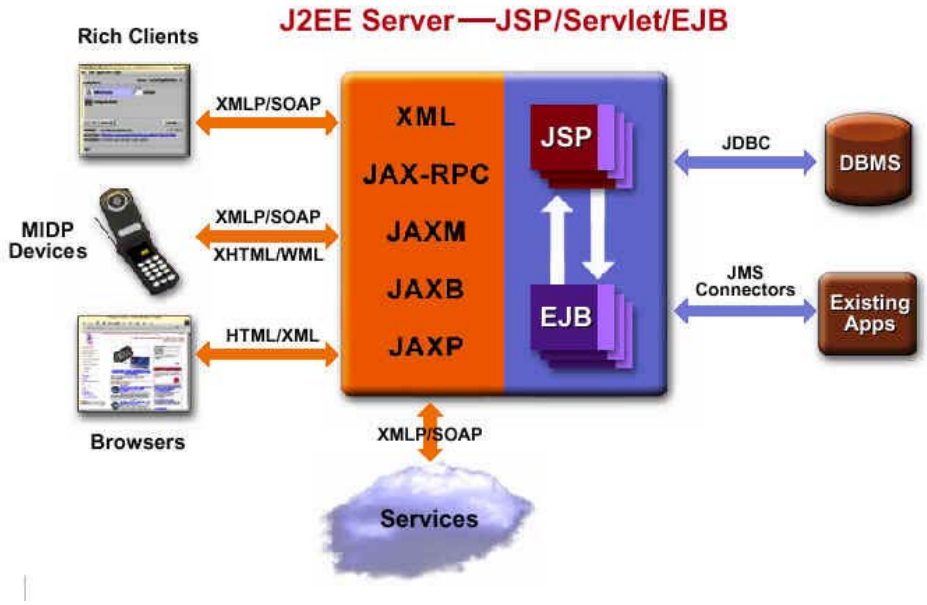


FIGURA No. E.10. Modelo de Operación de servicios web sobre J2EE

APÉNDICE D

PLATAFORMA TECNOLÓGICA DE PROCESAMIENTO

A continuación se muestra el detalle de los equipos a emplear en las Zonas de Servicios Públicos, Servicios Privados y Zona Militarizada, para la respectiva provisión de servicios.

TABLA D - I

EQUIPOS PARA SERVICIOS PÚBLICOS DE INTERNET (DMZ PÚBLICA)

Dependencia de Servicios	Detalles Específico del Servicio	
Servicios de Mensajería Electrónica Corporativa	Provee los servicios de mensajería electrónica a todos los usuarios de la Institución a través de los estándares POP3, IMAPv4, SMTP. **Software.-** Código abierto: Linux, SendMail y Squirrel para proveer WebMail. Soporte e-mail relay Server. Almacenamiento de cuotas de usuario en el NAS Filer.	
	Hardware.- Plataforma Intel / Linux	
	CPU	(2) Xeon 2.4 Ghz, 512 Kb Caché L2
	RAM	2 Gb / 4 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio mail.
Servicios Web y HTTP	Para páginas HTML/XML, soporte de Servlets y JavaServer Pages (JSPs) y soporte a servicios web; a través del servidor Web HTTP. **Software.-** Código abierto: Linux, Apache y Tomcat. Almacenamiento de archivos HTML, XML, JSP, Class, etc. en el NAS Filer.	
	Hardware.- Plataforma Intel / Linux; Servidores típicamente con buenas capacidades de procesamiento y memoria RAM, pero en los que el almacenamiento no es crítico, ya que está delegado a almacenamiento externo.	
	Cluster	3 Nodos
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2

Dependencia de Servicios	Detalles Específico del Servicio	
	RAM	2 Gb / 4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio http.
Consola Antivirus	Servidor de actualizaciones de definiciones de virus informáticos para actualización interna del software antivirus. **Software.-** Innoculate de Computer Associates	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	1 Gb / 4 Gb
	NIC	(2) 10/100 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1
Servidor Proxy Transparente / DNS	Configuración Proxy Transparente para caching de páginas web externas, y resolución de nombres de dominio internos. **Software.-** Código abierto: Linux, SQUID. Almacenamiento de caching en el NAS Filer.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio SQUID y DNS.
Servidor de Balanceo de Carga	Para proveer una infraestructura escalable y tolerante a fallas, especialmente en los servicios más sensibles al usuario final como el correo electrónico, el web interno y el servicio Proxy y Caching se emplea un balanceador de carga en una configuración activo – activo. El servidor global de balanceo de carga es un switch de capa 5/6/7 que permite tener dirección IP y dirección MAC virtuales de modo que en caso de falla de uno de los servidores, automáticamente las peticiones son enrutadas al respaldo.	
	Sesiones concurrentes	1’000.000
	Rendimiento	8 Gbps
	Capacidad de conmutación	32 Gbps (backplane)
	Tasa de redirección de paquetes	12’000.000 pps
	# direcciones IP virtuales	Ilimitadas
	# servidores reales	1.024

Dependencia de Servicios	Detalles Específico del Servicio	
	Puertos 10/100	12
	Puertos 1000	8
Almacenamiento Externo Tipo NAS	Dispositivo de almacenamiento conectado directamente a la red, para lectura / escritura de archivos, donde se instalará el almacenamiento del Mail Server, del Web Server y Caching del Proxy, de modo que se pueda proveer cuotas lo suficientemente grandes a los usuarios del servicio de e-mail y caching. **Software.-** Soporte NFS, HTTP, FTP, CIFS; administración dinámica del almacenamiento, snapshot y snapclone.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	6 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo.
	Capacidad Almacenamiento Inicial	1 Tb.
	Capacidad Almacenamiento Máximo	3 Tb.
IDS	**Sistema de Detección de Intrusos.-** Es un sistema que basado en firmas o patrones de ataques conocidos detecta ataques advirtiendo al administrador. Tipos de ataques a soportar:	
	Exploits	Actividad que indica que alguien intenta obtener acceso a un sistema dentro de la red, tal como un BackOrifice, intentos de login fallidos y TCP hijacking.
	DoS (Negación de servicio)	Actividad que indica que alguien intenta consumir ancho de banda o recursos computacionales para interrumpir las operaciones normales.
	Reconnaissance	Actividad indicativa de que alguien prueba o mapea la red para identificar una “oportunidad”, tales como puertos abiertos, algo que luego se podría convertir en un intento de acceso no autorizado.
	Misuse (mal uso)	Actividad indicativa de que alguien trata de violar la política corporativa de seguridad.
Firewall de borde	Mecanismo de control de flujo entre dos redes, normalmente una protegida y otra no confiable.	
	Arquitectura	ASIC (Application Specific Integrated Circuit)

Dependencia de Servicios	Detalles Específico del Servicio	
	ACL	Creación de Listas de Control de Acceso
	Análisis	Inspección de paquetes en tiempo real
	NAT	Network Address Translation
	Otras:	Reporte automático de actividades, SNMP, VPN, prevención ataques DoS, Mail Relay y filtrado de URL.

TABLA D – II

SERVICIOS PRIVADOS DE INTRANET (DMZ PRIVADA)

Dependencia de Servicios	Detalles Específico del Servicio	
Servidor de Infraestructura de Claves Públicas / Certificados Digitales	Empleo de dos pares de claves asimétricas públicas / privadas, para efectos de firma digital (identificación, autenticación, no repudio) y certificados digitales (encriptamiento, autenticación y autorización), emitidos internamente para usuarios internos y usuarios externos de servicios de red (Ejemplo: Proveedores) **Software.-** Evaluación especializada de seguridad entre Baltimore UniCERT, Entrust Authority Security Manager, OpenCA (Open Source)	
	Hardware.- Plataforma Intel / Linux	
	CPU	(2) Xeon 2.4 Ghz, 512 Kb Caché L2
	RAM	2 Gb / 4 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 72 Gb) Internos en RAID 1 para sistema operativo y repositorio de datos.
Servicios Web y HTTP (Privados)	Para páginas HTML/XML, soporte de Servlets y JavaServer Pages (JSPs) y soporte a servicios web; a través del servidor Web HTTP, para aplicaciones internas. **Software.-** Código abierto: Linux, Apache y Tomcat. Almacenamiento de archivos HTML, XML, JSP, Class, etc. en el NAS Filer del Data Center.	
	Hardware.- Plataforma Intel / Linux; Servidores típicamente con buenas capacidades de procesamiento y memoria RAM, pero en los que el almacenamiento no es crítico, ya que está delegado a almacenamiento externo.	

Dependencia de Servicios	Detalles Específico del Servicio	
	Cluster	3 Nodos
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y servicio HTTP.
Servicios de Directorio Corporativo	Servidor de directorio basado en el estándar LDAP (Lightweight Directory Access Protocol), para administración de identidades (usuarios, grupos de usuarios y recursos) con sus respectivos derechos de acceso para autenticación y autorización. **Software.-** Código abierto: Linux y OpenLDAP. Almacenamiento de archivos en el NAS Filer del Data Center.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	2 Gb / 4 Gb
	NIC	(2) 10/100 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1
Servidor de Servicios Colaborativos	Como Sistema de Información Comunicacional, provee los servicios de mensajería electrónica unificada avanzada a un segmento de usuarios privilegiados, compuesta de la unificación de: correo electrónico, correo de voz (a través de la integración del servidor a la central telefónica del sistema de comunicaciones de las Fuerzas Armadas vía CTI – Computer Telephony Integration), FAX y mensajería instantánea, incluyendo además servicios de valor agregado: Archivos compartidos, Calendario compartido, Reuniones virtuales vía Web Conference, búsquedas extendidas de documentos, gestión de contenido, todo unificado a través de un portal colaborativo. Software**.-** Sistema Operativo Código abierto: Linux; Aplicación: Oracle Collaboration Suite. Almacenamiento en el NAS Filer.	
	CPU	(4) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	12 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 72 Gb) Internos en RAID 1 para sistema operativo y aplicación.
Servicios de Audio / Video en demanda	Como parte de la plataforma de entrenamiento y educación a distancia por medios electrónicos (e-learning), se propone un servidor dedicado a la provisión de servicios de audio y video en demanda.	

Dependencia de Servicios	Detalles Específico del Servicio	
	Software.- Helix Universal Server de RealNetworks, y herramientas complementarias de creación.	
	Hardware.- Plataforma Intel	
	CPU	(1 / 2) Itanium 2 1.3 Ghz, 512 Kb Caché L2, 3 Mb Caché L3.
	RAM	12 Gb / 24 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación.
	Almacenamiento Externo Inicial	(3 x 146 Gb) en RAID 5 para alojamiento de contenido a través de Arreglo Externo conectado directamente (DAS: Direct Attachment Storage)
	Almacenamiento Externo Máximo	(10 x 146 Gb) en RAID 5 para alojamiento de contenido a través de Arreglo Externo conectado directamente (DAS: Direct Attachment Storage)
Servicios de Contenido	Soporte a la creación y administración del contenido corporativo de documentos electrónicos debidamente catalogados e indexados, con soporte a catalogación e indexación automática, generación de índices por palabras claves. **Software.-** Código abierto: Linux e Hipergate. Almacenamiento en el NAS Filer.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	4 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1
Servicios Terminales Windows – Citrix	Extensión de los servicios de terminal de Windows, para computación remota basada en servidor. Este servicio permite habilitar las aplicaciones legadas existentes del tipo cliente – servidor, basadas en Windows, al Intranet basándose en el concepto de emulación de terminales con el software de Citrix. **Software.-** Windows 2003 Server y Citrix Metaframe XP.	
	Hardware.- Plataforma Intel.	
	Cluster	2 Nodos
	CPU	(4) Xeon 2.4 Ghz; 512 Kb
	RAM	8 Gb
	NIC	(2) 10 / 100 / 1000 Mbps

Dependencia de Servicios	Detalles Específico del Servicio	
	Fuente de Poder	Redundante
	HD	(2 x 72 Gb) Internos en RAID 1 para sistema operativo, Citrix Metaframe y aplicaciones Windows.
Servicios DHCP	Para asignación dinámica de direcciones IP para toda la red corporativa, facilitando la administrabilidad de la red desde un sitio central. **Software.-** Código abierto: Linux habilitado el servicio DHCP Server.	
	Hardware.- Plataforma Intel / Linux.	
	Cluster	2 Nodos
	CPU	(2) Xeon 2.4 Ghz; 512 Kb
	RAM	2 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo
Servicios de Administración de Infraestructura	Administración de los dispositivos de la infraestructura tecnológica, basado en SNMP, para captura y presentación de variables SNMP de los diferentes dispositivos de procesamiento y red de la infraestructura; captura de mensajes de error / advertencias de los dispositivos de red y control de dispositivos de tiempo de la red. Verificación en tiempo real de parámetros de broadcast / multicast / unicast de la red. Autenticación a dispositivos críticos de la red a través de RADIUS/TACACS. Servidor de acceso a dispositivos de red vía SSH. Servidor de monitoreo de servicios.	
	Hardware.- Plataforma Intel.	
	Servidor de Monitoreo (W2K-AS) – Software Unicenter de Computer Associates	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb
	RAM	2 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 72 Gb) Internos en RAID 1 para sistema operativo y aplicación SNMP.
	Servidor de Sniffing de la red (W2K AS – LAN Explorer)	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb L2
	RAM	512 Mb
	NIC	(2) 10 / 100 / 1000 Mbps

Dependencia de Servicios	Detalles Específico del Servicio	
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación.
	Monitoreo de servicios: RADIUS/TACACS, NTP, MRTG – Linux.	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb
	RAM	1 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación.
	Servidor de acceso a dispositivos de red (SSH)	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb
	RAM	1 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación.
IDS	**Sistema de Detección de Intrusos.-** Es un sistema que basado en firmas o patrones de ataques conocidos detecta ataques advirtiendo al administrador. Tipos de ataques a soportar:	
	Exploits	Actividad que indica que alguien intenta obtener acceso a un sistema dentro de la red, tal como un BackOrifice, intentos de login fallidos y TCP hijacking.
	DoS (Negación de servicio)	Actividad que indica que alguien intenta consumir ancho de banda o recursos computacionales para interrumpir las operaciones normales.
	Reconnaissance	Actividad indicativa de que alguien prueba o mapea la red para identificar una “oportunidad”, tales como puertos abiertos, algo que luego se podría convertir en un intento de acceso no autorizado.
	Misuse (mal uso)	Actividad indicativa de que alguien trata de violar la política corporativa de seguridad.
Firewall	Mecanismo de control de flujo entre redes, normalmente una protegida y otra no confiable.	

Dependencia de Servicios	Detalles Específico del Servicio	
	Arquitectura	ASIC (Application Specific Integrated Circuit)
	ACL	Creación de Listas de Control de Acceso
	Análisis	Inspección de paquetes en tiempo real
	NAT	Network Address Translation
	Otras:	Reporte automático de actividades, SNMP, VPN, prevención ataques DoS, Mail Relay y filtrado de URL.

TABLA D – III

SERVICIOS DE ALMACENAMIENTO DE INFORMACIÓN (MZ)

Dependencia de Servicios	Detalles Específico del Servicio	
Servidores de Aplicaciones	Cluster de balanceo de carga, para ejecutar el servidor J2EE. **Software.-** Oracle Application Server Enterprise Edition.	
	Hardware.- Plataforma Intel Itanium 2 / Linux AS	
	Cluster	(2) Nodos
	CPU	(2) Itanium 2 1.3 Ghz, 256 Kb Caché L2, 3 Mb. Caché L3.
	RAM	8 Gb / 16 Gb
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo, servidor de aplicación y aplicaciones implantadas.
Almacenamiento Externo Tipo NAS Filer	Dispositivo de almacenamiento conectado directamente a la red, para lectura / escritura de archivos, donde se instalará el almacenamiento de la solución colaborativa del Intranet. **Software.-** Soporte NFS, HTTP, FTP, CIFS; administración dinámica del almacenamiento, snapshot y snapclone.	
	CPU	(2) Xeon 2.4 Ghz; 512 Kb Caché L2
	RAM	6 Gb
	NIC	(2) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo.
	Capacidad de	1 Tb.

Dependencia de Servicios	Detalles Específico del Servicio	
	Almacenamiento Inicial	
	Capacidad de Almacenameinto Máximo	3 Tb.
Servicios de Gestión de Datos	Cluster Hot Failover para los servidores de base de datos. **Software.-** Oracle 9i DB Enterprise Edition con Oracle Real Application Cluster.	
	Hardware.- Plataforma Intel Itanium 2 / Linux AS	
	Cluster	2
	CPU	(2) Itanium 2 1.3 Ghz, 256 Kb Caché L2, 3 Mb. Caché L3
	RAM	8 Gb / 16 Gb.
	NIC	(2) 10 / 100 / 1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y motor de base de datos.
Servidor de Almacenamiento	Dispositivo de almacenamiento conectado a los servidores de base de datos a través de una red de almacenamiento externo basada en Fibra Canal, para lectura / escritura de bloques de datos. **Software.-** Software de gestión del almacenamiento, configuración de arreglo, control de acceso, replicación, snapshots, snapclones, expansión en línea y cambio del nivel de RAID.	
	Capacidad de almacenamiento real inicial instalada	0,5 Tb
	Capacidad de almacenamiento real máxima	6 Tb
	Controlador	Redundante, con ruta redudante.
	Memoria cache controlador	1 Gb
	Switches de conexión	2 (redundante)
Servicios de Respaldo	Servicios de Respaldo/Restauración de Información de alto desempeño para los distintos servidores del Data Center en todas sus Zonas, con características de respaldo automatizado para operación sobre base de datos en línea y archivos abiertos. **Software.-** Windows 2000 Server y HP OpenView Data Guard	
	CPU	(1) Xeon 2.4 Ghz; 512 Kb Caché L2

Dependencia de Servicios	Detalles Específico del Servicio	
	RAM	1 Gb
	NIC	(1) 10/100/1000 Mbps
	Fuente de Poder	Redundante
	HD	(2 x 36 Gb) Internos en RAID 1 para sistema operativo y aplicación de respaldo.
Unidad de Respaldo en Cinta	Unidad de alto rendimiento para respaldo y restauración de grandes volúmenes de datos de manera automática sin intervención de operadores, para múltiples servidores del Data Center. **Software.-** Gestor de respaldos y restauración con características de respaldo en línea de bases de datos y de archivos abiertos.	
	Drives	1 / 2
	Tecnología	LTO Ultrium 2
	Capacidad nativa	3 Tb
	Autoloader	Mínimo 8 cartuchos
	Desempeño	30 Mb/seg
	MCBF	> 250.000 horas
	MTBF	> 100.000 horas
Firewall	Mecanismo de control de flujo entre redes, normalmente una protegida y otra no confiable.	
	Arquitectura	ASIC (Application Specific Integrated Circuit)
	ACL	Creación de Listas de Control de Acceso
	Análisis	Inspección de paquetes en tiempo real
	NAT	Network Address Translation
	Otras:	Reporte automático de actividades, SNMP, VPN, prevención ataques DoS, Mail Relay y filtrado de URL.

APÉNDICE E

PLATAFORMA TECNOLÓGICA DE CONECTIVIDAD

A continuación se muestra el detalle de los equipos a emplearse, para la respectiva conectividad.

TABLA E - I

EQUIPOS DE RED PREVISTOS PARA EL DATA CENTER

Rol de Red	Detalles Específico de los Equipos	
Balanceo de Carga (Zona Desmilitarizada Pública y Zona Desmilitarizada Privada)	Switch capa 4-7.- Distribución de servicios basados en IP con balanceo de carga transparente entre múltiples servidores, monitoreando permanentemente los servidores, las aplicaciones y el contenido. Incluye las características de Server Load Balance (SLB) y Global Server Load Balance (GSLB).	
	Marca.- Foundry Networks.	
	Modelo.- ServerIron XL	
	Cantidad:	2
	Sesiones concurrentes:	1'000.000
	Throughput:	2 Gbps
	# IP Virtuales:	Ilimitado.
	# Puertos 10/100:	24
	# Puertos Gigabit:	2 (RJ45)
Servicio Conmutación Zona Militarizada	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs; alta velocidad de conmutación.	
	Marca.- Cisco	
	Modelo.- Catalyst 3550-12T	
	Cantidad:	1
	Throughput:	
	# Puertos Gigabit RJ45:	10
	# Puertos GBIC:	2 (RJ45)
	Sistema Operativo:	Enhanced Multilayer Software Image

Rol de Red	Detalles Específico de los Equipos	
Servicios Conmutación Zona Desmilitarizada Pública	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs.	
	Marca.- Cisco	
	Modelo.- Catalyst 3550-24G	
	Cantidad:	1
	Throughput:	
	# Puertos 10/100 RJ45:	24
	# Puertos GBIC:	2 (RJ45)
	Sistema Operativo:	Enhanced Multilayer Software Image
Servicios de Conmutación Zona Desmilitarizada Privada (Backbone de la Red Naval de Datos)	Servicios de conmutación con capacidad de administrar capa 3 y 4, VLANs y ACLs; Switch modular con versatilidad de interfaces y número de puertos; máquina avanzada procesadora de paquetes y agente RMON; alta velocidad de conmutación. Switch principal de la Red de Campus de la Base Naval Sur. Colapsa la red de fibra óptica monomodo de Campus, y la red de fibra óptica multimodo del edificio principal.	
	Marca.- Cisco	
	Modelo.- Catalyst 4506.	
	Procesador:	Supervisor IV (2 GE)
	Disco Flash Memory	64 Mb Sup III/IV
	Módulo FX 10/100:	24 puertos
	Módulo RJ45 10/100 + GBIC:	32 puertos + 2
	Módulo RJ45 Gigabit:	48 puertos
	Otras características: Fuente de poder redundante, Sistema Operativo Cisco IOS Enhanced L3 SW C4000 SUP 3/4 (OSPF, IGRP, EIGRP), Licencia Agente RMON.	
Servicios de Firewall de Borde	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento, capacidad FailOver Activo-Pasivo. Aceleración de hardware para túneles VPN; control de tráfico entre la Zona Internet y la Zona Privada.	
	Marca.- Cisco	
	Modelo.- PIX 515E (Principal y Fail Over)	
	Cantidad:	2
	# Zonas:	6 puertos 10/100 Mbps
	Throughput Firewall:	180 Mbps
	Throughput VPN:	140 Mbps
	# sesiones concurrentes:	130.000
Servicios de Firewall Interno	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y	

Rol de Red	Detalles Específico de los Equipos	
	desde la Zona Desmilitarizada Privada.	
	Marca.- Lucent Technologies	
	Modelo.- Brick VPN 200.	
	Cantidad:	1
	# Zonas:	4 puertos 10/100 Mbps
	Throughput Firewall:	190 Mbps
	Throughput VPN:	180 Mbps
	# Sesiones concurrentes:	200.000
Servicios de Firewall Interno Militarizado	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y desde la Zona Militarizada.	
	Marca.- Cisco	
	Modelo.- PIX 515E (DMZ)	
	Cantidad:	1
	# Zonas:	3 puertos 10/100 Mbps
	Throughput Firewall:	188 Mbps
	# Sesiones concurrentes:	130.000

TABLA E – II

EQUIPOS DE RED DE LA CAPA DE DISTRIBUCIÓN DE LA RED DE CAMPUS DE LA BASE NAVAL SUR

Capa de Red	Detalles Específico de los Equipos	
Backbone y Distribución de la Red de Campus de la Base Naval Sur	Servicios de conmutación con capacidad de administrar capa 3 y 4, VLANs y ACLs; Switch modular con versatilidad de interfaces y número de puertos; máquina avanzada procesadora de paquetes y agente RMON; alta velocidad de conmutación. Switch principal de la Red de Campus de la Base Naval Sur. Colapsa la red de fibra óptica monomodo de Campus, y la red de fibra óptica multimodo del edificio principal. Habilitación PVST.	
	Marca.- Cisco	
	Modelo.- Catalyst 4506.	
	Ubicación.- Edificio DIGMAT – CETEIG.	
	Procesador:	Supervisor IV (2 GE)
	Disco Flash Memory	64 Mb Sup III/IV

Capa de Red	Detalles Específico de los Equipos	
	Módulo FX 10/100:	24 puertos
	Módulo RJ45 10/100 + GBIC:	32 puertos + 2
	Módulo RJ45 Gigabit:	48 puertos
	Otras características: Fuente de poder redundante, Sistema Operativo Cisco IOS Enhanced L3 SW C4000 SUP 3/4 (OSPF, IGRP, EIGRP), Licencia Agente RMON.	
Distribución de la Red de Campus de la Base Naval Sur	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs. Habilitación PVST.	
	Marca.- Cisco	
	Modelo.- Catalyst 3550-24-FX	
	Ubicación.- Edificio CENABS.	
	# Puertos 10/100 FX:	24
	# Puertos GBIC:	2 Gigabit SMF
	Sistema Operativo:	Enhanced Multilayer Software Image
Distribución de la Red de Campus de la Base Naval Sur	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs. Habilitación PVST.	
	Marca.- Cisco	
	Modelo.- Catalyst 2912-FX.	
	Ubicación.- Edificio Talleres Integrados DIECAR	
	# Puertos 10/100 FX:	12
	# Puertos GBIC:	2 Gigabit SMF
	Sistema Operativo:	Enhanced Multilayer Software Image

TABLA E – III

EQUIPOS DE RED DE LA CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR SUR

Capa de Red	Detalles Específico de los Equipos	
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del CENABS a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio CENABS.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Escuela de Superficie a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24.	
	Ubicación.- Edificio ESDESU	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Hospital Naval a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24.	
	Ubicación.- Edificio HOSNAG	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Edificio de la Base Naval a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24.	
	Ubicación.- Edificio BASUIL	
	# Puertos 10/100 RJ45:	24

Capa de Red	Detalles Específico de los Equipos	
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Sanidad a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24.	
	Ubicación.- Edificio DIRSAN	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación para brindar acceso a la Red del INOCAR hacia la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-12.	
	Ubicación.- Edificio INOCAR	
	# Puertos 10/100 RJ45:	12
	Sistema Operativo:	Standard Software Image
	Accesorios:	Extensor de LAN por cable categoría 3; 10 Mbps hasta 1,3 Km. Marca RAD Modelo ASM-61
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación para brindar acceso a la Red del Club Naval hacia la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-12.	
	Ubicación.- Edificio Club Naval	
	# Puertos 10/100 RJ45:	12
	Sistema Operativo:	Standard Software Image
	Accesorios:	Extensor de LAN por cable categoría 3; 10 Mbps hasta 1,3 Km. Marca RAD Modelo ASM-61
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Sur	Servicios de conmutación para brindar acceso al Gate Principal hacia la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-12.	
	Ubicación.- Edificio Gate Principal – Oficina de Seguridad	
	# Puertos 10/100 RJ45:	12
	Sistema Operativo:	Standard Software Image
	Accesorios:	Extensor LAN cable categoría 3; 10 Mbps. Marca RAD Modelo ASM-61

TABLA E – IV

EQUIPOS DE RED DE LA CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR DEL ÁREA OPERATIVA

Capa de Red	Detalles Específico de los Equipos	
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de los Talleres Integrados de DIECAR a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio Talleres Integrados DIECAR.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Maestranza de DINNAV a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24.	
	Ubicación.- Edificio Maestranza	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Comandancia de Escuadra a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 1924C.	
	Ubicación.- Edificio CODESC	
	# Puertos 10 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Standard Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Escuadrón de Fragatas y Auxiliares a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 1912C.	
	Ubicación.- Edificio ESFRAM/ESCAUX	

Capa de Red	Detalles Específico de los Equipos	
	# Puertos 10 RJ45:	12
	# Puertos 100 FX:	2
	Sistema Operativo:	Standard Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Escuadrón de Lanchas Misileras y Escuadrón de Submarinos a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 1912C.	
	Ubicación.- Edificio ESCLAM/ESCSUB	
	# Puertos 10 RJ45:	12
	# Puertos 100 FX:	2
	Sistema Operativo:	Standard Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Escuadrón de Corbetas a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 1912C.	
	Ubicación.- Edificio ESCORB	
	# Puertos 10 RJ45:	12
	# Puertos 100 FX:	2
	Sistema Operativo:	Standard Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector del Área Operativa	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Centro de Transporte a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-12.	
	Ubicación.- Edificio CETRAN	
	# Puertos 10 RJ45:	12
	Sistema Operativo:	Standard Software Image

TABLA E – V

EQUIPOS DE RED DE LA CAPA DE ACCESO A LA RED DE CAMPUS DE LA BASE NAVAL SUR DESDE EL SECTOR NOROCCIDENTAL Y DEL EDIFICIO DE LA DIRECCIÓN GENERAL DEL PERSONAL

Capa de Red	**Detalles Específico de los Equipos**	
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Noroccidental	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Nivel III de DIECAR a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio Nivel III DIECAR.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Sector Noroccidental	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios del Comando de Guardacostas a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio COGUAR.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección General del Material a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950G-24	
	Ubicación.- Edificio DIGPER – 1er. Piso.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Administración Financiera a la Red de Campus.	
	Marca.- Cisco	

Capa de Red	Detalles Específico de los Equipos	
	Modelo.- Catalyst 2924-XL	
	Cantidad: 2	
	Ubicación.- Edificio DIGPER – 1er. Piso.	
	# Puertos 10/100 RJ45:	22
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Investigación y Desarrollo a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio DIGPER – 2do. Piso.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Electrónica, Comunicaciones y Armamento a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2924-XL	
	Ubicación.- Edificio DIGPER – 3er. Piso.	
	# Puertos 10/100 RJ45:	22
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Ingeniería Naval a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio DIGPER – 3er. Piso.	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Abastecimientos a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950C-24	
	Ubicación.- Edificio DIGPER – 4to. Piso.	

Capa de Red	Detalles Específico de los Equipos	
	# Puertos 10/100 RJ45:	24
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección de Abastecimientos a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2924-XL	
	Ubicación.- Edificio DIGPER – 4to. Piso.	
	# Puertos 10/100 RJ45:	22
	# Puertos 100 FX:	2
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Base Naval Sur desde el Edificio DIGPER	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de la Dirección General del Personal a la Red de Campus.	
	Marca.- Cisco	
	Modelo.- Catalyst 2912-FX	
	Ubicación.- Edificio DIGPER – 5to. Piso.	
	# Puertos 100 FX:	12
	Sistema Operativo:	Enhanced Multilayer Software Image

TABLA E – X

EQUIPOS PARA LA RED DE CAMPUS DE LA COMANDANCIA GENERAL DE MARINA Y ACCESO A LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos	
Backbone y Distribución de la Red de Campus de la Comandancia General de Marina	Servicios de conmutación con capacidad de administrar capa 3, VLANs y ACLs; switch principal de la Red de Campus de la Comandancia General de Marina.	
	Marca.- Cisco	
	Modelo.- Catalyst 3550-24-EMI.	
	Ubicación.- Edificio ESNAQUI – CETEIQ.	
	# Puertos 10/100 RJ45:	24 puertos.
	# Puertos GBIC:	2 Gigabit sobre cobre.

Capa de Red	Detalles Específico de los Equipos	
	Sistema Operativo:	Enhanced Multilayer Software Image
Distribución de la Red de Campus de la Comandancia General de Marina	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs; para proveer acceso a los usuarios de la Dirección General de Finanzas	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-48-EI	
	Ubicación.- Edificio DIGFIN.	
	# Puertos 10/100 RJ45:	48
	# Puertos GBIC:	2 Gigabit sobre cobre
	Sistema Operativo:	Enhanced Multilayer Software Image
Distribución de la Red de Campus de la Comandancia General de Marina	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs para proveer acceso a los usuarios de la Estación Naval de Quito.	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-48-EI	
	Ubicación.- Edificio ESNAQUI	
	# Puertos 10/100 RJ45:	48
	# Puertos GBIC:	2 Gigabit sobre cobre
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso de la Red de Campus de la Comandancia General de Marina al Data Center	Servicios de conmutación con capacidad de soportar capa 3, VLANs y ACLs, alto desempeño; para proveer acceso a los servidores.	
	Marca.- Cisco	
	Modelo.- Catalyst 3550-12T	
	Ubicación.- Edificio ESNAQUI – CETEIQ	
	# Puertos 10/100/1000 RJ45:	10
	# Puertos GBIC:	2 Gigabit sobre cobre
	Sistema Operativo:	Enhanced Multilayer Software Image
Acceso a la Red de Campus de la Comandancia General de Marina	Servicios de conmutación con capacidad de soportar VLANs y ACLs; para distribución a usuarios de los diferentes repartos ubicados en la Comandancia General de Marina (DIRINT, AUDQUI, ESMAAR)	
	Marca.- Cisco	
	Modelo.- Catalyst 2924-XL	
	Cantidad: 3	

Capa de Red	Detalles Específico de los Equipos	
	Ubicación.- Edificio COGMAR	
	# Puertos 10/100 RJ45:	22
	# Puertos 100 FX:	2
	Sistema Operativo:	Standard Software Image
Servicios de Firewall Interno DMZ Privada	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y desde la Zona Desmilitarizada Privada de Quito.	
	Marca.- Cisco	
	Modelo.- PIX 515E (DMZ)	
	Cantidad:	1
	# Zonas:	3 puertos 10/100 Mbps
	Throughput Firewall:	188 Mbps
	# Sesiones concurrentes:	130.000

TABLA E – VII

EQUIPOS PARA LA RED DE CAMPUS DE LA BASE NAVAL NORTE Y ACCESO A INTERNET Y A LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos
Acceso a la Red de Campus de la Base Naval Norte desde los diferentes repartos	Extensores de redes de área local por cable de cobre categoría 3, soporte a VLANs.
	Marca.- RAD
	Modelo.- ASM-61
	Cantidad: 16 equipos
	Ubicación.- Edificios: Dirección de Educación, Academia de Guerra Naval, Edificio Comando de la Base Naval Norte, Liceo Naval Sección Secundaria, Liceo Naval Sección Primaria, Escuela de Marina Mercante, Gate Principal/Gasolinera, y Asociación Deportiva Naval. * El Centro Tecnológico Naval se encuentra en red con la sala de radio.
Distribución de Servicios a la Red de Campus de la Base Naval Norte	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de los diferentes repartos navales ubicados en la Base Naval Norte.

Capa de Red	Detalles Específico de los Equipos	
	Marca.- Cisco	
	Modelo.- Catalyst 2950-12	
	Ubicación.- Sala de Radio Base Naval Norte.	
	# Puertos 10/100 RJ45:	12
	Sistema Operativo:	Standard Software Image
Servicios de Firewall Interno DMZ Privada	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y desde la Zona Internet, la Red de Campus de BASNOR y la Red Naval de Datos.	
	Marca.- Cisco	
	Modelo.- PIX 515E (DMZ)	
	Cantidad:	1
	# Zonas:	3 puertos 10/100 Mbps
	Throughput Firewall:	188 Mbps
	# Sesiones concurrentes:	130.000

TABLA E – VIII

EQUIPOS PARA LA RED DE CAMPUS DE LA BASE NAVAL DE SALINAS Y ACCESO A INTERNET Y A LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos
Acceso a la Red de Campus de la Base Naval de Salinas desde los diferentes repartos	Extensores de redes de área local por cable de cobre categoría 3, soporte a VLANs.
	Marca.- RAD
	Modelo.- ASM-61
	Cantidad: 4 equipos
	Ubicación.- Edificios: Gate Principal, Hotel Naval. * La Escuela Superior Naval y la Escuela de Grumetes están enlazadas con la Sala de Radio a través de fibra óptica.
Distribución de Servicios a la Red de Campus de la Base Naval de Salinas	Servicios de conmutación con capacidad de soportar VLANs y ACLs, para brindar acceso a los usuarios de los diferentes repartos navales ubicados en la Base Naval de Salinas.
	Marca.- Cisco
	Modelo.- Catalyst 2950-12
	Ubicación.- Sala de Radio Base Naval de Salinas.

Capa de Red	Detalles Específico de los Equipos	
	# Puertos 10/100 RJ45:	12
	Sistema Operativo:	Standard Software Image
Servicios de Firewall Interno DMZ Privada	Firewall basado en inspección statefull de paquetes, alta capacidad de procesamiento. Para control de tráfico de paquetes hacia y desde la Zona Internet, la Red de Campus de BASALI y la Red Naval de Datos.	
	Marca.- Cisco	
	Modelo.- PIX 515E (DMZ)	
	Cantidad:	1
	# Zonas:	3 puertos 10/100 Mbps
	Throughput Firewall:	188 Mbps
	# Sesiones concurrentes:	130.000

TABLA E – IX

EQUIPOS PARA LA RED DE ÁREA EXTENDIDA PARA REPARTOS CON ENLACES DEDICADOS ISDN PARA ACCESO A LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos	
Acceso a la Red de Área Extendida de la Red Naval de Datos con Enlaces ISDN	Ruteadores IP con soporte a ACLs, para acceso de la Aviación Naval y la Base Naval de Jaramijó.	
	Marca.- Cisco	
	Modelo.- 1751	
	Cantidad: 2 equipos	
	Ubicación.- Edificios: Aviación Naval y Base Naval de Jaramijó.	
	Interfaces LAN:	1 – 10/100 Mbps
	Interfaces WAN:	3 Seriales (1 ISDN)
	Sistema Operativo:	Cisco 1700 Series IOS IP/FW/IDS PLUS IPSEC 3DES
	Accesorios:	1 TA con tarjeta S0 Alcatel. 2 Extensores de línea de cobre RAD ASM-31 para AVINAV.
Acceso a la Red de Área Extendida de la Red Naval de	Ruteadores IP con soporte a ACLs, para acceso de la Red de Campus de la Base Naval de Salinas y la Red de Campus de la	

Capa de Red	Detalles Específico de los Equipos	
Datos con Enlaces ISDN	Base Naval Norte.	
	Marca.- Cisco	
	Modelo.- 801 ISDN Router	
	Cantidad: 2 equipos	
	Ubicación.- Sala de Radio Base Naval de Salinas y Sala de Radio Base Naval Norte.	
	Interfaces LAN:	1 – 10 Mbps
	Interfaces WAN:	1 ISDN
	Sistema Operativo:	Cisco 800 Series IOS IP/FW PLUS IPSEC 3DES
	Accesorios:	1 TA con tarjeta S0 Alcatel

TABLA E – X

EQUIPOS PARA LA RED DE ÁREA EXTENDIDA PARA REPARTOS CON ENLACES SERIALES POR EL SISTEMA MULTIACCESO A LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos	
Acceso a la Red de Área Extendida de la Red Naval de Datos con Enlaces Seriales vía sistema multiacceso	Ruteadores IP con soporte a ACLs, para acceso del Comando de Operaciones Navales, la Inspectoría General de la Armada, la Dirección de Bienestar, el Cuerpo de Infantería de Marina, el Comando de Operaciones Norte y la Capitanía de Puerto de Esmeraldas.	
	Marca.- Cisco	
	Modelo.- 1751	
	Cantidad: 3 equipos	
	Ubicación.- Edificios: COOPNA – Sala de Radio, CUINMA – Sala de Radio, y COOPNO.	
	Interfaces LAN:	1 – 10/100 Mbps
	Interfaces WAN:	3 Seriales
	Sistema Operativo:	Cisco 1700 Series IOS IP/FW/IDS PLUS IPSEC 3DES

Capa de Red	Detalles Específico de los Equipos	
	Accesorios:	1 Convertidor de Interface RAD ASM-31
Acceso a la Red de Área Extendida de la Red Naval de Datos con Enlaces Seriales vía sistema multiacceso	Ruteadores IP con soporte a ACLs, para acceso de la Dirección General de Marina Mercante, la Dirección de Empresas de la Armada y el Instituto de Historia Marítima.	
	Marca.- Cisco	
	Modelo.- 1721	
	Cantidad: 1 equipos	
	Ubicación.- Sala de Radio Dirección General de Marina Mercante.	
	Interfaces LAN:	1 – 10/100 Mbps
	Interfaces WAN:	2 Seriales
	Sistema Operativo:	Cisco 1700 Series IOS IP/FW/IDS PLUS IPSEC 3DES
	Accesorios:	1 Convertidor de Interface RAD ASM-31
		4 Extensores de LAN por cable categoría 3; 10 Mbps hasta 1,3 Km. Marca RAD Modelo ASM-61
Acceso a la Red de Área Extendida de la Red Naval de Datos con Enlaces Seriales vía sistema multiacceso	Ruteadores IP con soporte a ACLs, para acceso de la Dirección General de Intereses Marítimos, el Batallón de Infantería de Marina de Esmeraldas, la Compañía de Infantería de Marina de San Lorenzo y la Compañía de Infantería de Marina de Jambelí.	
	Marca.- Cisco	
	Modelo.- 803 Serial Router	
	Cantidad: 4 equipos	
	Ubicación.- Edificios: DIGEIM, BIMESM, BIMLOR y CICJAM.	
	Interfaces LAN:	1 – 10 Mbps
	Interfaces WAN:	1 Serial
	Sistema Operativo:	Cisco 800 Series IOS IP/FW PLUS IPSEC 3DES
	Accesorios:	1 Convertidor de Interface RAD ASM-31

TABLA E – XI

EQUIPOS PARA LA INTERCONEXIÓN DE QUITO – GUAYAQUIL A TRAVÉS DEL ENLACE E1 EN LA RED NAVAL DE DATOS

Capa de Red	Detalles Específico de los Equipos	
Red de Área Extendida de la Red Naval de Datos	Ruteadores IP con soporte a ACLs, para interconexión del CETEIQ con el CETEIG.	
	Marca.- Cisco	
	Modelo.- 2620 Modular Router	
	Cantidad: 1 equipo	
	Ubicación.- Edificio ESNAQUI – CETEIQ.	
	Interfaces LAN:	1 – 10/100 Mbps
	Interfaces WAN:	1 Slot con módulo VWIC (E1)
	Sistema Operativo:	Cisco 2600 Series IOS IP/FW/IDS PLUS IPSEC 3DES
	Accesorios:	2 Modems de Fibra Óptica MMF RAD FOM-E1, 1 Adaptador BNC RAD RIC.
Red de Área Extendida de la Red Naval de Datos	Ruteadores Modular Multiservicio IP con soporte a ACLs, para acceso al nodo principal en el CETEIG.	
	Marca.- Cisco	
	Modelo.- 3745 Multiservice Router	
	Cantidad: 1 equipo	
	Ubicación.- Edificio DIGPER – CETEIG.	
	Interfaces LAN:	2 – 10/100 Mbps
	Módulos:	1 Slot con módulo de red (4) puertos ISDN BRI
		1 Slot con módulo de red (4) puertos seriales de baja velocidad
		1 Slot con módulo acelerador de contenido: Content Engine 3745 (40 Gb)
		1 Slot con módulo de detección de intrusos (IDS)
		1 Módulo AIM Acelerador VPN DES/3DES
	Sistema Operativo:	Cisco 3745 Series IOS ENTERPRISE IP/FW/IDS PLUS IPSEC 3DES
	Accesorios:	2 Modems de Fibra Óptica MMF RAD FOM-E1, 1 Adaptador BNC RAD RIC. Fuente de poder redundante.

APÉNDICE F

SEGURIDAD DE REDES

1. Control de Servicios del Sistema Operativo Linux

- ✓ **systat.-** Asociado al puerto 11 en TCP, permite mostrar una imagen de la tabla de procesos del sistema. Debe estar cerrado puesto que cualquier información relacionada con procesos, nombres de usuario, máquinas desde donde se conectan, puede ser aprovechada por un hacker mal intencionado. Si es necesario administrar varios servidores desde una sola posición, se puede habilitar systat con restricciones desde las direcciones que se puede acceder al servicio a través de TCP Wrappers.

- ✓ **daytime.-** Asociado al puerto 13 en TCP y UDP, permite mostrar la fecha-hora del sistema. Por no ser un servicio estrictamente necesario debe mantenerse cerrado. A un atacante le puede dar una idea geográfica de la ubicación del servidor. Un servicio parecido es **time** que funciona en el puerto 37 (TCP y UDP), pero su salida no es legible por el hombre.

- ✓ **netstat.-** Ofrece información de estado de la red. Está asociado al puerto 15 en TCP y muestra principalmente las conexiones activas

en las máquinas. Se puede deshabilitar el servicio comentando la línea correspondiente de /etc/inetd.conf; o restringiendo el acceso desde direcciones específicas mediante TCP Wrappers. Un atacante puede obtener nombres de máquinas e interpretar una idea del tráfico que soporta una máquina, los servicios que ofrece y de los hábitos de conexión de los usuarios.

- ✓ **chargen.-** Asociado al puerto 19 (TCP y UDP) es un servidor de caracteres utilizado para comprobar el estado de las conexiones de red. Los problemas de seguridad asociados son la negación de servicio.

- ✓ **tftp (trivial file transfer protocol).-** Asociado al puerto 69 en UDP que no proporciona ninguna seguridad. Su uso principal es el arranque de estaciones sin disco, y actualmente de ruteadores a través de la red. Muchos sistemas que se instalan tal como vienen habilitan este servicio por defecto, el mismo que no emplea ningún esquema de autenticación por lo cual es totalmente inseguro.

- ✓ **finger.-** Asociado al puerto 79 (TCP) es una de las principales fuentes de problemas de Unix. Proporciona información demasiado detallada de los usuarios de una máquina, estén o no conectados al momento de acceder al servicio. Proporciona información detallada

del usuario: nombre, hábitos de conexión, cuentas inactivas, etc.. esto puede ser aprovechado fácilmente por un hacker para realizar ingeniería social. Es básico su deshabilitación.

- ✓ **POP (Post Office Protocol).**- Asociado a los puertos 109 y 110 en TCP se utiliza para que los usuarios puedan acceder al correo electrónico. El correo electrónico utiliza el servicio SMTP para enviar correo y POP para recogerlo. Es un servicio que se puede considerar peligroso por lo que si no se trata de un servidor de correo electrónico, deberíamos deshabilitarlo. Algunos demonios de POP tienen defectos que incluso pueden otorgar privilegios de root sin necesidad de conocer la clave. Incluso en un servidor de correo electrónico este servicio se puede convertir en un problema. POP ofrece tres esquemas de autenticación: uno basado en *Kerberos*, poco utilizado; otro basado en protocolo de desafío respuesta (APOP) que tampoco se lo emplea mucho, y otro basado en un simple nombre de usuario y contraseña correspondiente, siendo éste último el más empleado. Un servidor POP es un blanco excelente para un hacker a través de un sniffer para obtener contraseñas, ya que la mayoría de usuarios suelen configurar a sus clientes de mail (Outlook) para que cada cierto tiempo verifiquen nuevo correo electrónico, con lo que cada cierto tiempo envían su

clave a un puerto conocido de una máquina conocida, todo esto sucede en claro, por lo que el atacante solo tiene que interceptar la sesión POP para averiguar nombres y claves (violando en el mejor de los casos la privacidad). Se puede utilizar otro de los esquemas de autenticación para evitar éste inconveniente.

- ✓ **auth.-** Asociado al puerto 113 en TCP, sirve para resolver el usuario que está empleando un determinado socket. Para ello envía al demonio **identd** los datos que distinguen una conexión (los componentes de dirección de máquina y puerto de los dos sockets que intervienen), el demonio identifica al usuario en cuestión y devuelve información sobre dicho usuario, normalmente el *login.* Este servicio no se debe utilizar con propósitos de autenticación robusta, ya que no dependemos de nuestros sistemas sino de la honestidad de la máquina remota. Si es necesario utilizar el servicio para detectar violaciones de seguridad, se debe limitar su uso mediante TCP Wrappers.

- ✓ **NNTP (Network News Transfer Protocol).**- Asociado al puerto 119 en TCP se utiliza para intercambiar mensajes de grupos de noticias entre servidores de *news.* Los problemas de seguridad suelen estar asociados más bien a la falsificación de identidad. Un atacante

puede enviar mensajes con contenido cuestionable utilizando nuestro nombre y nuestros recursos. Un atacante también puede tener acceso a discusiones habilitadas por el servicio de *news* de manera privada enterándose de aspectos internos. Normalmente no se dispone de éste tipo de servicios, y si se lo requiere se emplea uno en toda la organización que puede ser protegido con servicios de firewall.

- ✓ **NTP (Network Time Protocol).-** Asociado al puerto 123 en TCP y UDP es un protocolo utilizado para sincronizar relojes de máquinas en forma precisa. Los problemas asociados al tiempo correcto pueden ser pricipalmente los relacionados a la fiabilidad de los registros de auditoría o *logs* de nuestros sistemas. Otro inconveniente resultante de la manipulación de la hora de un servidor es la alteración de la calendarización de procesos programados. Es conveniente tenerlo deshabilitado y emplear el reloj de sistema de cada máquina con una buena administración.

- ✓ **UUCP (Unix to Unix CoPy).**- Asociado al puerto 540 TCP se utilize para copier archivos entre máquinas Unix a través de redes de baja velocidad. Hoy en día es poco utilizado y por tanto conveniente deshabilitar.

- ✓ **FTP.**- Asociado al puerto 21 TCP es un protocolo de transferencia de archivos. Es un protocolo diseñado para ofrecer la más alta velocidad de transmisión, pero no seguridad. Todo el intercambio, incluido el usuario y contraseña, se transmite en claro. Para evitar riesgos es preferible concientizar el uso de protocolos incluidos en aplicaciones SSH como SCP y SFTP, donde toda la transmisión es encriptada. Bajo las restricciones de seguridad de la Red Naval de Datos, no es necesario considerar un servicio FTP anónimo.

- ✓ **telnet.-** Asociado al puerto 23 TCP, permite utilizar una máquina como terminal virtual de otra, creando un canal virtual sin seguridad ya que funciona en modo texto. Es un servicio que no es fácil deshabilitar puesto que muchos usuarios (especialmente administrativos) requieren tener acceso a las máquinas Unix, por lo cual es necesario utilizar otras aplicaciones equivalentes como SSH, y deshabilitar el servicio telnet. Además como medida complementaria, es necesario asegurarse estar empleando una versión del demonio actualizada, puesto que en muchos existen bastantes defectos normalmente empleados por los atacantes.

- ✓ **SMTP (Simple Mail Transfer Protocol).**- Asociado al puerto 25 en TCP se utiliza para transferir correo electrónico entre equipos

remotos. Este servicio es atendido por el demonio sendmail, un programa lleno de defectos y problemas. Una medida básica recomendada para mitigar los riesgos, es que existe la posibilidad de servir a sendmail desde inetd en vez de hacerlo como demonio independiente, y por tanto restringir el acceso a través de TCP Wrappers. Además como en la mayoría de organizaciones existe un servidor de correo principal que es el encargado de recoger el mail para todas las direcciones (Ej: *@*.armada.mil.ec); el resto de equipos solamente recibirán correo electrónico desde éste equipo, siendo factible establecer reglas básicas que mejoran la seguridad. Para esto hay que modificar el *script* correspondiente para que sendmail no se lance como demonio de arranque, y además identificar el servicio en /etc/services; tras reconocer el servicio hay que añadir una línea en /etc/inetd.conf indicando como se ha de ejecutar sendmail cuando inetd reciba una petición en el puerto 25; una vez realizados estos cambios podemos controlar el acceso a nuestro servicio SMTP mediante TCP Wrappers.

- ✓ **Servidores WWW.**- Es el servicio de uso más extendido en el Internet, asociado al puerto 80 en TCP. Utiliza el protocolo http. Los problemas de seguridad asociados a éste protocolo se dividen en tres grupos en función a los datos que pueden afectar:

- **Seguridad en el servidor.**- Es necesario garantizar que la información almacenada en el servidor no se pueda modificar sin autorización, que permanezca disponible y que solo pueda ser accedida por los usuarios a los que les esté legítimamente permitido (de manera total o parcial).

- **Seguridad en la red.**- Cuando un usuario se conecta a un servidor web, se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente son los mismos que ha enviado el servidor evitando que sufran modificaciones por terceros, y también que la información que el usuario envía hacia el servidor no sea capturada, destruida o modificada por el atacante. Esto es vital especialmente si la información en tránsito es sensible como el caso de contraseñas, o números de tarjetas de crédito.

- **Seguridad en el cliente.-** Es necesario garantizar al usuario que lo que descarga de un servidor no va a perjudicar a la seguridad de su equipo; no solo consideraremos applets maliciosos o virus, sino también

que el navegador del usuario no se cuelgue al acceder a las páginas servidas por nuestro servidor. Siempre será recomendable que la máqu servidor web, sea una máquina dedicada. En lo posible se debe restringir el empleo de CGIs por considerar que se han propuesto mejores opciones en éste trabajo.

Violaciones a la seguridad en las redes

Existen tres tipos de ataques a una red:

- ✓ **Ataques de reconocimiento.-** Un intruso trata de descubrir sistemas, servicios y puntos débiles en la red. También se lo denomina **recopilación de información**, y la mayoría de veces precede a un acceso real o a un ataque de negación de servicio (DoS). Una de las técnicas utilizadas son los barrido de pings para determinar primero las IP activas, luego tratar de determinar los servicios o puertos activos, luego tratar de determinar el tipo y versión de aplicación que se ejecuta en el host, así como también el tipo y versión del sistema operativo, para luego tratar de descubrir sus vulnerabilidades (exploits).

- ✓ **Ataques de acceso.**- Hace referencia a la capacidad que tiene un origen concreto de conectarse a un destino concreto. Una vez precisado el destino, el atacante tratará de usar alguna aplicación de software para llegar a él. Puede representar en recuperación y manipulación no autorizada de datos, acceso a un sistema e incremento de privilegios de acceso. Se suele emplear también para instalar y ocultar software para que los hackers los utilicen con posterioridad.

- ✓ **Ataques de negación de servicio.**- Tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para negar el servicio a los usuarios. Implica que el sistema colapsa dejándolo inutilizable. Tan solo basta la ejecución de un script o una herramienta, no se necesita tener acceso al destino, sino sólo una ruta a éste. Dado que es muy fácil de iniciar y se puede realizar de manera anónima, es el ataque más temido en el Internet. Un ataque de negación de servicio distribuida (DDoS) es aquel que el origen del ataque proviene de muchas computadoras (generalmente diseminadas en un área geográfica muy amplia), haciendo que sea complicado localizar y detener el origen.

Conforme a las normas de seguridad de redes, debemos aplicar los cuatro pasos del ciclo de seguridad:

Paso 1 – Asegurar

Implementación de dispositivos y/o sistemas de seguridad con el fin de impedir el acceso no autorizado a los sistemas de red:

a) **Los sistemas de autenticación de la identificación,** como las contraseñas únicas, proporcionan acceso a los usuarios autenticados y autorizados. Algunos ejemplos de éste tipo de sistemas son el servidor de control de acceso de Cisco Secure (CSACS), CryptoCard y SecurID.

b) El **cifrado** puede disfrazar el tráfico, lo que impide la revelación no deseado a usuarios no autorizados o fraudulentos. Así se puede garantizar la confidencialidad del tráfico de los datos. La seguridad IP (IPSec) es el cifrado estándar que se usa en Internet.

c) Los **firewall** pueden permitir y denegar datos concretos para autorizar únciamente el tráfico y los servicios válidos.

d) La **reparación de puntos débiles** es el acto de colocar parches o tomar medidas que detengan la explotación de los puntos débiles

conocidos. Esto incluye la desactivación de servicios no necesarios en todos los sistemas, cuanto menos servicios estén activados, más difícil será que los hackers tengan acceso.

e) La **seguridad física** es un aspecto importantísimo de la protección. Si alguien puede apropiarse del hardware del sistema, el resto de las medidas pierden totalmente el sentido. Es necesario también proteger la instalación no autorizada de dispositivos promiscuos que puedieran apropiarse de datos importantes.

Paso 2 – Supervisar

Supervisar la red para evitar las violaciones y los ataques contra las normas de seguridad establecidas. Las violaciones pueden ser producidas en el perímetro protegido por un empleado o desde el exterior por un hacker. Un sistema de detección de intrusos en tiempo real, como el Intruction Detection System de Cisco Secure, puede detectar y evitar las entradas no autorizadas. El IDS puede garantizar que los dispositivos de seguridad del paso 1 han sido configurados correctamente. El registro es un aspecto importante del control. El seguimiento del tráfico de datos que fluye por una red puede ser la diferencia entre la detección de un ataque y la adopción de medidas

antes de que se convierta en un problema, y la no detección del mismo y dejar que éste inutilice la red.

Paso 3 – Probar

Probar la efectividad de las medidas de protección. La validación es una necesidad. Posiblemente se tenga un sistema de seguridad de red muy sofisticado, pero si no está configurado correctamente, la red podría verse afectada. Una herramienta que se puede usar para identificar la seguridad de la red es Cisco Secure Scanner.

Paso 4 – Mejorar

El mejoramiento continuo de las normas de seguridad es fundamental puesto que las amenazas no son estáticas. Reúna y analice la información procedente de las fases de control y prueba para realizar las mejoras en los mecanismos de seguridad.

En la Figura D.1 se muestran los cuatro pasos del ciclo de la seguridad de las redes:

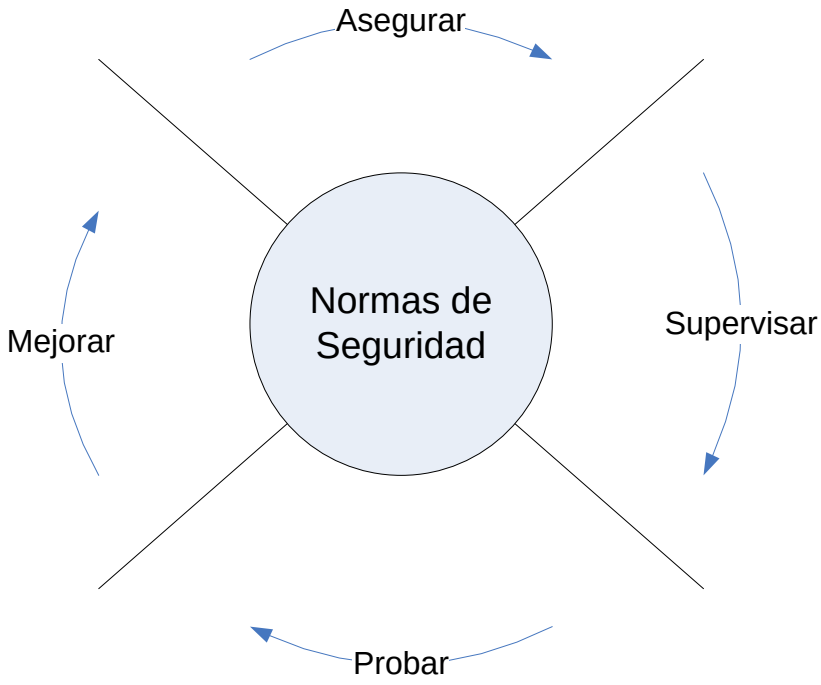


FIGURA No. D.1 CICLO DE SEGURIDAD DE REDES

APÉNDICE G

PROCEDIMIENTOS PARA ADMINISTRACION DE INTRANET-INTERNET EN INOCAR

1. CREACION DE INFORMACION

a) Se genera un requerimiento de presentación de información por parte del Jefe Departamental, usuario(s) de un determinado departamento o división.
b) El o los usuarios encargados de la información, recopilan la información que desean presentar en el sitio web INOCAR.
c) Realizan un bosquejo de cómo desean que se presente la información: datos o información que se presentarán, gráficos, imágenes o animaciones.
d) El encargado de presentar la información se reúne con el Jefe Departamental para presentar su bosquejo y pedir la aprobación para presentación de la información.
e) Se genera un pedido de creación de página por parte del usuario, el mismo que deberá llevar la firma del Jefe Departamental autorizando la presentación de esta información en el sitio web.
f) El webmaster recibe el oficio generado por el usuario y autorizado por el Jefe Departamental y se coordina una reunión con el usuario.
g) Se sostiene una reunión entre el webmaster y el (los) usuario(s), para definir el tipo y el tamaño de la información, así como la(s) imagen(es) que se van a presentar, vínculos que contendrá la página, dándole al

usuario un tamaño predefinido de la imágenes para que aplique esto en su bosquejo.

h) Se define la frecuencia con que se recibirán las actualizaciones por parte del encargado.
i) Se define junto con el usuario en que directorio del sitio web se creará la(s) nueva(s) página(s).
j) En caso de ser un usuario nuevo del grupo de Webmasters, el webmaster creará una carpeta en el directorio webINO, del servidor de archivos (Srv-archivos) de CENDO, otorgándole los permisos totales a esta nueva carpeta.
k) Esta carpeta se identificará por la división que genera la información o el usuario que realizará la actualización de la misma. Por ejemplo:
   - ✓ TSUNAMIS: identifica a la carpeta para información de la división Tsunamis.
   - ✓ JREGALADO: identifica que la carpeta es asignada al usuario Juan Regalado de la división de Climatología.
l) Se define con el encargado de la actualización, la asignación de un alterno y además de un subalterno, para que en caso de faltar el principal, nunca exista una desactualización de la información presentada.
m) El usuario se encarga de colocar la información en su carpeta dentro del directorio webINO, para que el webmaster proceda a realizar su trabajo.
n) Al momento de crear la página web, el usuario deberá enviar solo por esta ocasión al webmaster, su información en formato word, hasta que se le instale el programa Dreamwaver para la actualización de la información.
o) Una vez definida el tipo de información, imágenes a presentar, el webmaster crea una presentación preliminar la página (formato html o php), dejándose a libertad del mismo, la utilización de colores, estilos,

fuentes, fondos de pantalla, nombre de la página, etc., según él crea conveniente para la mejor visualización de la información y sin que se aparte del formato existente en el sitio web.

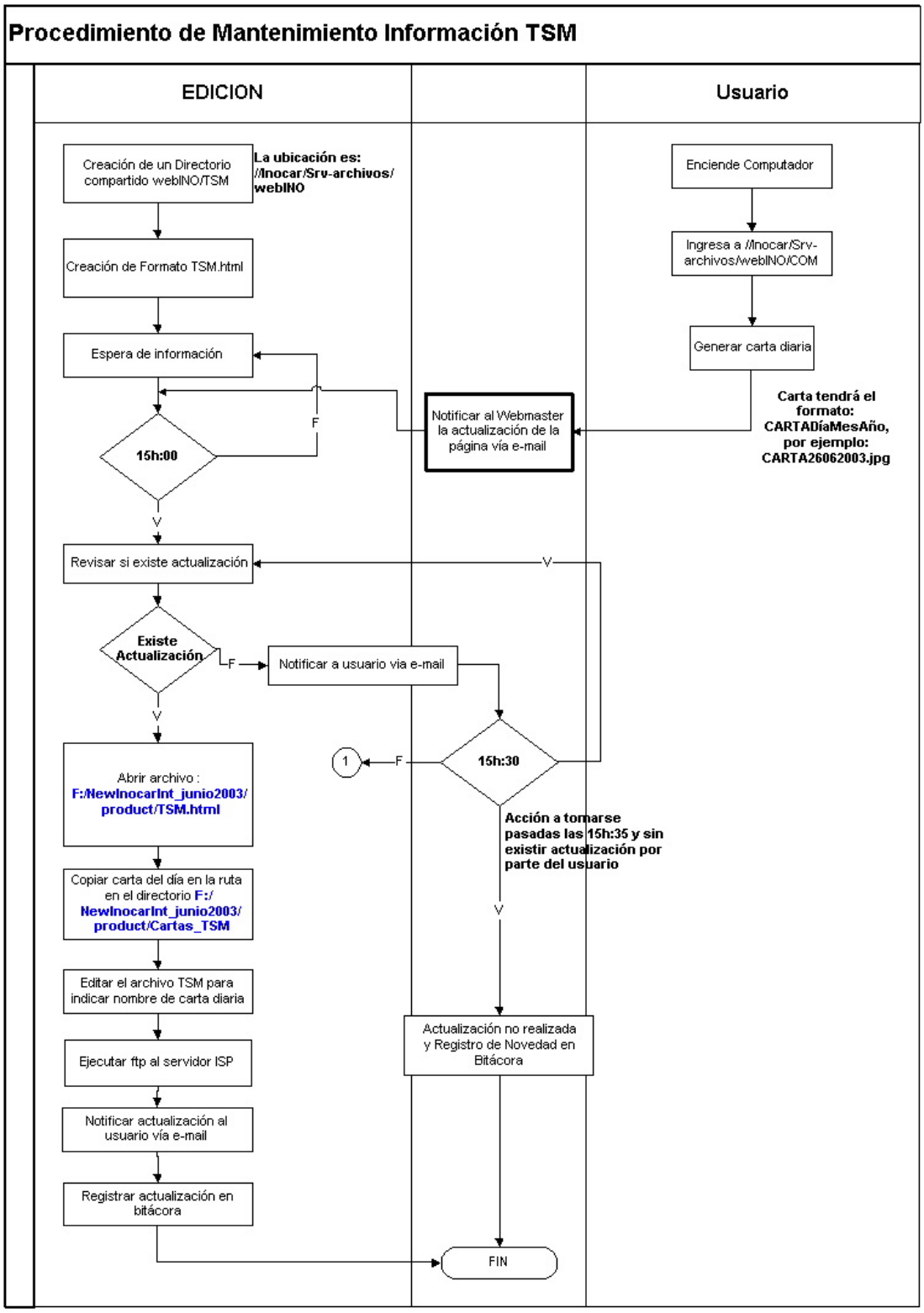
p) El webmaster procede a actualizar esta información en el directorio ya definido en el sitio web, para la visualización preliminar y sugerencias por parte del usuario.
q) Una vez que la presentación preliminar fue aprobada por el usuario, se procede a realizar una demostración de la misma al Jefe Departamental, el mismo que dará la aprobación final para su publicación en la web.
r) En caso de existir sugerencias por parte del usuario o Jefe de Departamento, estos comunicarán al webmaster, el cual procederá a realizar las correcciones o mejoras solicitadas.
s) Una vez realizadas las mejoras y/o correcciones solicitadas y teniendo la aprobación correspondiente, se procede a la publicación de esta página en el sitio web Inocar.
t) La página web creada por el webmaster, pasará a ser el formato o plantilla en el cual el usuario procederá a actualizar su información.
u) El webmaster anotará el trabajo realizado, así como las modificaciones realizadas en bitácora.

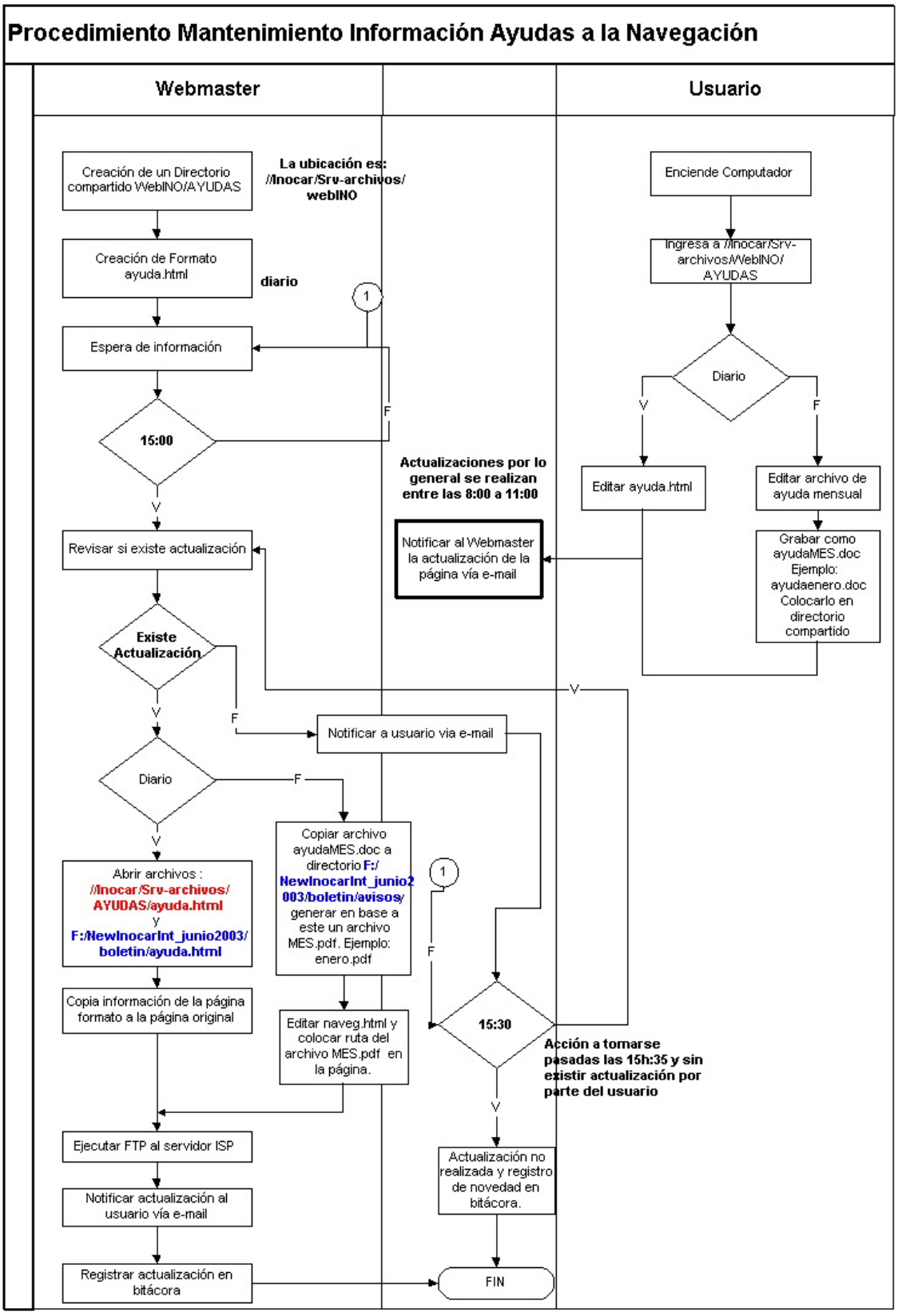
2. ACTUALIZACIÓN DE INFORMACIÓN

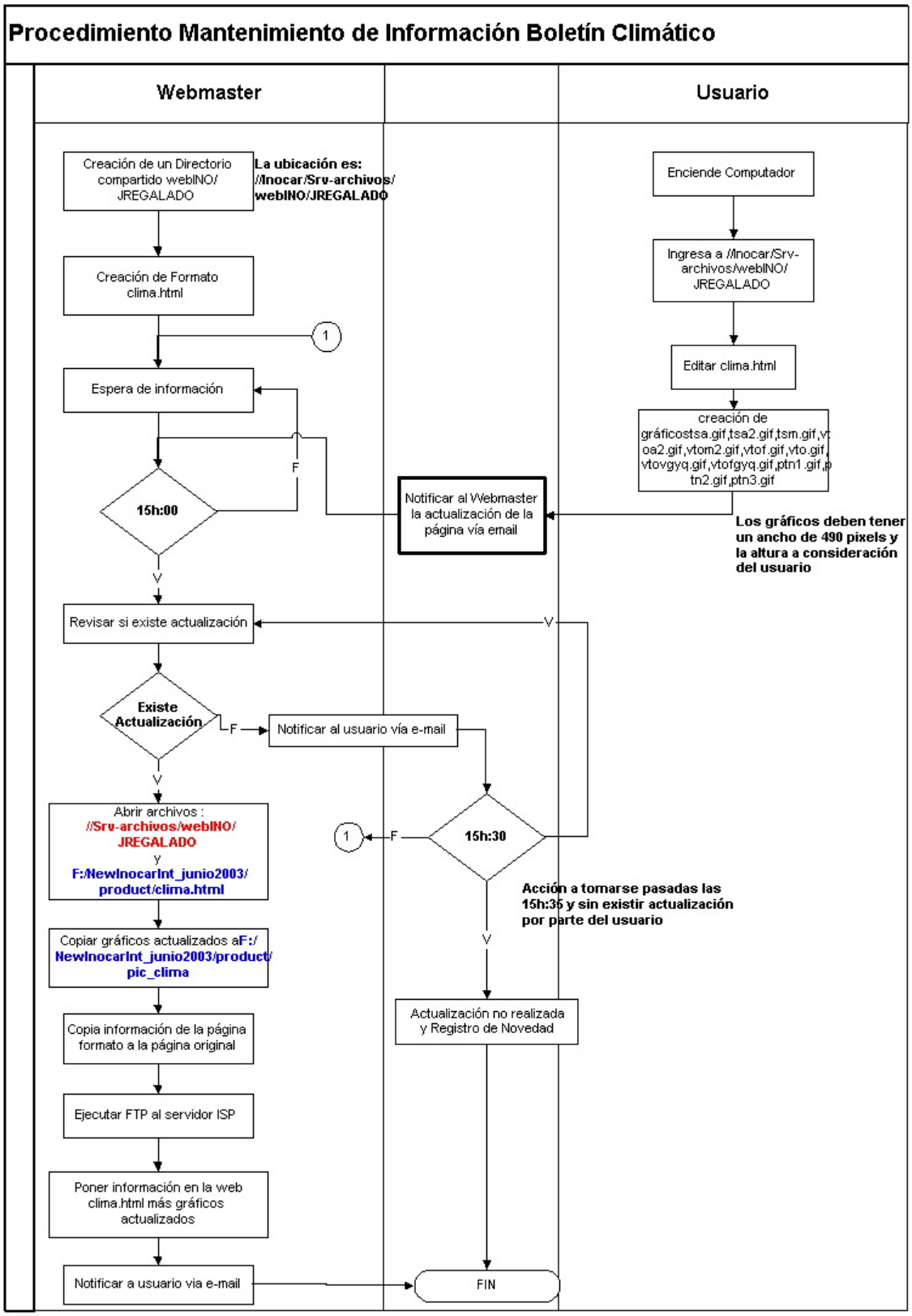
a) El usuario deberá realizar una solicitud de trabajo al departamento de Soporte Técnico, para que se le instale en su computador el software Dreamweaver para actualización y modificación de la información.
b) Una vez instalado el software, el usuario procederá a realizar la actualización de su información y de los gráficos, si estos existieren, en el formato o plantilla ya creado por el webmaster; este formato estará en la carpeta ya creada con anterioridad.

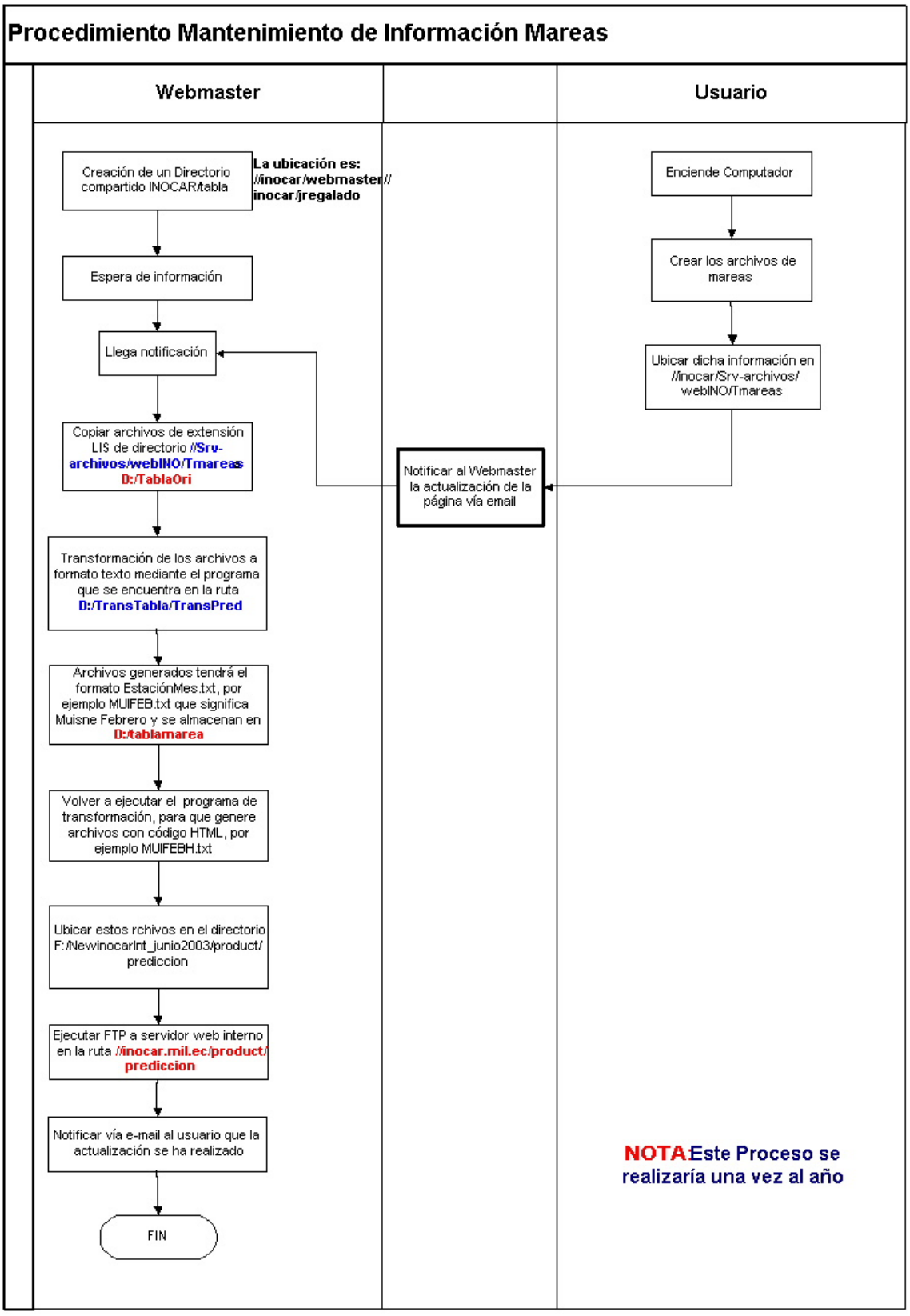
c) En el caso de usuarios que solo manejan gráficos, estos deberán ser colocados en la carpeta, sin que esto implique hacer modificación en la página, por parte del usuario.
d) El usuario solo actualizará la información, en caso de querer modificar algún hipervínculo, colocar otra imagen o hacer cualquier otro tipo de cambio que no sea actualización, deberá comunicar al webmaster, para que este proceda a realizar estos cambios.
e) Una vez que la actualización ha sido realizada por el usuario, este deberá notificar al webmaster, vía e-mail, indicando si la actualización realizada es a la información en sí, gráficos o imágenes presentadas.
f) El webmaster procederá a abrir el archivo formato (plantilla) y el archivo original (página web presentada).
g) Procederá a copiar la información del archivo formato a la página web original, guardando estos cambios.
h) Luego se procederá a realizar FTP al servidor del ISP o webhosting que se haya contratado para alojar el sitio web de la página y/o gráficos actualizados.
i) Se comunica al usuario vía e-mail que la actualización ha sido realizada, para que este revise si hay alguna modificación que hacer.
j) Si no existen modificaciones que realizar, se registra la actualización en la bitácora de actividades diarias.

2.1 PROCEDIMIENTOS ESPECIFICOS DE MANTENIMIENTO POR AREAS




Procedimiento Mantenimiento Información Ayudas a la Navegación
Webmaster
Usuario
Creación de un Directorio compartido WebINO/AYUDAS
La ubicación es: //Inocar/Srv-archivos/ webINO
Creación de Formato ayuda.html
diario
Espera de información
15:00
Revisar si existe actualización
Existe Actualización
Diario
Abrir archivos : /Inocar/Srv-archivos/ AYUDAS/ayuda.html y F:/NewInocarInt_junio2003/ boletin/ayuda.html
Copia información de la página formato a la página original
Ejecutar FTP al servidor ISP
Notificar actualización al usuario vía e-mail
Registrar actualización en bitácora
Copiar archivo ayudaMES.doc a directorio F:/ NewInocarInt_junio2003/boletin/avisos/ generar en base a este un archivo MES.pdf. Ejemplo: enero.pdf
Editar naveg.html y colocar ruta del archivo MES.pdf en la página.
Actualizaciones por lo general se realizan entre las 8:00 a 11:00
Notificar al Webmaster la actualización de la página vía e-mail
Notificar a usuario via e-mail
15:30
Acción a tomarse pasadas las 15h:35 y sin existir actualización por parte del usuario
Actualización no realizada y registro de novedad en bitácora.
FIN
Enciende Computador
Ingresa a //Inocar/Srv-archivos/WebINO/ AYUDAS
Diario
Editar ayuda.html
Editar archivo de ayuda mensual
Grabar como ayudaMES.doc Ejemplo: ayudaenero.doc Colocarlo en directorio compartido
V
F
1


Procedimiento Mantenimiento de Información Boletín Climático
Webmaster
Usuario
Creación de un Directorio compartido webINO/ JREGALADO
La ubicación es: //Inocar/Srv-archivos/ webINO/JREGALADO
Creación de Formato clima.html
1
Espera de información
F
15h:00
V
Revisar si existe actualización
Existe Actualización
F
Notificar al usuario vía e-mail
V
Abrir archivos : //Srv-archivos/webINO/ JREGALADO y F:/NewInocarInt_junio2003/ product/clima.html
Copiar gráficos actualizados aF:/ NewInocarInt_junio2003/product/ pic_clima
Copia información de la página formato a la página original
Ejecutar FTP al servidor ISP
Poner información en la web clima.html más gráficos actualizados
Notificar a usuario via e-mail
Notificar al Webmaster la actualización de la página vía email
1
F
15h:30
V
Actualización no realizada y Registro de Novedad
FIN
Acción a tomarse pasadas las 15h:35 y sin existir actualización por parte del usuario
Enciende Computador
Ingresa a //Inocar/Srv-archivos/webINO/ JREGALADO
Editar clima.html
creación de gráficostsa.gif,tsa2.gif,tsm.gif,vtoa2.gif,vtom2.gif,vtof.gif,vto.gif,vtovgyq.gif,vtofgyq.gif,ptn1.gif,ptn2.gif,ptn3.gif
Los gráficos deben tener un ancho de 490 pixels y la altura a consideración del usuario


Procedimiento Mantenimiento de Información Mareas
Webmaster
Usuario
Creación de un Directorio compartido INOCAR/tabla
La ubicación es: //inocar/webmaster// inocar/jregalado
Espera de información
Llega notificación
Copiar archivos de extensión LIS de directorio //Srv-archivos/webINO/Tmareas D:/TablaOri
Transformación de los archivos a formato texto mediante el programa que se encuentra en la ruta D:/TransTabla/TransPred
Archivos generados tendrá el formato EstaciónMes.txt, por ejemplo MUIFEB.txt que significa Muisne Febrero y se almacenan en D:/tablamarea
Volver a ejecutar el programa de transformación, para que genere archivos con código HTML, por ejemplo MUIFEBH.txt
Ubicar estos rchivos en el directorio F:/NewinocarInt_junio2003/product/ prediccion
Ejecutar FTP a servidor web interno en la ruta //inocar.mil.ec/product/ prediccion
Notificar vía e-mail al usuario que la actualización se ha realizado
FIN
Notificar al Webmaster la actualización de la página vía email
Enciende Computador
Crear los archivos de mareas
Ubicar dicha información en //inocar/Srv-archivos/ webINO/Tmareas
NOTA:Este Proceso se realizaría una vez al año

3. ELIMINACION DE INFORMACION

1. Si el Jefe Departamental da la aprobación, considerando que se tiene información que ya no se desea presentar, este o el usuario deberán comunicar al webmaster que se desea eliminar del sitio una determinada página; el webmaster eliminará este archivo de su máquina y procederá a eliminarlo del directorio del ISP o webhosting en el cual se encuentra el sitio web.

2. Se procede a comunicar al usuario que la eliminación de la página se ha realizado.

APÉNDICE H

DOCUMENTACIÓN TÉCNICA DEL ANALISIS Y DISEÑO APLICANDO EL PARADIGMA ORIENTADO A OBJETOS AL SISTEMA AVISOS A LOS NAVEGANTES

1. Lista de Casos de Usos

a) Registro de Usuario
b) Registro de Provincia
c) Registro de Sector
d) Registro de Reparto
e) Registro de Carta
f) Registro de Ayuda
g) Registro de Aviso a Navegantes
h) Registro de Vehículo
i) Registro de Comisión
j) Reporte de Comisión
k) Envío de Reportes
l) Histórico de Ayudas
m) Histórico de Avisos de Ayudas
n) Creación de Boletín Mensual
o) Creación de Boletín Anual

2. Descripción de Casos de Usos

Código	1.
Nombre	**Registro de Usuario.**
Descripción	Este caso de uso permitirá el ingreso de los Usuarios a los cuales le llegara el reporte de los avisos, además permitirá el ingreso de Usuarios que pueden utilizar el sistema y de los usuarios que participan en una comisión.
	Deberá especificarse a cada uno de los usuarios ingresado los parámetros de configuración de su medio de aviso (email, número telefónico, proveedor de pager). Dependiendo del tipo de usuario, es decir al usuario del sistema se le deberá agregar el user y password.

Código	2.
Nombre	**Registro de Provincia.**
Descripción	Este caso de uso permitirá el ingreso de las Provincias en las cuales se encuentra la Ayuda.
Nota	Cuando se cree el Aviso a los navegantes que posea una Ayuda, se mostrara la provincia en donde se encuentra la Ayuda.

Código	3.
Nombre	**Registro de Sector.**
Descripción	Este caso de uso permitirá el ingreso de los Sectores en las cuales se encuentra la Ayuda, estos sectores pertenecen a una provincia.
Nota	Cuando se cree el Aviso a los navegantes que posea una Ayuda, se mostrara el sector en donde se encuentra la Ayuda.

Código	4.
Nombre	**Registro de Reparto.**
Descripción	Este caso de uso permitirá el ingreso de los Repartos que reportan los Avisos y/o los repartos a los cuales habría que enviar los avisos de los navegantes.
Nota	Cuando se cree el Aviso a los navegantes, se debe indicar el Reparto que reporta el Aviso, por omisión los avisos son reportados por INOCAR.

Código	5.
Nombre	**Registro de Carta.**
Descripción	Este caso de uso permitirá el ingreso de las Cartas en donde se registran las ayudas.
Nota	Cuando se cree el Aviso a los navegantes que posea una Ayuda, se mostrara a que cartas puede pertenece la Ayuda.

Código	6.
Nombre	**Registro de Ayuda.**
Descripción	Este caso de uso permitirá el ingreso de la Ayuda a los navegantes (Boya, Faro, Farolete, Baliza, Enfilada) .
Nota	Las ayudas debe de tener una posición geográfica fija, por tal motivo a pesar que los corrimientos de los bajos son publicados en algunas ocasiones en los avisos no pueden ser incluidos como ayuda, estos deberán ser ingresados en los avisos.

Código	7.
Nombre	**Registro de Aviso a los Navegantes.**
Descripción	Este caso de permitirá el ingreso de los avisos a los navegantes .
Nota	Una Vez ingresado el aviso, este no será enviado a los usuarios registrados hasta que se utilice el caso de uso Envío de Reportes.

Código	8.
Nombre	**Registro de Vehículos.**
Descripción	Este caso de permitirá el ingreso de vehículos que son asignados a las comisiones.
Nota	la información que se necesita conocer de los vehículos será su código y su descripción.

Código	9.
Nombre	**Registro de Comisión.**
Descripción	Este caso de uso permitirá el ingreso de comisiones , las cuales se pueden generar a partir de un aviso de una ayuda o por un mantenimiento de la misma, esta comisión se le asignan integrantes de los cuales uno de ellos es el jefe de la comisión, además se le asignan vehículos, materiales para que los integrantes puedan realizar la misma.
Nota	Una comisión puede salir a revisar una o más ayudas.

Código	10.
Nombre	**Reporte de Comisión.**
Descripción	Este caso de uso permitirá que una vez realizada la revisión de la comisión esta pueda generar su reporte en la cual se podrá ingresar la descripción del trabajo realizado, las novedades y trabajo realizado.
Nota	La comisión genera un reporte por cada ayuda que se revisa y una conclusión general del trabajo realizado.

Código	11.
Nombre	**Envío de Reportes.**
Descripción	Este caso de uso me permitirá realizar el envío del reporte de Aviso de los navegantes a los usuarios registrados (email, pager, fax).
Nota	para poder enviar el aviso al pager se enviara un mensaje al servicio del proveedor de pager por Internet, es decir para que el mensaje pueda llegar al usuario del pager, el usuario deberá tener la contratación del servicio de mensajería por Internet brindado por su proveedor .

Código	12.
Nombre	**Histórico de Ayudas.**
Descripción	Este caso de uso permitirá realizar la consulta de los cambios que se sufren las ayudas en el tiempo.
Nota	Se guardar un histórico por cada cambio que se realice en un ayuda.

Código	13.
Nombre	**Histórico de Avisos de Ayudas.**
Descripción	Este caso de uso permitirá realizar las consultas de los avisos que se han publicado para las respectivas ayudas.
Nota	deberá mostrar el estado del aviso es decir si es Permanente, Temporal (vigente)

Código	14.
Nombre	**Creación de Boletín Mensual.**
Descripción	Este caso de uso permitirá la creación del boletín mensual en base a los avisos diarios permanentes y temporales, cada tipo de avisos están codificados de forma independiente es decir los permanentes tiene su propio código y los temporales el suyo, este código deberá poseer el siguiente formato: #/año en donde el # corresponde al número del aviso en el año.
Nota	Solo se tomara en consideración los avisos vigentes para la creación del Boletín Mensual.

Código	15.
Nombre	**Creación del Boletín Anual.**
Descripción	Este caso de uso permitirá la creación del Boletín Anual que es la recopilación de los Boletines mensuales.
Nota	Solo se tomara en consideración los avisos permanentes que se han publicado en los Boletines Mensuales

3. Escenarios

Caso de Uso: **1. Registro de Usuario**

Código	1.1
Nombre	**Creación Usuario para el envío de Avisos.**
Suposiciones	El Usuario no ha sido creado previamente. Posee un medio para recibir información.
Resultados	El usuario es creado. El usuario podrá recibir los mensajes de los Avisos.

Código	1.2
Nombre	**Creación Usuario para el envío de Avisos y el usuario ya se encuentra creado.**
Suposiciones	El Usuario ha sido creado previamente.

	Posee un medio para recibir información.
Resultados	El usuario es mostrado. El usuario podrá recibir los mensajes de los Avisos.

Código	1.3
Nombre	**Creación Usuario para uso de SISNAV.**
Suposiciones	El Usuario no ha sido creado previamente en SISNAV.
Resultados	El usuario es creado. El usuario podrá ingresar a SISNAV.

Código	1.4
Nombre	**Creación Usuario para uso de SISNAV y el usuario ya se encuentra creado.**
Suposiciones	El Usuario ha sido creado previamente en SISNAV.
Resultados	El usuario es mostrado. El usuario podrá ingresar a SISNAV.

Código	1.5
Nombre	**Creación Usuario para asignación a una comisión.**
Suposiciones	El Usuario no ha sido creado previamente. El Usuario posee información válida.
Resultados	El usuario es creado. El usuario podrá ser asignados a comisiones.

Código	1.6
Nombre	**Creación Usuario para asignación a una comisión y el usuario ya se encuentra creado.**
Suposiciones	El Usuario ha sido creado previamente.
Resultados	El usuario es mostrado. El usuario podrá ser asignados a comisiones.

Caso de Uso: **2. Registro de Provincia.**

Código	2.1
Nombre	**Creación de Provincia.**
Suposiciones	Provincia no ha sido creada previamente.
Resultados	Provincia es creada. Los sectores se pueden asignar a la Provincia.

Código	2.2
Nombre	**Creación de Provincia y Provincia ya se encuentra creada.**
Suposiciones	Provincia ha sido creada previamente.
Resultados	Provincia es mostrada. Los sectores se pueden asignar a la Provincia.

Caso de Uso: **3. Registro de Sector**

Código	3.1
Nombre	**Creación de Sector.**
Suposiciones	Sector no ha sido creado previamente. Se encuentra creada una Provincia para asignarla al sector.
Resultados	Sector es creado. Se crea la relación entre sector y la Provincia.

Código	3.2
Nombre	**Creación de Sector y Sector ya se encuentra creado.**
Suposiciones	Sector ha sido creado previamente.
Resultados	Sector es mostrado. Relación entre sector y la Provincia es mostrada.

Caso de Uso: **4. Registro de Reparto**

Código	4.1
Nombre	**Creación de Reparto.**
Suposiciones	Reparto no ha sido creado previamente.
Resultados	Reparto es creado.

Código	4.2
Nombre	**Creación de Reparto y Reparto ya se encuentra creado.**
Suposiciones	Reparto ha sido creado previamente.
Resultados	Reparto es mostrado.

Caso de Uso: **5. Registro de Carta**

Código	5.1
Nombre	**Creación de Carta.**
Suposiciones	Carta no ha sido creada previamente.
Resultados	Carta es creada.

Código	5.2
Nombre	**Creación de Carta y Carta ya se encuentra creada.**
Suposiciones	Carta ha sido creada previamente.
Resultados	Carta es mostrada.

Caso de Uso: **6. Registro de Ayuda**

Código	6.1
Nombre	**Creación de nueva Ayuda.**
Suposiciones	La Ayuda no ha sido creada previamente Las Cartas a la que afecta la Ayuda han sido creadas previamente. La Provincia en donde se encuentra la Ayuda ha sido creada previamente.
Resultados	La Ayuda es creada. La relación entre provincia y Ayuda es creada. La relación entre carta y ayuda es creada

Código	6.2
Nombre	**Creación de nueva Ayuda y Ayuda ya ha sido creada con anterioridad.**
Suposiciones	La Ayuda ha sido creada previamente Existe una relación entre provincia y Ayuda. Existe una relación entre carta y ayuda.
Resultados	La Ayuda es mostrada. La relación entre provincia y Ayuda es mostrada. La relación entre carta y ayuda es mostrada

Código	6.3
Nombre	**Creación de nueva Ayuda y Carta o Provincia no ha sido creada con anterioridad.**
Suposiciones	La Ayuda no ha sido creada previamente Las Cartas a la que afecta la Ayuda no ha sido creadas previamente. La Provincia en donde se encuentra la Ayuda no ha sido creada previamente.
Resultados	La Ayuda no es creada. La relación entre provincia y Ayuda no es creada. La relación entre carta y ayuda no es creada

Caso de Uso: **7. Registro de Aviso a los Navegantes**

Código	7.1
Nombre	**Registro de Aviso a los Navegante Permanente para Ayuda.**
Suposiciones	Ayuda ha sido creada. Cartas han sido creadas. Reparto ha sido creado.
Resultados	Aviso es creado.

Código	7.2
Nombre	**Registro de Aviso a los Navegante Permanente y no es Ayuda.**
Suposiciones	Posee coordenadas (Latitud y Longitud). Se conoce Provincia Afectada Se conoce las Cartas Afectadas. Reparto ha sido creado.
Resultados	Aviso es creado.

Código	7.3
Nombre	**Registro de Aviso a los Navegante Temporal para Ayuda.**
Suposiciones	Ayuda ha sido creada. Cartas han sido creadas. Reparto ha sido creado. No Afecta a otro Aviso Temporal.
Resultados	Aviso es creado. Estado del Aviso Vigente.

Código	7.4
Nombre	**Registro de Aviso a los Navegante Temporal para Ayuda y afecta a otro aviso.**
Suposiciones	Ayuda ha sido creada. Cartas han sido creadas. Reparto ha sido creado. Afecta a otro Aviso Temporal.
Resultados	Aviso es creado. Estado del Aviso ingresado Vigente. Estado del Aviso Afectado Anulado.

Caso de Uso: **8. Registro de Vehículos.**

Código	8.1
Nombre	**Creación de Vehículo.**
Suposiciones	Vehículo no ha sido creado previamente.
Resultados	Vehículo es creado.

Código	8.2
Nombre	**Creación de Vehículo y Vehículo ya se encuentra creado.**
Suposiciones	Vehículo ha sido creado previamente.

Resultados	Vehículo es mostrado.

Caso de Uso: **9. Registro de Comisión.**

Código	9.1
Nombre	**Creación de Comisión.**
Suposiciones	Comisión no ha sido creada previamente. Integrantes de Comisión están creados Vehículos asignados a la comisión están creados Ayudas que la comisión revisará están creadas
Resultados	Comisión es creada. Relación entre comisión e Integrantes es creada. Relación entre comisión y vehículo es creada. Relación entre Comisión y ayudas a revisar es creada.

Código	9.2
Nombre	**Creación de Comisión y Comisión ya se encuentra creada.**
Suposiciones	Comisión ha sido creada previamente.
Resultados	Comisión es mostrada. Relación entre comisión e Integrantes es mostrada. Relación entre comisión y vehículo es mostrada. Relación entre Comisión y ayudas a revisar es mostrada.

Caso de Uso: **10. Reporte de Comisión.**

Código	10.1
Nombre	**Creación de Reporte de Comisión.**
Suposiciones	Comisión ha sido creada previamente. Integrantes de Comisión estregaron reporte.
Resultados	Reporte de comisión es creado. Reporte es creado por cada ayuda revisada por la comisión.

Código	10.2
Nombre	**Creación de Reporte de Comisión y Comisión no ha sido creada.**
Suposiciones	Comisión no ha sido creada previamente. Integrantes de Comisión estregaron reporte
Resultados	Reporte de comisión no es creado.

Caso de Uso: **11. Envío de Reportes.**

Código	11.1
Nombre	**Envió de Reporte a Usuario registrado.**
Suposiciones	Fecha de Generación de Reporte posee avisos para los navegantes. Usuario posee la configuración de sus parámetros correctamente. Existe conexión a Internet, proveedor de page y Telefónica .

Resultados	El reporte es enviado satisfactoriamente a los diferentes usuarios por los diferentes medios.

Caso de Uso: **12. Histórico de Ayudas.**

Código	12.1
Nombre	**Consulta de Modificación de Ayuda.**
Suposiciones	Ayuda ha sufrido modificaciones en diferentes fechas.
Resultados	Se muestra el histórico los Ayudas de la Ayuda solicitada.

Caso de Uso: **13. Histórico de Avisos de Ayudas**

Código	13.1
Nombre	**Consulta de Avisos de Ayuda.**
Suposiciones	Avisos para Ayuda han sido ingresados en diferentes fechas.
Resultados	Se muestra el histórico los Avisos de la Ayuda solicitada. Se indica el estado de los Aviso. (Permanente/Temporal vigente o anulado)

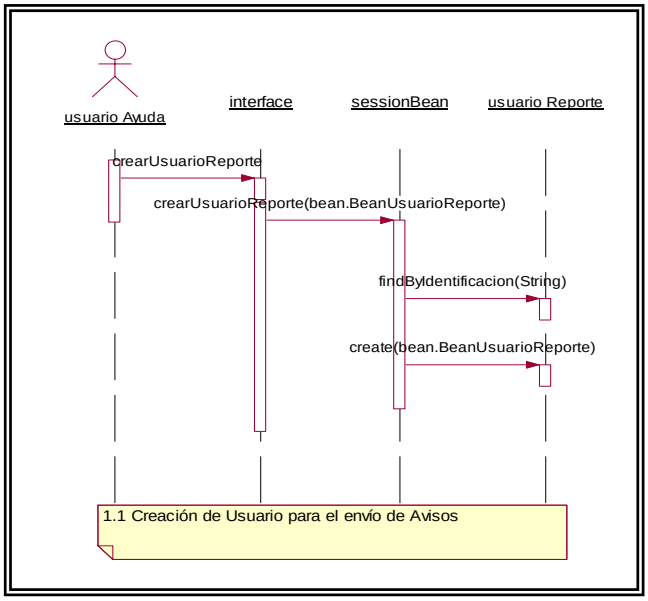
Caso de Uso: **14. Creación de Boletín Mensual.**

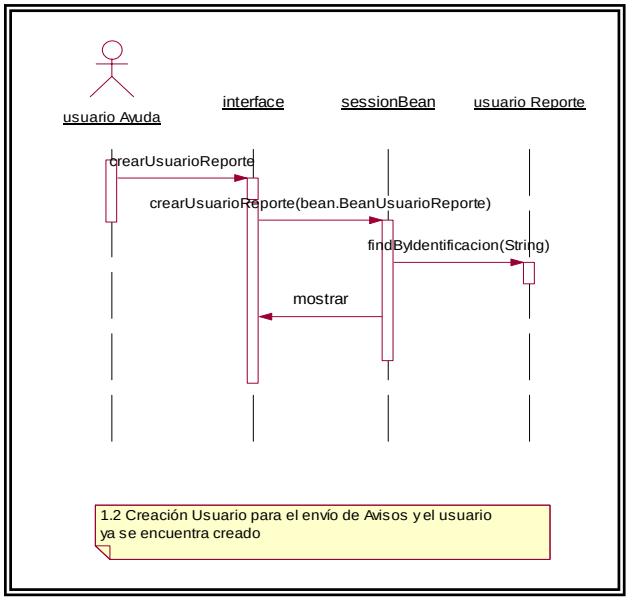
Código	14.1
Nombre	**Creación del Boletín Mensual.**
Suposiciones	Existen avisos vigentes. Boletín del mes no ha sido creado.
Resultados	Se codifica los avisos Permanentes y Temporales con su respectivo código.

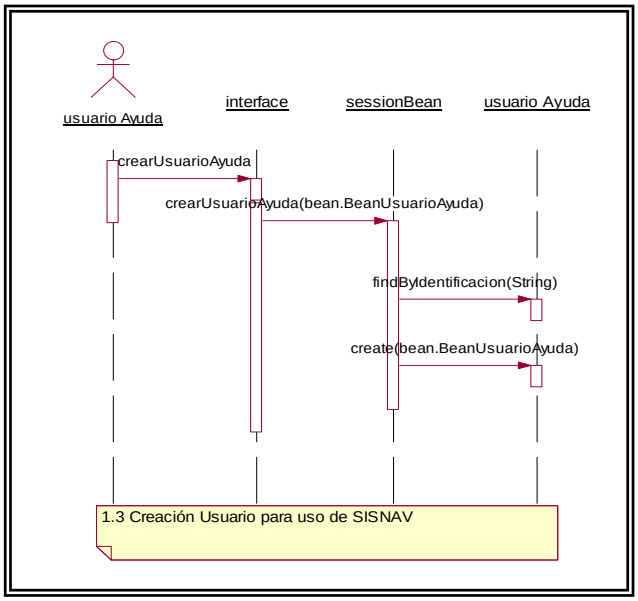
Caso de Uso: **15. Creación del Boletín Anual.**

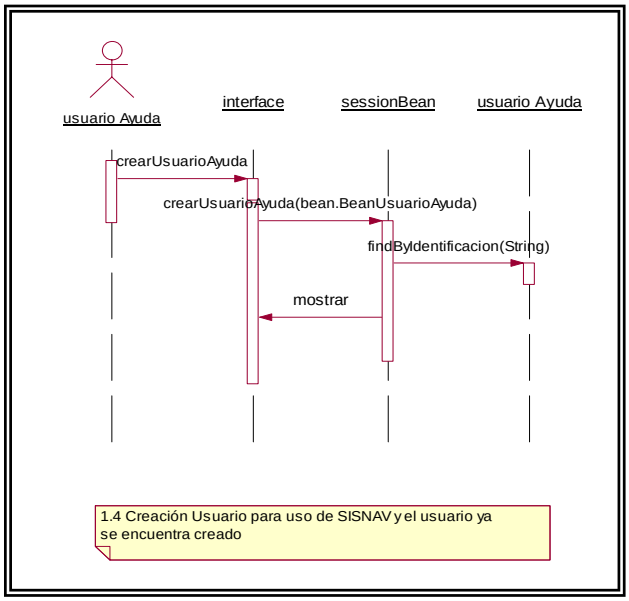
Código	15.1
Nombre	**Creación del Boletín Anual.**
Suposiciones	Se han creado los boletines mensuales. Boletín Anual no ha sido creado.
Resultados	Se selecciona los avisos permanentes de todos los avisos publicados en los boletines mensuales.

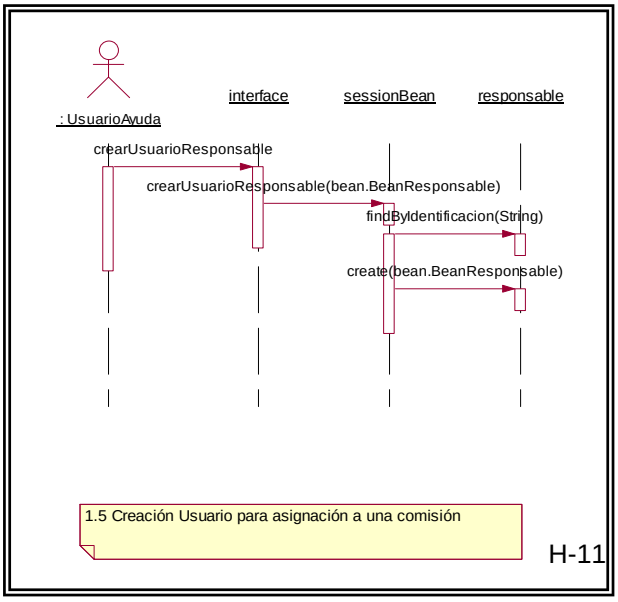
3. Diagramas de Interacción de Objetos de Diseño

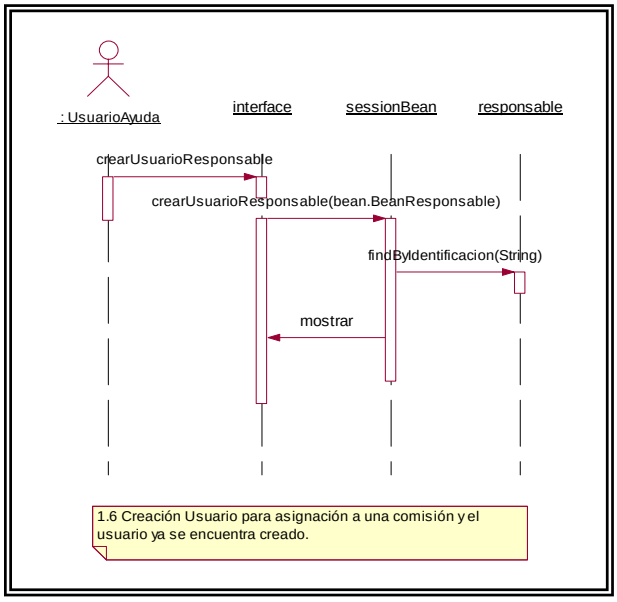


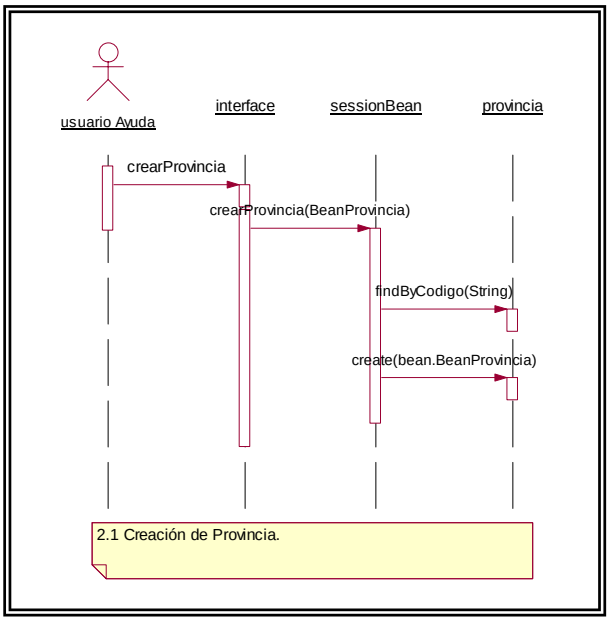


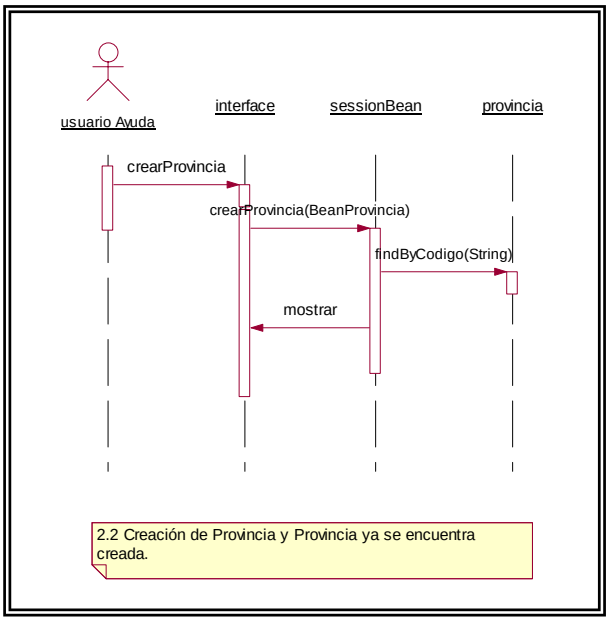


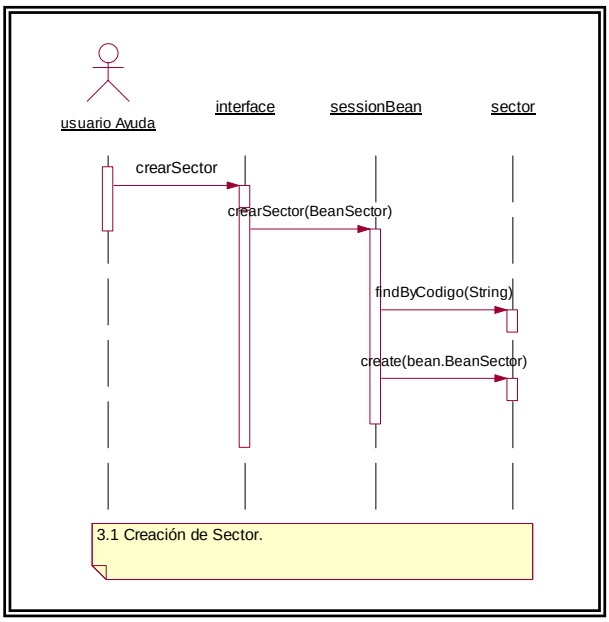


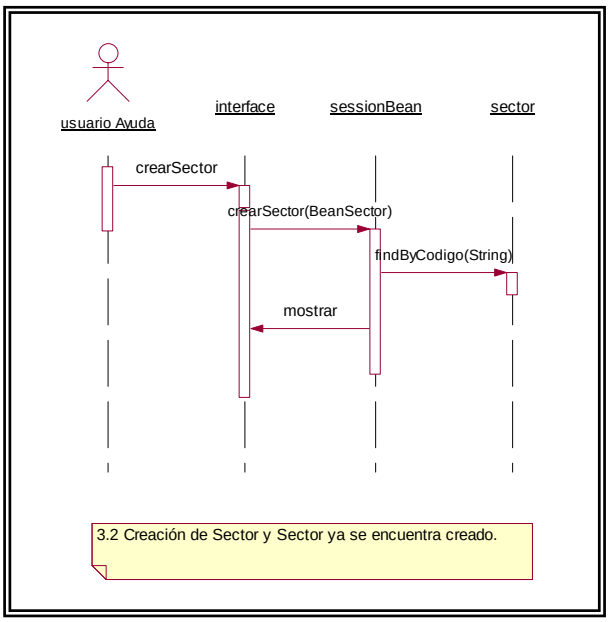


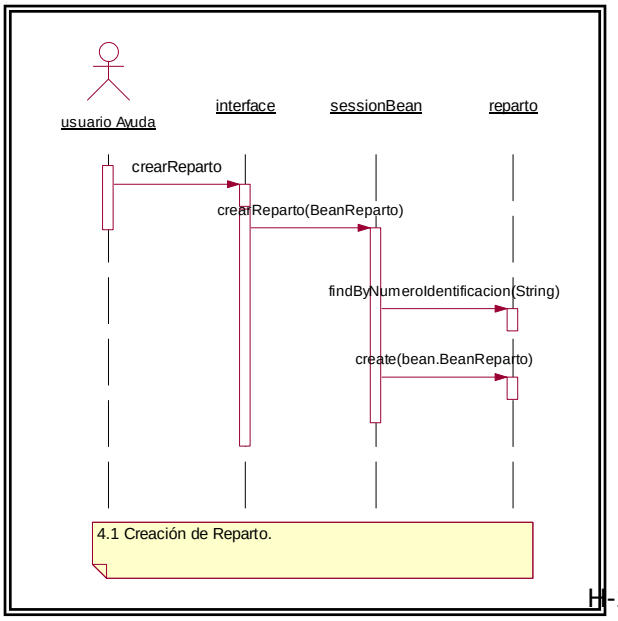


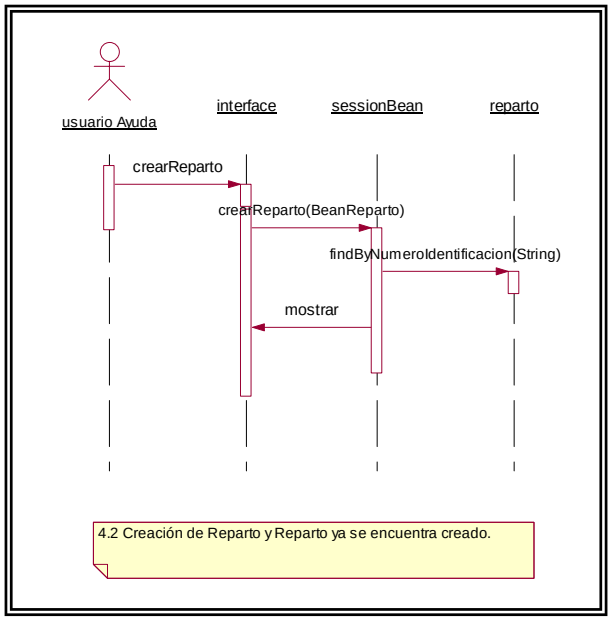

usuario Ayuda
interface
sessionBean
provincia
crearProvincia
crearProvincia(BeanProvincia)
findByCodigo(String)
create(bean.BeanProvincia)
2.1 Creación de Provincia.

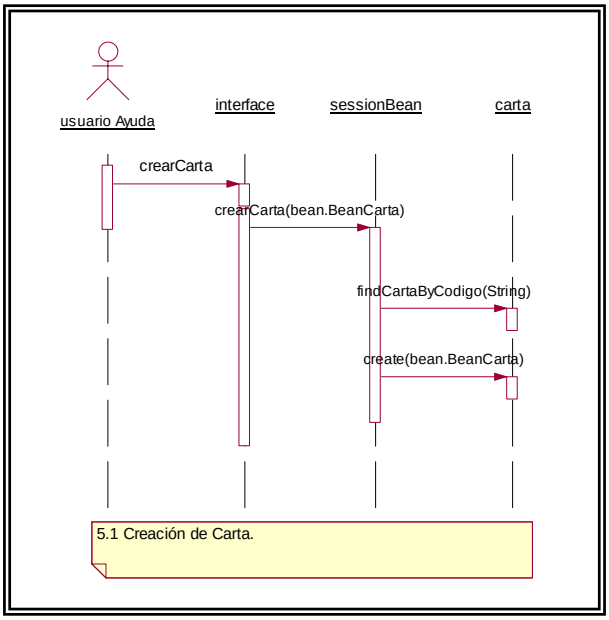

usuario Ayuda
interface
sessionBean
provincia
crearProvincia
crearProvincia(BeanProvincia)
findByCodigo(String)
mostrar
2.2 Creación de Provincia y Provincia ya se encuentra creada.

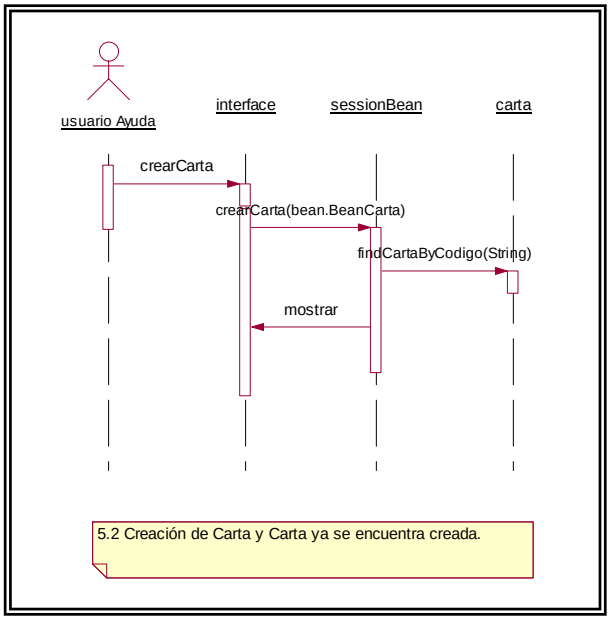

usuario Ayuda
interface
sessionBean
sector
crearSector
crearSector(BeanSector)
findByCodigo(String)
create(bean.BeanSector)
3.1 Creación de Sector.

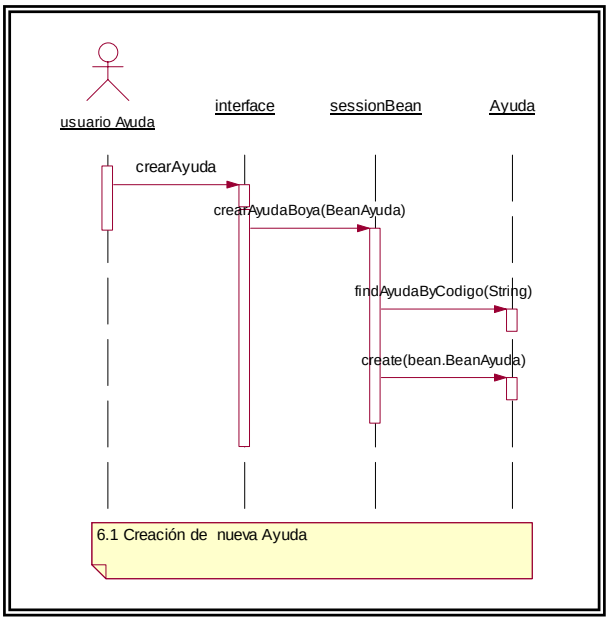

usuario Ayuda
interface
sessionBean
sector
crearSector
crearSector(BeanSector)
findByCodigo(String)
mostrar
3.2 Creación de Sector y Sector ya se encuentra creado.

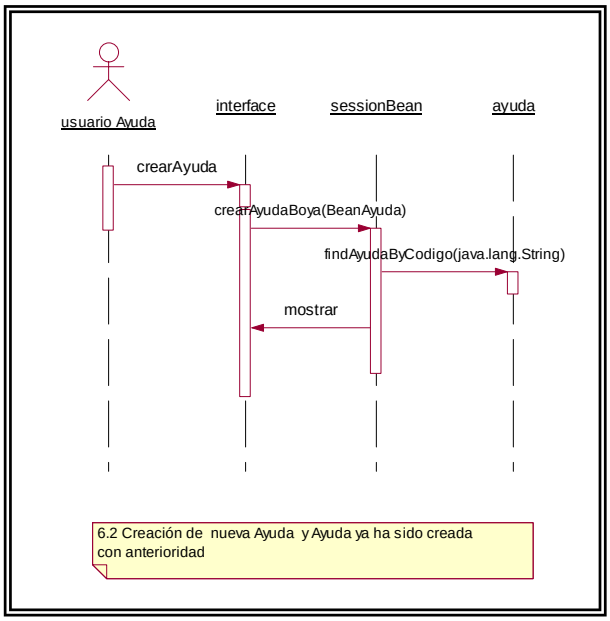

usuario Ayuda
interface
sessionBean
reparto
crearReparto
crearReparto(BeanReparto)
findByNumeroIdentificacion(String)
create(bean.BeanReparto)
4.1 Creación de Reparto.

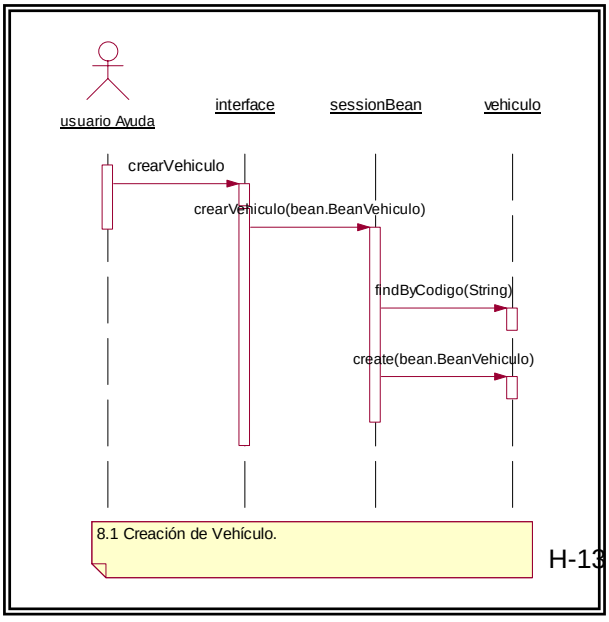

usuario Ayuda
interface
sessionBean
reparto
crearReparto
crearReparto(BeanReparto)
findByNumeroIdentificacion(String)
mostrar
4.2 Creación de Reparto y Reparto ya se encuentra creado.

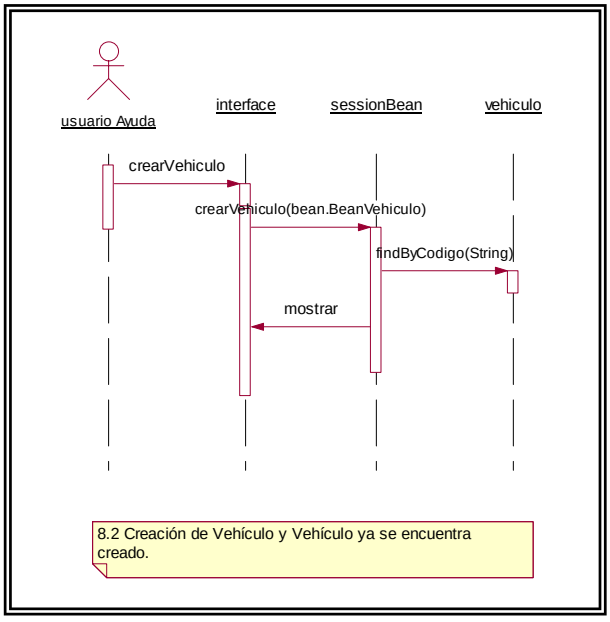

usuario Ayuda
interface
sessionBean
carta
crearCarta
crearCarta(bean.BeanCarta)
findCartaByCodigo(String)
create(bean.BeanCarta)
5.1 Creación de Carta.

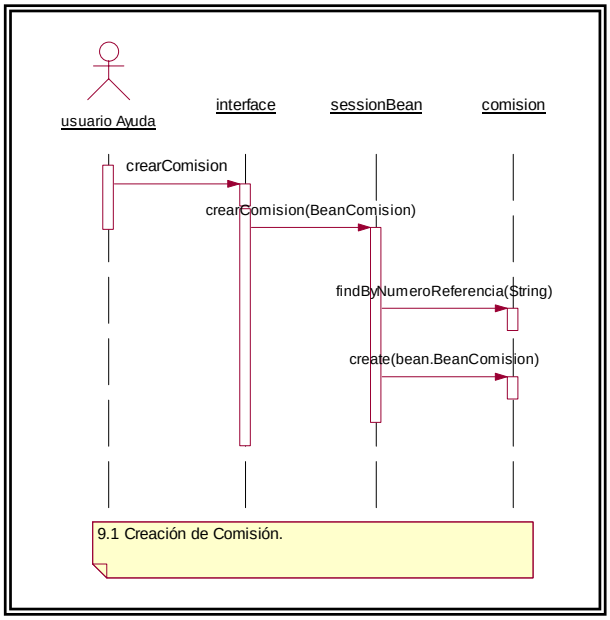

usuario Ayuda
interface
sessionBean
carta
crearCarta
crearCarta(bean.BeanCarta)
findCartaByCodigo(String)
mostrar
5.2 Creación de Carta y Carta ya se encuentra creada.

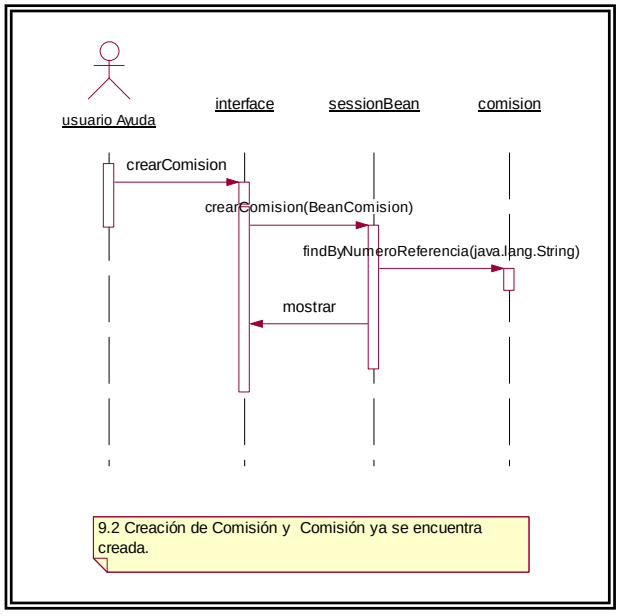

usuario Ayuda
interface
sessionBean
Ayuda
crearAyuda
crearAyudaBoya(BeanAyuda)
findAyudaByCodigo(String)
create(bean.BeanAyuda)
6.1 Creación de nueva Ayuda


usuario Ayuda
interface
sessionBean
ayuda
crearAyuda
crearAyudaBoya(BeanAyuda)
findAyudaByCodigo(java.lang.String)
mostrar
6.2 Creación de nueva Ayuda y Ayuda ya ha sido creada con anterioridad


usuario Ayuda
interface
sessionBean
vehiculo
crearVehiculo
crearVehiculo(bean.BeanVehiculo)
findByCodigo(String)
create(bean.BeanVehiculo)
8.1 Creación de Vehículo.


usuario Ayuda
interface
sessionBean
vehiculo
crearVehiculo
crearVehiculo(bean.BeanVehiculo)
findByCodigo(String)
mostrar
8.2 Creación de Vehículo y Vehículo ya se encuentra creado.


usuario Ayuda
interface
sessionBean
comision
crearComision
crearComision(BeanComision)
findByNumeroReferencia(String)
create(bean.BeanComision)
9.1 Creación de Comisión.


usuario Ayuda
interface
sessionBean
comision
crearComision
crearComision(BeanComision)
findByNumeroReferencia(java.lang.String)
mostrar
9.2 Creación de Comisión y Comisión ya se encuentra creada.

4. Descripción de Clases de Análisis

Nombre de Clase: ProvinciaBean

Esta clase representa a las provincias del perfil costanero en donde se encuentras las Ayudas.

Atributos	Descripción
latitud Máxima	Representa la latitud máxima, la cual es un vértice de un rectángulo en donde se encuentra la provincia
latitud Mínima	Representa la latitud mínima, la cual es un vértice de un rectángulo en donde se encuentra la provincia
longitud Máxima	Representa la longitud máxima, la cual es un vértice de un rectángulo en donde se encuentra la provincia
longitud Mínima	Representa la longitud mínima, la cual es un vértice de un rectángulo en donde se encuentra la provincia
código	Código que representa a la provincia
nombre	Nombre de la provincia
descripción	Descripción de la provincia
sigla	Sigla que representa a la provincia
posiciónLatMax	Representa la posición de la latitud Máxima
posiciónLatMin	Representa la posición de la latitud Mínima
posiciónLogMax	Representa la posición de la longitud Máxima
posiciónLogMin	Representa la posición de la longitud Mínima

Clase Relacionada	Tipo de Relación	nombre
SectorBean	Una Provincia posee muchos sectores	Posee
Subclase		
Superclase		

Nombre de Clase: SectorBean

Esta clase representa a los diferentes sectores que posee una provincia, en estos sectores son donde se encuentra las ayudas.

Atributos	Descripción
código	Código que representa al sector
nombre	Nombre del sector

Clase Relacionada	Tipo de Relación	nombre
ProvinciaBean	Un Sector solo se encuentra en una sola provincia	Posee
AyudaBean	Una Sector se encuentra muchas ayudas	Ubica

Subclase
Superclase

Nombre de Clase: AyudaBean

Esta clase representa las ayudas que se encuentran en el perfil costanero.

Atributos	**Descripción**
alcanceGeografico	Alcance geográfico de la ayuda en millas
alcanceNominal	Alcance nominal de la ayuda en millas
alturaFisica	Altura física de la ayuda en metros
alturaNivelMar	Altura desde el nivel del mar donde se encuentra la ayuda en metros
latitud	Latitud que se encuentra ubicada la ayuda
longitud	Longitud que se encuentra ubicada la ayuda
luminosidad	Descripción de la provincia
periodo	Tiempo del periodo en segundos
veces	Numero de veces que se repiten datos como el destello eclipse
anioConstruccion	Año de construcción de la ayuda
anioModificacion	Año que la ayuda a sufrido modificaciones
anioUltimaModificacion	Año de la última modificación
descripción	Descripción de la ayuda
nombre	Nombre de la ayuda
noOrdenNacional	Número de la orden nacional de la ayuda
noOrdenInternacional	Número de la orden internacional de la ayuda
observación	Observación de la ayuda
color	Color de la ayuda
posicionLog	Representa la posición de la longitud
posicionLat	Representa la posición de la latitud

Clase Relacionada	**Tipo de Relación**	**nombre**
CartaBean	Una ayuda se encuentra muchas cartas	seEncuentra
Reporte	Una ayuda realiza muchos reportes de Comisión	Realizan
SectorBean	Una ayuda se encuentra en un solo sector	Ubica
DetalleAvisoBean	Una ayuda se puede encontrar en muchos detalles de aviso	SeEncuentra

Subclase: • FaroBean • FaroleteBean • BoyaBean • BalizaBean • EnfiladaBean
Superclase

Nombre de Clase: **CartaBean**

Esta clase representa a las Cartas Náuticas en donde se encuentran localizadas las ayudas

Atributos	Descripción
latitud Máxima	Representa la latitud máxima que posee la Carta.
latitud Mínima	Representa la latitud mínima que posee la Carta.
longitud Máxima	Representa la longitud máxima que posee la Carta.
longitud Mínima	Representa la longitud mínima que posee la Carta.
código	Código que representa a la Carta.
nombre	Nombre de la Carta.
posiciónLatMáx	Representa la posición de la latitud Máxima.
posiciónLatMín	Representa la posición de la latitud Mínima.
posiciónLogMáx	Representa la posición de la longitud Máxima.
posiciónLogMín	Representa la posición de la longitud Mínima.

Clase Relacionada	Tipo de Relación	nombre
AyudaBean	Una Carta Contiene muchas ayudas	Posee

Subclase
Superclase

Nombre de Clase: **ReporteBean**

Esta clase representa a los diferentes reportes que generan las comisiones a partir de las ayudas

Atributos	Descripción
trabajoRealizado	trabajo realizado en la Ayuda
descripcionTrabajo	Una descripción del tipo de trabajo que se realizo
novedadesSolución	Novedades que se presentaron en la reparación
fecha	Fecha en que se efectuó dicho trabajo

Clase Relacionada	Tipo de Relación	Nombre
AyudaBean	un reporte solo es de una ayuda	Realizan
ComisionBean	Un reporte solo lo hace una comisión	Realiza

Subclase
Superclase

Nombre de Clase: **DetalleAvisoBean**

Esta clase representa al detalle de los avisos temporales o permanentes que se generan por motivo de las ayudas.

Atributos	Descripción
latitud	Representa la latitud de la ayuda del aviso
longitud	Representa la longitud de la ayuda del aviso
nombre	Nombre de la Ayuda
descripción	Descripción del Aviso
posiciónLat	Representa la posición de la latitud
posiciónLog	Representa la posición de la longitud
tipo	El tipo de ayuda

Clase Relacionada	Tipo de Relación	nombre
AyudaBean	Un detalleAviso puede pertenecer a una ayuda	SeEncuentra
AvisoBean	Un detalleAviso corresponde aun aviso	corresponde

Subclase
Superclase

Nombre de Clase: **VehiculoBean**

Esta clase representa a los vehículos que se asignan a las comisiones.

Atributos	Descripción
código	Código que representa al vehículo
descripción	Descripción del vehículo

Clase Relacionada	Tipo de Relación	Nombre
ComisionBean	Un vehículo puede ser asignado a muchas comisiones	Asigna

Subclase
Superclase

Nombre de Clase: **ComisiónBean**

Esta clase representa a las comisiones que se generan para el mantenimiento o reparación de la Ayuda.

Atributos	Descripción
materiales	Materiales utilizados
numero	Numero de la comisión

referencia	Referencia de la comisión
Estado	Estado de dicha comisión
fechaSalida	Fecha de salida de la comisión
fechaRetorno	Fecha de retorno de la comisión

Clase Relacionada	**Tipo de Relación**	**Nombre**
VehiculoBean	Una comisión puede usar muchos vehículos	asigna
AvisoBean	Una comisión se puede generar de un aviso	Generar
ResponsableBean	Una comisión se puede asignar a muchos responsable	Asignar
ReporteBean	Una comisión puede realizar varios reportes	Realiza

Subclase
Superclase

Nombre de Clase: **UsuarioBean**

Esta clase representa a los posibles usuarios que participan en SISNAV.

Atributos	**Descripción**
apellido	Apellido del usuario
nombre	Nombre del usuario
cargo	Cargo del usuario
NumeroIdentificación	Número de identificación
tipoIdentificación	Tipo de identificación Ruc/cedula
titulo	Titulo del usuario

Clase Relacionada	**Tipo de Relación**	**Nombre**

Subclase • ResponsableBean • UsuarioAyudaBean • UsuarioResponsableBean
Superclase

Nombre de Clase: **UsuarioAyudaBean**

Esta clase representa a los usuarios que tienen acceso a SISNAV

Atributos	Descripción
password	Password para poder ingresar al sistema
user	User para poder ingresar al sistema

Clase Relacionada	Tipo de Relación	Nombre
AvisoBean	Un UsuarioAyuda crea muchos avisos	Crea

Subclase
Superclase • UsuarioBean

Nombre de Clase: UsuarioReporteBean

Esta clase representa a los usuarios que SISNAV deberá enviar información de los reportes.

Atributos	Descripción
email	Email del usuario
fax	Fax del usuario
pin	Pin del beeper
servicio	Tipo de servicio
tipoBeeper	Tipo de Beeper

Clase Relacionada	Tipo de Relación	Nombre

Subclase
Superclase • UsuarioBean

Nombre de Clase: UsuarioResponsableBean

Esta clase representa a los usuarios que pueden participar en una comisión.

Atributos	Descripción
email	Email del usuario
fax	Fax del usuario
pin	Pin del beeper
servicio	Tipo de servicio
tipoBeeper	Tipo de Beeper

Clase Relacionada	Tipo de Relación	Nombre

Subclase
Superclase • UsuarioBean

Nombre de Clase: AvisoBean

Esta clase representa a los avisos que se generan para las diferentes Ayudas.

Atributos	**Descripción**
descripción	Descripción del aviso
estado	Estado del aviso
mensaje	Mensaje de aviso
numero	Numero de aviso
tipo	Tipo de aviso que se genera
listaFaroBoya	Este aviso modifica la listado de faros y boya
derroteroEcuador	Este aviso modifica la lista de derrotero del Ecuador
enviado	Si el aviso ha sido enviado o no

Clase Relacionada	**Tipo de Relación**	**Nombre**
UsuarioAyudaBean	Un Aviso es creado por un Usuario.	Crea
ComisionBean	Un Aviso puede generar una Comisión.	Generar
DetalleAvisoBean	Un Aviso contiene muchos detalles de aviso	Corresponde
RepartoBean	Un Aviso puede ser informado por un reparto	OrigenInformacion
AvisoBean	Un aviso puede anular a otro aviso	Anula

Subclase
Superclase

Nombre de Clase: RepartoBean

Esta clase representa a los Repartos que en el país.

Atributos	**Descripción**
descripción	Descripción del Reparto
estado	Estado del reparto
nombre	Nombre del Reparto
numeroIdentificación	Número de identificación
razón	Razón social del reparto
tipoIdentificación	Tipo de identificación Ruc/cedula
email	Email del reparto

fax	Fax del reparto
pin	Pin del beeper
servicio	Tipo de servicio

Clase Relacionada	Tipo de Relación	Nombre
AvisoBean	Un Reparto puede informar muchos Avisos	Generar

Subclase
Superclase

5. Descripción de Clases de Diseño

Nombre de Clase: <u>ProvinciaBean</u>

Atributos	Tipo	Descripción
oid	Double	Identificador único para los objetos
latitud Máxima	Double	
latitud Mínima	Double	
longitud Máxima	Double	
longitud Mínima	double	
código	String	
nombre	String	
descripción	String	
sigla	String	
posiciónLatMáx	String	
posiciónLatMín	String	
posiciónLogMáx	String	
posiciónLogMín	String	
usuarioMOid	double	oid del último usuario que modifico la provincia
usuarioOid	double	oid del usuario que creo la provincia
fechaUsuarioM	Timestamp	Fecha de la última modificación de la provincia
fechaUsuario	Timestamp	Fecha de creación de la provincia

Clase Relacionada	Tipo de Relación	Método	Tipo Devuelto
SectorBean	Una Provincia posee muchos sectores	getSector()	Enumeration

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create()	BeanProvincia	ProvinciaBean	Permite crear una instancia de ProvinciaBean a partir de un objeto liviano que proviene de la clase BeanProvincia
getCodigo()		String	Permite recupera el código
getDescripcion()		String	Permite recuperar la descripción
get latitudMaxima()		Double	Permite recupera la latitud máxima
get latitudMinima()		Double	Permite recupera la latitud mínima
get longitudMaxima()		Double	Permite recupera la longitud máxima
get longitudMinima()		Double	Permite recupera la longitud mínima
getNombre()		String	Permite recuperar el nombre
getSiglas()		String	Permite recuperar las siglas
getPosicionLatMax()		String	Permite recupera la posición de latitud máxima
getPosicionLatMin()		String	Permite recupera la posición de latitud mínima
getPosicionLogMax()		String	Permite recupera la posición de longitud máxima
getPosicionLogMin()		String	Permite recupera la posición de longitud mínima
getUsuarioMOid()		double	Permite recuperar el usuario que modifico el objeto
getUsuarioOid()		double	Permite recuperar el usuario que creo el objeto
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setCodigo()	String	Void	Permite poner el código
setDescripcion()	String	Void	Permite poner la descripción
setLatitudMaxima()	double	Void	Permite poner la latitud máxima
setLatitudMinima()	double	void	Permite poner la latitud mínima
setLongitudMaxima()	double	void	Permite poner la longitud máxima
setLongitudMinima()	double	void	Permite poner la longitud mínima
setNombre()	String	void	Permite poner el nombre
setSiglas()	String	void	Permite poner las siglas
setPosicionLatMax()	String	void	Permite poner la posición de la latitud máxima
setPosicionLatMin()	String	void	Permite poner la posición de la latitud mínima

setPosicionLogMax()	String	void	Permite poner la posición de la longitud máxima
setPosicionLogMin()	String	void	Permite poner la posición de la longitud mínima
setUsuarioMOid()	Double	void	Permite poner el usuario que modifico el objeto
setUsuarioOid()	Double	void	Permite poner el usuario que creo el objeto
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
findAll()		Enumeration	Permite recuperar todas las provincias
findByCodigo()	String	Provincia	Permite recuperar la provincia según el código

Nombre de Clase: **SectorBean**

Esta clase Representa a los diferentes sectores que contiene una provincia.

Atributos	**Tipo**	**Descripción**
oid	double	Identificador único para los objetos
código	String	
nombre	String	
provincia_oid	Double	Para mantener la relación con provincia
usuarioMOid	Double	oid del último usuario que modifico el sector
usuarioOid	Double	oid del usuario que creo el sector
fechaUsuarioM	Timestamp	fecha de la última modificación del sector
fechaUsuario	Timestamp	fecha de creación del sector

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
ProvinciaBean	Un Sector solo se encuentra en una sola provincia	getProvincia()	ProvinciaBean
AyudaBean	Una Sector posee muchas ayudas	getAyuda()	Enumeration

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create()	BeanSector	SectorBean	Permite crear una instancia de SectorBean a partir de un objeto liviano que proviene de la clase BeanSector
getCodigo()		String	Permite recupera el código
getNombre()		String	Permite recuperar el nombre

getCodigo()		String	Permite recupera el código
getNombre()		String	Permite recuperar el nombre
getUsuarioMOid()		Double	Permite recuperar el usuario que modifica
getUsuarioOid()		Double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setCodigo()	String	void	Permite poner el código
setNombre()	String	void	Permite poner el nombre
setUsuarioMOid()	Double	void	Permite poner el usuario que modifica
setUsuarioOid()	Double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
SetFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
findAll()		Enumeration	Permite recuperar todos los sectores
findByCodigo()	String	Sector	Permite recuperar todos los sectores por el código

Nombre de Clase: **AyudaBean**

Esta clase Representa Todas las posibles ayudas que se encuentran en el perfil costanero

Atributos	**Tipo**	**Descripción**
Oid	Double	Identificador único para los objetos
AlcanceGeografico	double	
AlcanceNominal	double	
AlturaFisica	double	
AlturaNivelMar	double	
Latitud	double	
Longitud	double	
Luminosidad	double	
Periodo	double	
Veces	double	
AnioConstruccion	String	
AnioModificacion	String	
AnioUltimaModificacion	String	
Descripción	String	
Nombre	String	

NoOrdenNacional	String	
NoOrdenInternacional	String	
Observación	String	
Color	String	
PosicionLog	String	
PosicionLat	String	
usuarioMOid	Double	oid del último usuario que modifico la ayuda
usuarioOid	Double	oid del usuario que creo la ayuda
fechaUsuarioM	Timestamp	fecha de la última modificación la ayuda
fechaUsuario	Timestamp	fecha de creación de la ayuda
SectorOid	String	Representa la relación con sector

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
GrupoBean	UnaAyuda contiene muchos grupos	getGrupo()	Enumeration
ReporteBean	Una ayuda posee muchos reportes	getReporte()	Enumeration
SectorBean	Una ayuda se encuentra en un solo sector	getSector()	SectorBean
DetalleAvisoBean	Una ayuda se encuentra en muchos detalles de aviso	getDetalleAviso()	Enumeration
CartaAyudaBean	Una ayuda se encuentra en muchas CartasAyuda	getCartaAyuda()	Enumeration

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
Create	BeanAyuda	AyudaBean	Permite crear una instancia de AyudaBean a partir de un objeto liviano que proviene dela clase BeanAyuda
getAlcanceGeografico()		double	Permite recuperar el alcance geográfico de la Ayuda
getAlcanceNominal()		double	Permite recuperar el alcance nominal de la Ayuda
getAlturaNivelMar()		double	Permite recuperar la altura a nivel del mar de la Ayuda
getAnioConstruccion()		String	Permite recuperar el año de construcción
getAnioModificacion()		String	Permite recuperar el año de modificación

GetAnioUltimaModificacion( )		String	Permite recuperar el año de la ultima modificación
getColor()		String	Permite recuperar el color
getDescripcion()		String	Permite recuperar la descripción
get latitud()		double	Permite recuperar la latitud de la ayuda
get longitud()		double	Permite recuperar la longitud de la ayuda
getLuminosidad()		Double	Permite recuperar la luminosidad
getNombre()		String	Permite recuperar el nombre
getNombreSector()		String	Permite recuperar el nombre del sector
GetNoOrdenInternacional()		String	Permite recuperar el número de orden internacional
getNoOrdenNacional()		String	Permite recuperar el número de orden nacional
getObservacion()		String	Permite recuperar la observación
getPeriodo()		String	Permite recuperar el periodo
getPosicionLat()		String	Permite recuperar la posición de la latitud
getPosicionLog()		String	Permite recuperar la posición de la longitud
getVeces()		String	Permite recuperar el numero de veces
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setAlcanceGeografico()	double	void	Permite poner el alcance geográfico de la Ayuda
setAlcanceNominal()	double	void	Permite poner el alcance nominal de la Ayuda
setAlturaNivelMar()	double	void	Permite poner la altura a nivel del mar de la Ayuda
setAnioConstruccion()	String	void	Permite poner el año de construcción
setAnioModificacion()	String	void	Permite poner el año de modificación
SetAnioUltimaModificacion( )	String	void	Permite poner el año de la ultima modificación
setColor()	String	void	Permite poner el color
setDescripcion()	String	void	Permite poner la descripción

set latitud()	double	void	Permite poner la latitud de la ayuda
set longitud()	double	void	Permite poner la longitud de la ayuda
setLuminosidad()	Double	void	Permite poner la luminosidad
setNombre()	String	void	Permite poner el nombre
setNombreSector()	String	void	Permite poner el nombre del sector
SetNoOrdenInternacional()	String	void	Permite poner el número de orden internacional
setNoOrdenNacional()	String	void	Permite poner el número de orden nacional
setObservacion()	String	void	Permite poner la observación
setPeriodo()	String	void	Permite poner el periodo
setPosicionLat()	String	void	Permite poner la posición de la latitud
setPosicionLog()	String	void	Permite poner la posición de la longitud
setVeces()	String	void	Permite poner el numero de veces
setUsuarioMOid()	Double	void	Permite poner el usuario que modifica
setUsuarioOid()	Double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
findAll()		Enumeration	Permite recuperar todos las ayudas

Subclase: • FaroBean • FaroleteBean • BoyaBean • BalizaBean • EnfiladaBean
Superclase

Nombre de Clase: **CartaAyudaBean**

Esta clase Representa a los diferentes CartaAyuda que contiene una Ayuda y Carta.

Atributos	Tipo	Descripción
Ayuda_oid	Double	Representa la relación con ayuda
Carta_oid	Double	Representa la relación con carta

Clase Relacionada	Tipo de Relación	método	Tipo Devuelto
CartaBean	Un CartaAyuda contiene a una carta	getCarta()	CartaBean
AyudaBean	Un CartaAyuda contiene a una ayuda	getAyuda()	AyudaBean

Subclase
Superclase

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
Create	double	CartaAyudaBean	Permite crear una instancia de CartaAyudaBean a partir de dos valores, uno de ayuda y otro de carta por medio del Oid

Nombre de Clase: **ReporteBean**

Esta clase Representa a los reportes que se generan por las ayudas.

Atributos	Tipo	Descripción
Oid	Double	identificador único para los objetos
trabajoRealizada	String	
descripcionTrabajo	String	
novedadesSolución	String	
fecha	Date	
ayuda_oid	Double	Representa la relación con ayuda
comision_oid	Double	Representa la relación con comisión
usuarioMOid	Double	oid del último usuario que modifico el reporte
usuarioOid	Double	oid del usuario que creo el reporte
fechaUsuarioM	Timestamp	fecha de la última modificación del reporte
fechaUsuario	Timestamp	fecha de creación del reporte

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
AyudaBean	Un reporte es solo de una ayuda	getAyuda()	AyudaBean
ComisionBean	Un reporte solo pertenece una comisión	getComision()	ComisionBean

Subclase			
Superclase			
Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create	BeanReporte	ReporteBean	Permite crear una instancia de ReporteBean a partir de un objeto liviano que proviene de la clase BeanReporte
getDescripcionTrabajo()		String	Permite recupera la fecha
getFecha()		Date	Permite recuperar la descripción
getNovedadesSolucion()		String	Permite recupera las novedades de la solución
getTrabajoRealizado()		String	Permite recupera el trabajo realizado
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setDescripcionTrabajo()	String	void	Permite poner la fecha
setFecha()	Date	void	Permite poner la poner
setNovedadesSolucion()	String	void	Permite recupera las novedades de la solución
setTrabajoRealizado()	String	void	Permite poner el trabajo realizado
setUsuarioMOid()	double	void	Permite poner el usuario que modifica
setUsuarioOid()	double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación

Nombre de Clase: **CartaBean**

Esta clase Representa a las cartas de las diferentes ayudas

Atributos	**Tipo**	**Descripción**
oid	Double	identificador único para los objetos
latitud Máxima	Double	
latitud Mínima	Double	
longitud Máxima	Double	
longitud Mínima	Double	
código	String	
nombre	String	
posiciónLatMáx	String	
posiciónLatMín	String	
posiciónLogMáx	String	
posiciónLogMín	String	
usuarioMOid	Double	oid del último usuario que modifico la carta
usuarioOid	Double	oid del usuario que creo la carta
fechaUsuarioM	Timestamp	fecha de la última modificación la carta
fechaUsuario	Timestamp	fecha de creación de la carta

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
CartaAyudaBean	Una carta se encuentra en muchas CartasAyuda	getCartaAyuda( )	Enumeration

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create	BeanCarta	CartaBean	Permite crear una instancia de CartaBean a partir de un objeto liviano que proviene de la clase BeanCarta
getCodigo()		String	Permite recupera el código
get latitudMax ()		double	Permite recupera la latitud máxima
get latitudMin()		double	Permite recupera la latitud mínima
get longitudMax ()		double	Permite recupera la longitud máxima

get longitudMin()		double	Permite recupera la longitud mínima
getNombre()		String	Permite recuperar el nombre
getPosicionLatMax()		String	Permite recupera la posición latitud máxima
getPosicionLatMin()		String	Permite recupera la posición latitud mínima
getPosicionLogMax()		String	Permite recupera la posición longitud máxima
getPosicionLogMin()		String	Permite recupera la posición longitud mínima
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setCodigo()	String	void	Permite poner el código
set latitudMax ()	double	void	Permite poner la latitud máxima
set latitudMin ()	double	void	Permite poner la latitud mínima
set longitudMax ()	double	void	Permite poner la longitud máxima
set longitudMin ()	double	void	Permite poner la longitud mínima
setNombre()	String	void	Permite poner el nombre
setPosicionLatMax()	String	void	Permite poner la posición latitud máxima
setPosicionLatMin()	String	void	Permite poner la posición latitud mínima
setPosicionLogMax()	String	void	Permite poner la posición longitud máxima
setPosicionLogMin()	String	void	Permite poner la posición longitud mínima
setUsuarioMOid()	double	void	Permite poner el usuario que modifica
setUsuarioOid()	double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
findAll()		Enumeration	Permite recuperar todas las cartas
findByCodigo()	String	Carta	Permite recuperar la carta según el código

Nombre de Clase: **OidKeeperBean**

Esta clase Representa a los diferentes números para generar los Oid de las clases

Atributos	Tipo	Descripción
Oid	Double	identificador único para los objetos
nombre	String	Nombre del identificador

Clase Relacionada	Tipo de Relación	método	Tipo Devuelto

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
getOid()		Double	Permite recupera el número para generar secuencia
setOid()	Double	void	Permite poner el número para generar secuencia

Nombre de Clase: **VehiculoBean**

Esta clase Representa a los vehículos que se encuentran para las reparaciones.

Atributos	Tipo	Descripción
oid	Double	identificador único para los objetos
código	String	
descripción	String	
usuarioMOid	Double	oid del último usuario que modifico el vehículo
usuarioOid	Double	oid del usuario que creo el vehículo
fechaUsuarioM	Timestamp	fecha de la última modificación del vehículo
fechaUsuario	Timestamp	fecha de creación del vehículo

Clase Relacionada	Tipo de Relación	método	Tipo Devuelto
ComisionVehiculoBean	Un vehículo puede estar en muchos comisionVehiculo	getComisionVehiculo()	Enumeration

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
Create	BeanVehiculo	VehiculoBean	Permite crear una instancia de VehiculoBean a partir de un objeto liviano que proviene de la clase BeanVehiculo
getCodigo()		String	Permite recupera el código

getDescripcion()		String	Permite recuperar la descripción
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setCodigo()	String	void	Permite poner el código
setDescripcion()	String	void	Permite poner el descripción
setUsuarioMOid()	Double	void	Permite poner el usuario que modifica
setUsuarioOid()	Double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
findAll()		Enumeration	Permite recuperar todos los vehículos
findByCodigo()	String	VehiculoBean	Permite recuperar un vehículo por el código

Nombre de Clase: ComisionVehiculoBean

Esta clase Representa a los diferentes ComisionVehiculo que permite enlazar Comisión y vehículo

Atributos	**Tipo**	**Descripción**
Comision_oid	Double	Representa a la relación con comisión
Vehiculo_oid	Double	Representa a la relación con vehículo

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
ComisionBean	Una ComisionVehiculo pertenece a una Comisión	getComision()	ComisionBean
VehiculoBean	Una ComisionVehiculo posee un vehículo	getVehiculo()	VehiculoBean

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**

Create	double	ComisionVehiculoBean	Permite crear una instancia de CartaAyudaBean a partir de dos valores, uno de Carta y otro de vehículo por medio del Oid
setComision	ComisionBean	void	Permite poner el identificador de comisión
setVehiculo	VehiculoBean	void	Permite poner el identificador de vehículo
getComision		ComisionBean	Permite extraer el identificador de comisión
getVehiculo		VehiculoBean	Permite extraer el identificador de vehículo

Nombre de Clase: ComisionResponsableBean

Esta clase Representa a los diferentes ComisionResponsable que permite enlazar Comisión y Responsable

Atributos	**Tipo**	**Descripción**
Comision_oid	Double	Representa la relación con comisión
Responsable_oid	Double	Representa la relación con responsable

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
ComisionBean	Un ComisionResponsable pertenece a una comision	getComision()	ComisionBean
ResponsableBean	Un ComisionResponsable posee un responsable	getResponsable()	ResponsableBean

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create	double	ComisionResponsableBean	Permite crear una instancia de ComisionResponsable Bean a partir de dos valores, uno de comisión y otro de responsable por medio del Oid
setComision	ComisionBean	Void	Permite poner el identificador de comisión
setResponsable	ResponsableBean	Void	Permite poner el identificador de vehículo
getComision		ComisionBean	Permite extraer el identificador de comisión

getResponsable		ResponsableBean	Permite extraer el identificador de Responsable

Nombre de Clase: **DetalleAvisoBean**

Esta clase Representa los detalles de avisos generados al efectuar algún cambio en una ayuda

Atributos	**Tipo**	**Descripción**
Oid	Double	Double
descripción	String	
latitud	double	
longitud	double	
provincia	String	
posicionLog	String	
posicionLat	String	
tipo	String	
Ayuda_Oid	Double	Representa la relación con ayuda
Aviso_Oid	Double	Representa la relación con aviso

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
AyudaBean	Un detalleAviso se encuentra en una ayuda	getAyuda()	AyudaBean
AvisoBean	Un detalleAviso solo corresponde aun aviso	getAviso()	AvisoBean

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create	BeanDetalleAviso	DetalleAvisoBean	Permite crear una instancia de DetalleAvisoBean a partir de un objeto liviano que proviene dela clase BeanDetalleAviso
getDescripcion()		String	Permite recuperar la descripción
get latitud()		double	Permite recuperar la latitud de la ayuda
get longitud()		double	Permite recuperar la longitud de la ayuda
getNombre()		String	Permite recuperar el nombre

getPosicionLat()		String	Permite recuperar la posición de la latitud
getPosicionLog()		String	Permite recuperar la posición de la longitud
getProvincia()		String	Permite recuperar el nombre de la provincia
getTipo()		String	El tipo de detalle que genera el aviso
setDescripcion()	String	void	Permite poner la descripción
set latitud()	double	void	Permite poner la latitud de la ayuda
set longitud()	double	void	Permite poner la longitud de la ayuda
setNombre()	String	void	Permite poner el nombre
setPosicionLat()	String	void	Permite poner la posición de la latitud
setPosicionLog()	String	void	Permite poner la posición de la longitud
setProvincia()	String	Void	Permite poner el nombre de la provincia
setTipo()	String	Void	El tipo de detalle que genera el aviso

Subclase:
Superclase

Nombre de Clase: **UsuarioBean**

Esta clase Representa a todos los usuarios de las ayudas y del sistema.

Atributos	**Tipo**	**Descripción**
oid	Double	identificador único para los objetos
apellido	String	
cargo	String	
nombre	String	
numeroIdentificacion	String	
tipoIdentificacion	String	
titulo	String	
usuarioMOid	Double	oid del último usuario que modifico el usuario
usuarioOid	Double	oid del usuario que creo el usuario
fechaUsuarioM	Timestamp	fecha de la última modificación del usuario
fechaUsuario	Timestamp	fecha de creación del usuario

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**

Subclase • ResponsableBean • UsuarioAyudaBean • usuarioResponsableBean
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
getApellido()		String	Permite recupera el apellido
getCargo()		String	Permite recuperar el cargo
getNombre()		String	Permite recupera el nombre
getNumeroIdentificacion( )		String	Permite recuperar el numero de la identificación
getTipoIdentificacion()		String	Permite recuperar el tipo de la identificación
getTitulo()		String	Permite recupera el titulo
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setApellido()	String	void	Permite poner el apellido
setCargo()	String	void	Permite poner el cargo
setNombre()	String	void	Permite poner el nombre
setNumeroIdentificacion( )	String	void	Permite poner el numero de la identificación
setTipoIdentificacion()	String	void	Permite poner el tipo de la identificación
setTitulo()	String	void	Permite poner el titulo
setUsuarioMOid()	double	void	Permite poner el usuario que modifica
setUsuarioOid()	double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación

Nombre de Clase: **UsuarioReporteBean**

Esta clase Representa a todos los usuarios a los que se les enviara información sobre las ayudas de las ayudas y del sistema.

Atributos	Tipo	Descripción
email	String	
fax	String	
pin	String	
servicio	String	
tipoBeeper	String	

Clase Relacionada	Tipo de Relación	método	Tipo Devuelto

Subclase
Superclase • usuarioBean

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
getEmail()		String	Permite recuperar el email
getFax()		String	Permite recuperar el numero de fax
getPin()		String	Permite recuperar el numero de pin
getServicio()		String	Permite recuperar el tipo de servicio
getTipoBeeper()		String	Permite recuperar la dirección del beeper
setEmail()		String	Permite poner el email
setFax()		String	Permite poner el numero de fax
setPin()	String	void	Permite poner el numero de pin
setServicio()	String	void	Permite poner el tipo de servicio
setTipoBeeper()	String	void	Permite poner la dirección del beeper
create	Bean usuarioReporte	usuarioReporteBean	Permite crear una instancia de usuarioReporteBean a partir de un objeto liviano que proviene de la clase Bean usuarioReporte

findAll()		Enumeration	Permite recuperar todos los usuarioReporte
findByIdentificacion()	String	usuarioReporte	Permite recuperar todos los usuarioReporte por el numero de identificación

Nombre de Clase: UsuarioAyudaBean

Esta clase Representa a todos los usuarios que pueden crear y modificar información sobre las ayudas y demás.

Atributos	**Tipo**	**Descripción**
password	String	Contiene el password del usuario para el ingreso
user	String	Contiene el usuario con que se identificara a la persona

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**

Subclase
Superclase • usuarioBean

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
getPassword()		String	Permite recuperar el password
getUser()		String	Permite recuperar el usuario con que se identifica a la persona
setPassword()	String	void	Permite poner el password
setUser()	String	void	Permite poner el usuario con que se identifica a la persona
create	BeanUsuarioAyuda	UsuarioAyudaBean	Permite crear una instancia de usuarioAyudaBean a partir de un objeto liviano que proviene de la clase BeanUsuarioAyuda
findAll()		Enumeration	Permite recuperar todos los usuarioAyuda

findByIdentificacion()	String	usuarioAyuda	Permite recuperar todos los usuarioAyuda por el numero de identificación
findByUserAndPassword()	String	usuarioAyuda	Permite recuperar todos los usuarioAyuda por el user y el password

Nombre de Clase: UsuarioResponsableBean

Esta clase Representa a todos los usuarios que se asignan para reparaciones de las ayudas.

Atributos	**Tipo**	**Descripción**

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
ComisionResponsableBean	Un usuarioReponsable se encuentra en muchas ComisionReponsable	getComisionResponsable()	Enumeration

Subclase
Superclase • usuarioBean

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
create	BeanResponsable	ResponsableBean	Permite crear una instancia de ResponsableBean a partir de un objeto liviano que proviene de la clase BeanResponsable
findAll()		Enumeration	Permite recuperar todos los usuarioResponsable
findByIdentificacion()	String	usuarioAyuda	Permite recuperar todos los usuarioResponsable por el numero de identificación

Nombre de Clase: **RepartoBean**

Esta clase Representa a todos los repartos que existen.

Atributos	Tipo	Descripción
oid	Double	identificador único para los objetos
descripcion	String	
estado	String	
nombre	String	
numeroIdentificacion	String	
razón	String	
siglas	String	
tipoIdentificacion	String	
email	String	
fax	String	
pin	String	
servicio	String	
tipoBeeper	String	
usuarioMOid	Double	oid del último usuario que modifico el reparto
usuarioOid	Double	oid del usuario que creo el reparto
fechaUsuarioM	Timestamp	fecha de la última modificación del reparto
fechaUsuario	Timestamp	fecha de creación del reparto

Clase Relacionada	Tipo de Relación	método	Tipo Devuelto
AvisoBean	Un reparto puede reportar muchos avisos	getAviso()	Enumeratión

Subclase
Superclase

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
getDescripción()		String	Permite recuperar la descripción
getEstado()		String	Permite recuperar el estado
getNombre()		String	Permite recuperar el nombre
getNumeroIdentificacion()		String	Permite recuperar el numero de la identificación
getRazon()		String	Permite recuperar la razón
getSigla()		String	Permite recuperar la sigla
getTipoIdentificacion()		String	Permite recuperar el tipo de la identificación

getEmail()		String	Permite recuperar el email
getFax()		String	Permite recuperar el numero de fax
getPin()		String	Permite recuperar el numero de pin
getServicio()		String	Permite recuperar el tipo de servicio
getTipoBeeper()		String	Permite recuperar la dirección del beeper
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setDescripción()	String	void	Permite poner la descripción
setEstado()	String	void	Permite poner el estado
setNombre()	String	void	Permite poner el nombre
setNumeroIdentificacion()	String	void	Permite poner el numero de la identificación
setRazon()	String	void	Permite poner la razón
setSigla()	String	void	Permite poner la sigla
setTipoIdentificacion()	String	void	Permite poner el tipo de la identificación
setEmail()	String	void	Permite poner el email
setFax()	String	void	Permite poner el numero de fax
setPin()	String	void	Permite poner el numero de pin
setServicio()	String	void	Permite poner el tipo de servicio
setTipoBeeper()	String	void	Permite poner la dirección del beeper
setUsuarioMOid()	Double	void	Permite poner el usuario que modifica
setUsuarioOid()	Double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación
setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
create()	BeanReparto	RepartoBean	Permite crear una instancia de RepartoBean a partir de un objeto liviano que proviene de la clase BeanReparto
findAllMail()		Enumeration	Permite recuperar todos los Repartos con su email

findAll()		Enumeration	Permite recuperar todos los Repartos
findByNumeroIdentificacion()	String	usuarioReporte	Permite recuperar todos los Repartos por el numero de identificación

Nombre de Clase: **AvisoBean**

Esta clase Representa a todos los Avisos que se generan por las ayudas.

Atributos	**Tipo**	**Descripción**
oid	Double	identificador único para los objetos
descripcion	String	
estado	String	
mensaje	String	
numero	String	
publicacionAfectada	String	
tipo	String	
repartoOid	Double	
listaFaroBoya	String	
derroteroEcuador	String	
enviado	String	
anula_oid	Double	Representa la relación con un Aviso Anulado
reparto_oid	Double	Representa la relación con el Reparto
usuarioMOid	Double	oid del último usuario que modifico el aviso
usuarioOid	Double	oid del usuario que creo el aviso
fechaUsuarioM	Timestamp	fecha de la última modificación del aviso
fechaUsuario	Timestamp	fecha de creación del aviso

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
AvisoBean	Un aviso pude anular a otro aviso	getAnulaOid()	Double
ComisionBean	un aviso puede generar una comisión	getComision()	ComisionBean
DetalleAvisoBean	Un aviso contiene muchos detalles de aviso	getDetalleAviso()	Enumeration
CartaAvisoBean	Un Aviso puede estar en muchas CartaAvios	getCartaAviso()	Enumeration
RepartoBean	Un Aviso puede ser generado por un reparto	getReparto()	RepartoBean

Subclase
Superclase

Métodos	Tipo parámetro	Tipo Devuelto	Descripción
getDerroteroEcuador()		String	Indica si el aviso afecta a la lista de Derrotero del Ecuador
getDescripcion()		String	Permite recuperar la descripción
getDetaleAviso()		String	Permite recuperar el detalle
getEnviado()		String	Permite recuperar si fue enviado o no
getEstado()		String	Permite recuperar el estado
getFecha()		String	Permite recuperar la fecha
getListaFaroBoya()		String	Indica si el aviso afecta a la lista de faros y boyas
getMensaje()		String	Permite recuperar el mensaje
getNumero()		String	Permite recuperar el número de aviso
getPublicacionAfectada()		String	Permite recuperar la publicación que afecta
getTipo()		String	Permite recuperar el tipo
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setDerroteroEcuador()	String	void	Permite poner derrotero Ecuador
setDescripcion()	String	void	Permite poner la descripción
setDetaleAviso()	String	void	Permite poner el detalle
setEnviado()	String	void	Permite poner si fue enviado o no
setEstado()	String	void	Permite poner el estado
setFecha()	String	void	Permite poner la fecha
setListaFaroBoya()	String	void	Permite poner el lista faro boyas
setMensaje()	String	void	Permite poner el mensaje
setNumero()	String	void	Permite poner el número de aviso
setPublicacionAfectada()	String	void	Permite poner la publicación que afecta
setTipo()	String	void	Permite poner el tipo
setUsuarioMOid()	Double	void	Permite poner el usuario que modifica
setUsuarioOid()	Double	void	Permite poner el usuario que crea
setFechaUsuarioM()	Timestamp	void	Permite poner la fecha de Modificación

setFechaUsuario()	Timestamp	void	Permite poner la fecha de creación
create()	BeanAviso	AvisoBean	Permite crear una instancia de AvisoBean a partir de un objeto liviano que proviene de la clase BeanAviso
findAll ()		Enumeration	Permite recuperar todos los Avisos
findAvisoPorNumero()	String	AvisoBean	Permite recuperar todos los Avisos
findAvisoPorEnviar ()		Enumeration	Permite recuperar todos los avisos para enviar
findAvisosVigentes()		Enumeration	Permite recuperar todos los avisos vigentes

Nombre de Clase: **ComisionBean**

Esta clase Representa a todos las comisiones que se generan para las ayudas

Atributos	**Tipo**	**Descripción**
oid	Double	identificador único para los objetos
materiales	String	
numeroReferencia	String	
estado	String	
fechaRetorno	String	
fechaSalida	String	
Aviso_oid	Double	Representa la relación con aviso
usuarioMOid	Double	oid del último usuario que modifico la comisión
usuarioOid	Double	oid del usuario que creo la comisión
fechaUsuarioM	Timestamp	fecha de la última modificación la comisión
fechaUsuario	Timestamp	fecha de creación de la comisión

Clase Relacionada	**Tipo de Relación**	**método**	**Tipo Devuelto**
ComisionVehiculoBean	Una comisión puede tener asignado muchas ComisionVehiculo	getComisionResponsable ()	Enumeration
ComisionResponsableBean	Una comisión tiene asignados muchos ComisionResponsable	getComisionVehiculo()	Enumeration
AvisoBean	Una comisión puede estar o no relacionada con un aviso	getAviso()	AvisoBean

ReporteBean	Una comisión puede realizar varios reportes	getReporte()	Enumeration

Subclase
Superclase

Métodos	**Tipo parámetro**	**Tipo Devuelto**	**Descripción**
getEstado()		String	Permite recuperar el estado
getFechaRetorno()		String	Permite recuperar la fecha de retorno
getFechaSalida()		String	Permite recuperar la fecha de Salida
getMateriales()		String	Permite recuperar el detalle de materiales
getNumeroReferencia()		String	Permite recuperar el número de referencia
getUsuarioMOid()		double	Permite recuperar el usuario que modifica
getUsuarioOid()		double	Permite recuperar el usuario que crea
getFechaUsuarioM ()		Timestamp	Permite recuperar la fecha de la última modificación
getFechaUsuario ()		Timestamp	Permite recuperar la fecha de creación
setEstado()	String	void	Permite poner el estado
setFechaRetorno()	String	void	Permite poner la fecha de retorno
setFechaSalida()	String	void	Permite poner la fecha de Salida
setMateriales()	String	void	Permite poner el detalle de materiales
setNumeroReferencia()	String	void	Permite poner el número de referecia
setUsuarioMOid()	double	void	Permite poner el usuario que modifica
getUsuarioOid()	double	void	Permite recuperar el usuario que crea
create	BeanAviso	ComisionBean	Permite crear una instancia de ComisonBean a partir de un objeto liviano que proviene de la clase BeanComision
findAll ()		Enumeration	Permite recuperar todas las Comisiones

5. Mapeo del Modelo de la Base de Datos

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANPROVINCIA			**ProvinciaBean**		
	oid	double		oid	double
	LatitudMáxima	Double		latitud Máxima	Double
	LatitudMínima	Double		latitud Mínima	Double
	longitudMáxima	Double		longitudMáxima	Double
	longitud Mínima	Double		longitud Mínima	Double
	código	Varchar(30)		código	String
	nombre	Varchar(30)		nombre	String
	descripción	Varchar(300)		descripción	String
	sigla	Varchar(30)		sigla	String
	posiciónLatMáx	Varchar(30)		posiciónLatMáx	String
	posiciónLatMín	Varchar(30)		posiciónLatMín	String
	posiciónLogMáx	Varchar(30)		posiciónLogMáx	String
	posiciónLogMín	Varchar(30)		posiciónLogMín	String
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	Double		usuarioMOid	Double
	usuarioOid	Double		usuarioOid	Double

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANSECTOR			SectorBean		
	oid	double		oid	double
	código	Varchar(30)		código	String
	nombre	Varchar(100)		nombre	String
	provincia_oid	Double		provincia_oid	Double
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	double		usuarioMOid	double
	usuarioOid	double		usuarioOid	double

Nombre de Tabla	Columnas		Clase	Atributo	
ANAYUDA			AyudaBean		
	oid	double		oid	double
	alcanceGeografico	double		alcanceGeografico	double
	alcanceNominal	double		alcanceNominal	double
	alturaFisica	double		alturaFisica	double
	alturaNivelMar	double		alturaNivelMar	double
	latitud	double		latitud	double
	Longitud	double		Longitud	double
	luminosidad	double		luminosidad	double
	Periodo	double		Periodo	double
	Veces	double		Veces	double
	anioConstruccion	Varchar(30)		anioConstruccion	String
	anioModificacion	Varchar(30)		anioModificacion	String
	anioUltimaModificacion	Varchar(30)		anioUltimaModificacion	String
	descripción	Varchar(300)		descripción	String
	Nombre	Varchar(30)		Nombre	String
	NoOrdenNacional	Varchar(30)		NoOrdenNacional	String
	NoOrdenInternacional	Varchar(30)		NoOrdenInternacional	String
	observación	Varchar(300)		observación	String
	Color	Varchar(30)		Color	String
	posicionLog	Varchar(30)		posicionLog	String
	posicionLat	Varchar(30)		posicionLat	String
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	Double		usuarioMOid	double
	usuarioOid	Double		usuarioOid	double
	sectorOid	Varchar(30)		sectorOid	String

Nombre de Tabla	Columnas		Clase	Atributo	
ANCARTAAYUDA			CartaAyudaBean		
	Ayuda_oid	Double		Ayuda_oid	Double
	Carta_oid	Double		Carta_oid	Double

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANREPORTE			ReporteBean		
	oid	double		oid	double
	trabajoRealizada	Varchar(500)		trabajoRealizada	String
	descripcionTrabajo	Varchar(500)		descripcionTrabajo	String
	novedadesSolución	Varchar(500)		novedadesSolución	String
	fecha	Date		fecha	Date
	ayuda_oid	Double		ayuda_oid	Double
	comision_oid	Double		comision_oid	Double
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	Double		usuarioMOid	Double
	usuarioOid	Double		usuarioOid	Double

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANCARTA			CartaBean		
	oid	double		oid	double
	latitud Máxima	Double		latitud Máxima	Double
	latitud Mínima	Double		latitud Mínima	Double
	longitudMáxima	Double		longitud Máxima	Double
	longitud Mínima	Double		longitud Mínima	Double
	código	Varchar(30)		código	String
	nombre	Varchar(100)		nombre	String
	posiciónLatMáx	Varchar(30)		posiciónLatMáx	String
	posiciónLatMín	Varchar(30)		posiciónLatMín	String
	posiciónLogMáx	Varchar(30)		posiciónLogMáx	String
	posiciónLogMín	Varchar(30)		posiciónLogMín	String
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	Double		usuarioMOid	Double
	usuarioOid	Double		usuarioOid	Double

Nombre de Tabla	Columnas		Clase	Atributo	
ANOIDKEEPER			OidKeeperBean		
	oid	double		oid	double
	nombre	Varchar(30)		nombre	String

Nombre de Tabla	Columnas		Clase	Atributo	
ANVEHICULO			VehiculoBean		
	oid	double		oid	double
	código	Varchar(30)		código	String
	descripción	Varchar(100)		descripción	String
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	double		usuarioMOid	double
	usuarioOid	double		usuarioOid	double

Nombre de Tabla	Columnas		Clase	Atributo	
ANCOMISIONVEHICULO			ComisionVehiculoBean		
	Comision_oid	Double		Comision_oid	Double
	Vehiculo_oid	Double		Vehiculo_oid	Double

Nombre de Tabla	Columnas		Clase	Atributo	
ANCOMISIONRESPONSABLEBEAN			ComisionResponsableBean		
	Comision_oid	Double		Comision_oid	Double
	Responsable_oid	Double		Responsable_oid	Double

Nombre de Tabla	Columnas		Clase	Atributo	
ANCOMISION			ComisionBean		
	oid	double		oid	double
	materiales	Varchar(100)		materiales	String
	numero	Varchar(30)		numero	String

	referencia	Varchar(30)		referencia	String
	estado	Varchar(30)		estado	String
	fechaRetorno	Varchar(30)		fechaRetorno	String
	fechaSalida	Varchar(30)		fechaSalida	String
	Aviso_oid	Double		Aviso_oid	Double
	usuarioMOid	double		usuarioMOid	double
	usuarioOid	double		usuarioOid	double
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANDETAAVIS			DetalleAvisoBean		
	oid	Double		oid	double
	Descripción	Varchar(100)		Descripción	String
	latitud	Double		latitud	Double
	longitud	Double		longitud	Double
	nombre	Varchar(100)		nombre	String
	provincia	Varchar(150)		provincia	String
	posicionLog	Varchar(30)		posicionLog	String
	posicionLat	Varchar(30)		posicionLat	String
	tipo	Varchar(30)		tipo	String
	Ayuda_oid	Double		Ayuda_oid	Double
	Aviso_oid	Double		Aviso_oid	Double
	fechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	fechaUsuario	Timestamp		fechaUsuario	Timestamp
	usuarioMOid	Double		usuarioMOid	Double
	usuarioOid	Double		usuarioOid	Double
	Ayuda_Oid	Double		Ayuda_Oid	Double
	Aviso_Oid	Double		Aviso_Oid	Double

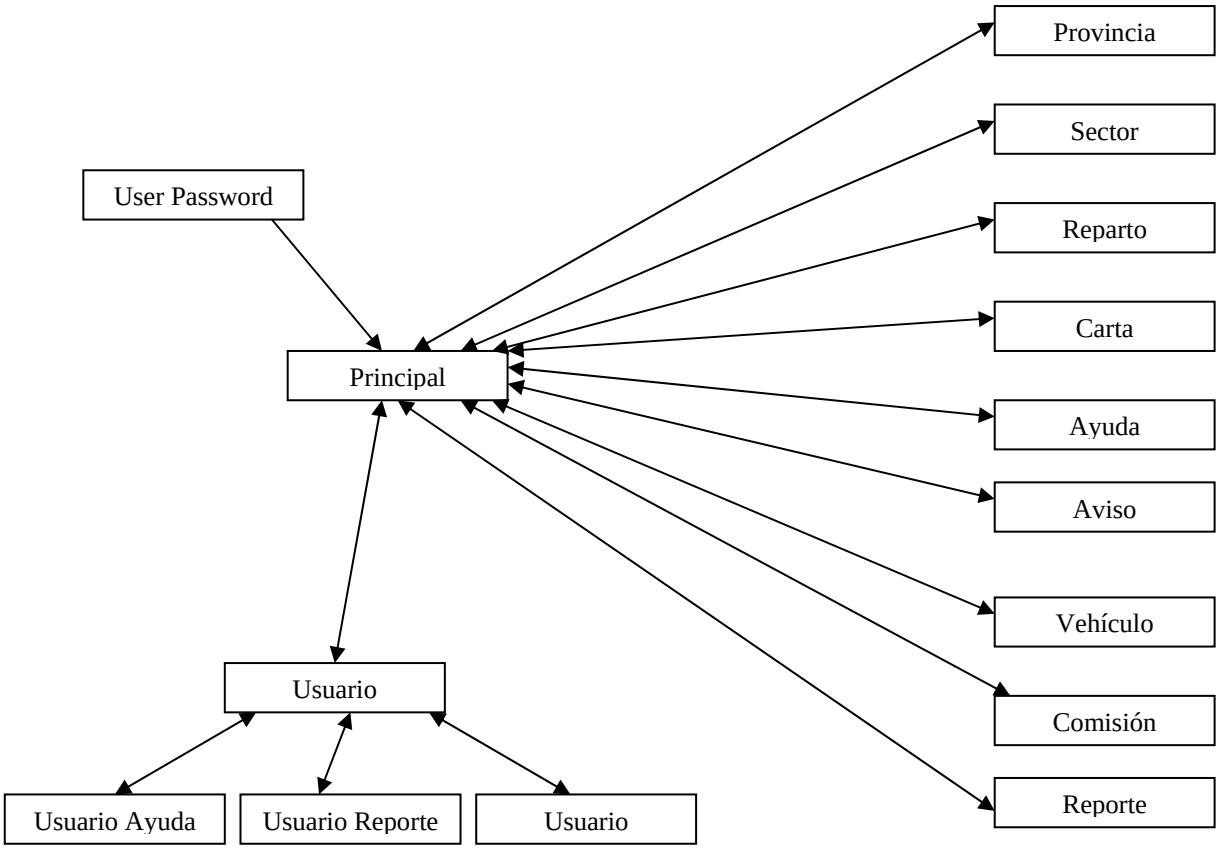
Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANREPARTO			RepartoBean		
	oid	DOUBLE		oid	double
	descripcion	Varchar(300)		descripcion	String
	estado	Varchar(30)		estado	String
	nombre	Varchar(100)		nombre	String

	numeroIdentificacion	Varchar(30)		numeroIdentificacion	String
	razón	Varchar(30)		razón	String
	siglas	Varchar(30)		siglas	String
	tipoIdentificacion	Varchar(30)		tipoIdentificacion	String
	email	Varchar(30)		email	String
	fax	Varchar(30)		fax	String
	pin	Varchar(30)		pin	String
	servicio	Varchar(30)		servicio	String
	TipoBeeper	Varchar(30)		tipoBeeper	String
	FechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	FechaUsuario	Timestamp		fechaUsuario	Timestamp
	UsuarioMOid	double		usuarioMOid	double
	UsuarioOid	double		usuarioOid	double

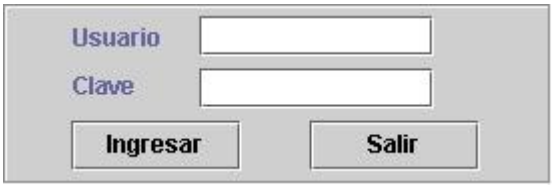
Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANUSUARIO			usuarioBean		
	oid	double		oid	double
	Apellido	Varchar(30)		apellido	String
	Cargo	Varchar(30)		cargo	String
	Nombre	Varchar(30)		nombre	String
	NumeroIdentificacion	Varchar(30)		numeroIdentificacion	String
	TipoIdentificacion	Varchar(30)		tipoIdentificacion	String
	Titulo	Varchar(30)		titulo	String
	Email	Varchar(30)		email	String
	Fax	Varchar(30)		fax	String
	Pin	Varchar(30)		pin	String
	Servicio	Varchar(30)		servicio	String
	TipoBeeper	Varchar(30)		tipoBeeper	String
	Password	Varchar(30)		password	String
	User	Varchar(30)		user	String
	FechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	FechaUsuario	Timestamp		fechaUsuario	Timestamp
	UsuarioMOid	Double		usuarioMOid	Double
	UsuarioOid	Double		usuarioOid	Double

Nombre de Tabla	**Columnas**		**Clase**	**Atributo**	
ANAVISOBEAN			AvisoBean		
	oid	double		oid	double
	Descripcion	Varchar(100)		descripcion	String
	Estado	Varchar(30)		estado	String
	Mensaje	Varchar(500)		mensaje	String
	Numero	Varchar(30)		numero	String
	PublicacionAfectada	Varchar(30)		publicacionAfectada	String
	Tipo	Varchar(30)		tipo	String
	RepartoOid	double		repartoOid	double
	ListaFaroBoya	Varchar(30)		listaFaroBoya	String
	DerroteroEcuador	Varchar(30)		derroteroEcuador	String
	Enviado	Varchar(30)		enviado	String
	anula_oid	double		anula_oid	double
	reparto_oid	double		reparto_oid	double
	UsuarioMOid	double		usuarioMOid	double
	UsuarioOid	double		usuarioOid	double
	FechaUsuarioM	Timestamp		fechaUsuarioM	Timestamp
	FechaUsuario	Timestamp		fechaUsuario	Timestamp

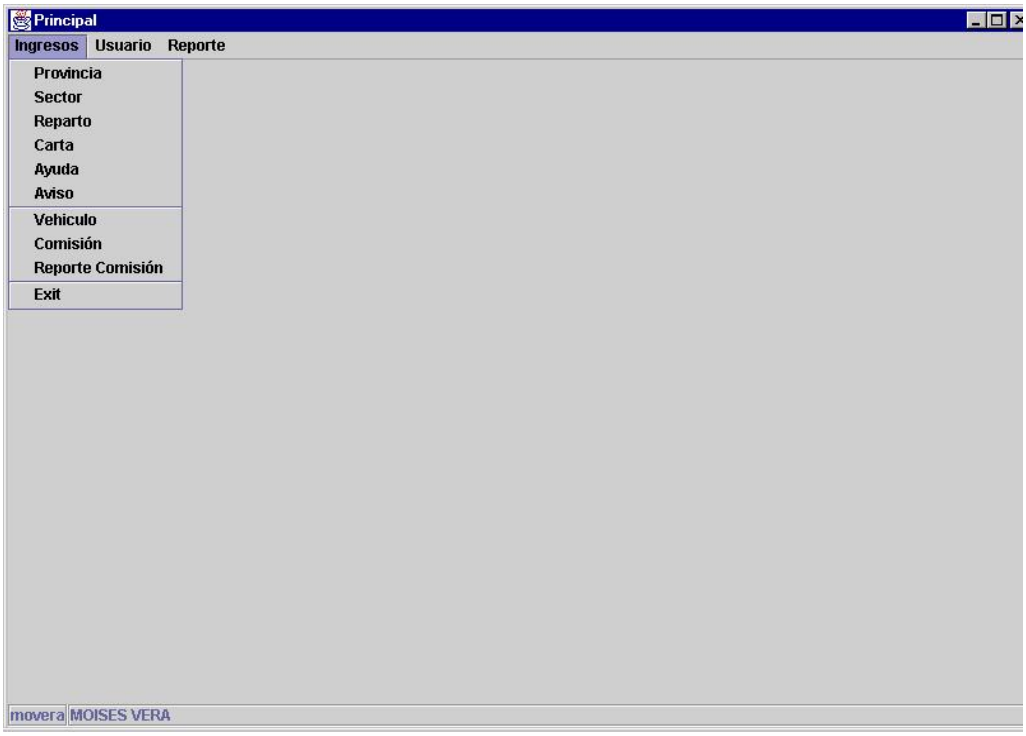
6. Flujo de Ventanas y Layout



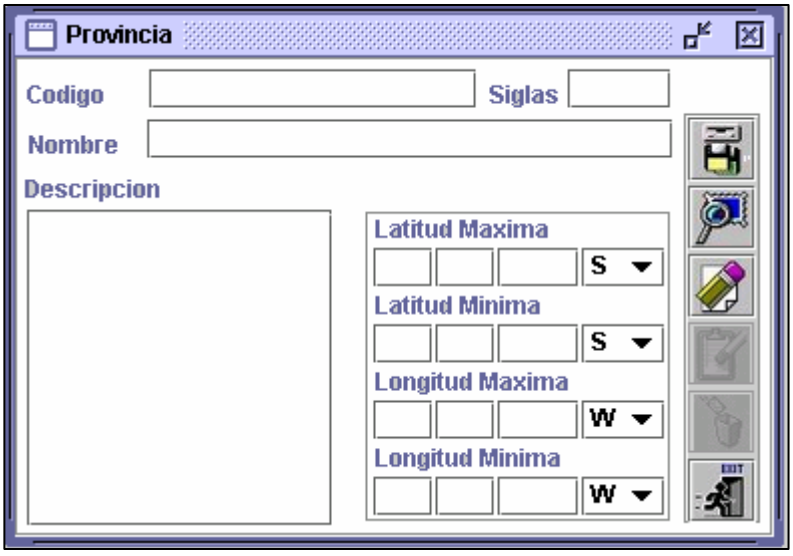
UserPassword



Principal

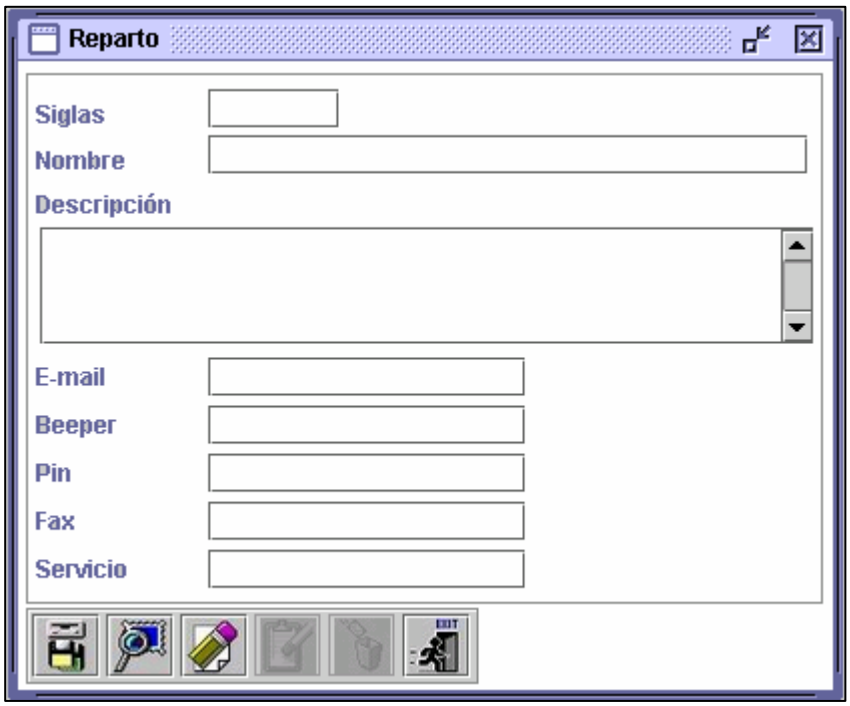


Provincia

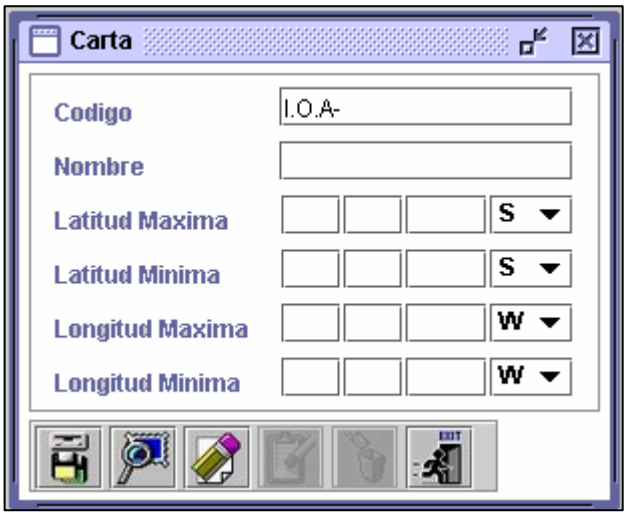


Sector

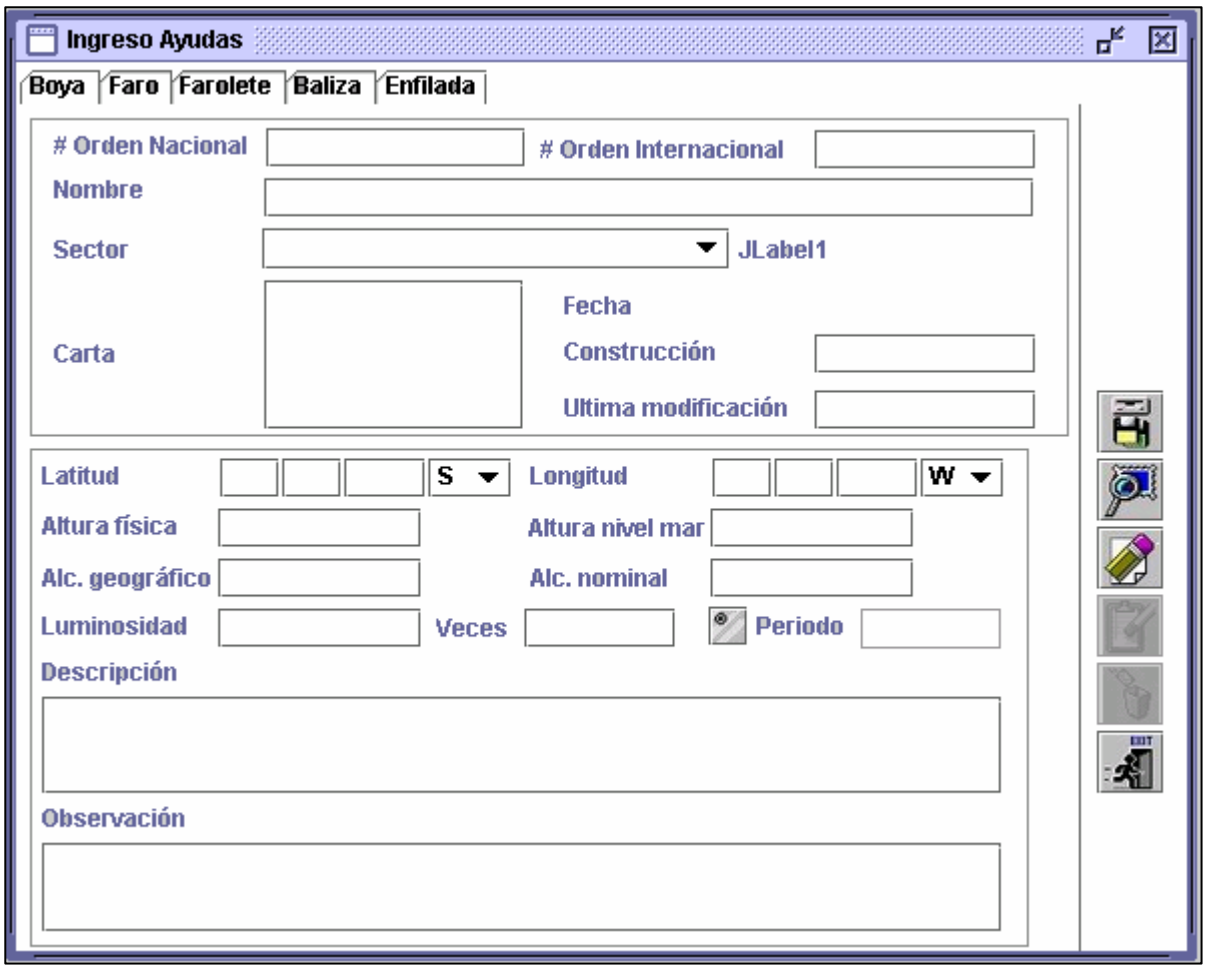
Reparto



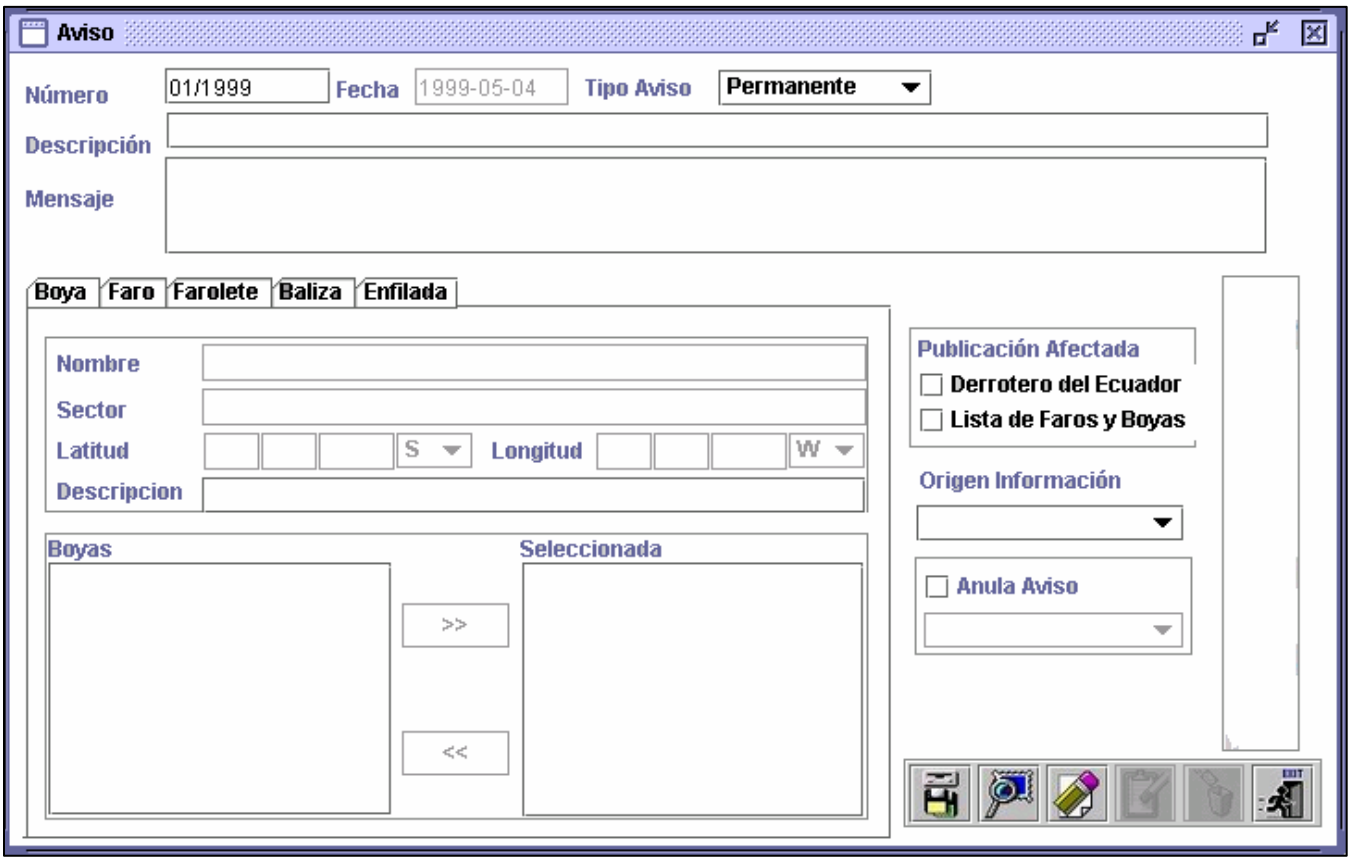
Carta



Ayuda

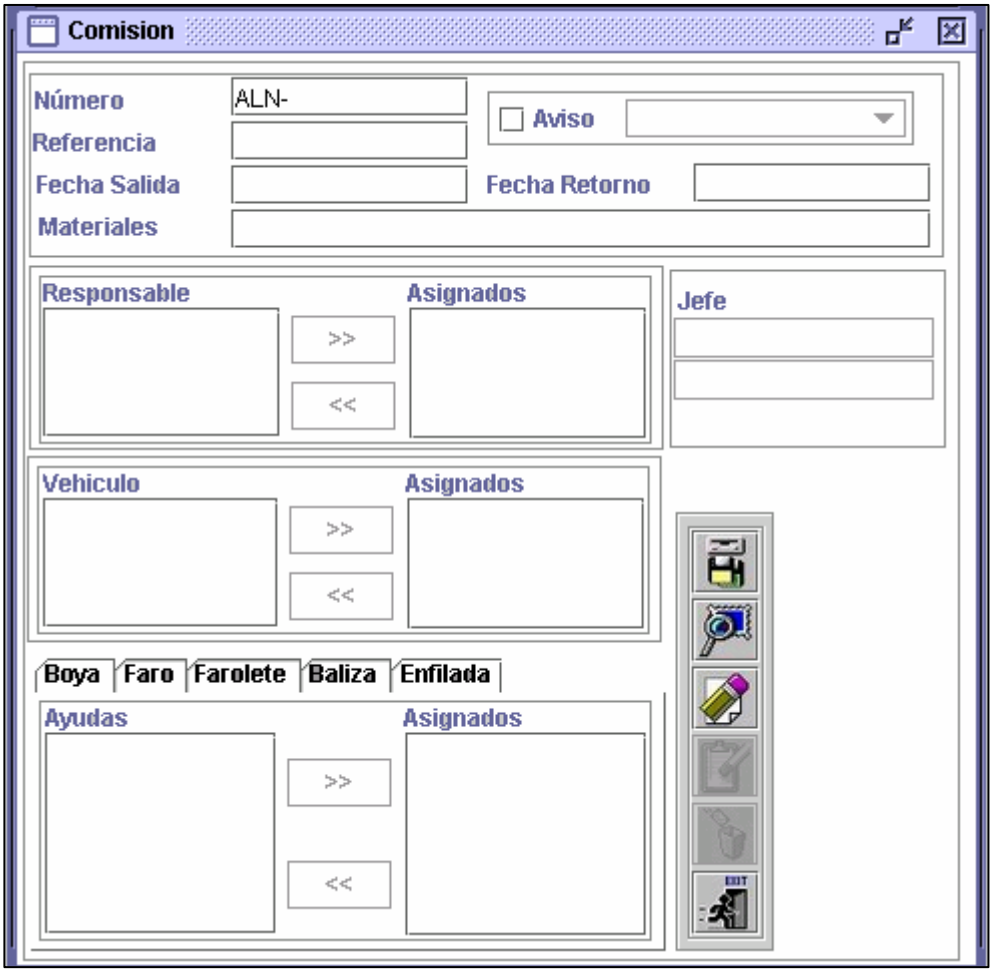

Ingreso Ayudas
Boya
Faro
Farolete
Baliza
Enfilada
Orden Nacional
Orden Internacional
Nombre
Sector
JLabel1
Carta
Fecha
Construcción
Ultima modificación
Latitud
S
Longitud
W
Altura física
Altura nivel mar
Alc. geográfico
Alc. nominal
Luminosidad
Veces
Periodo
Descripción
Observación

Aviso

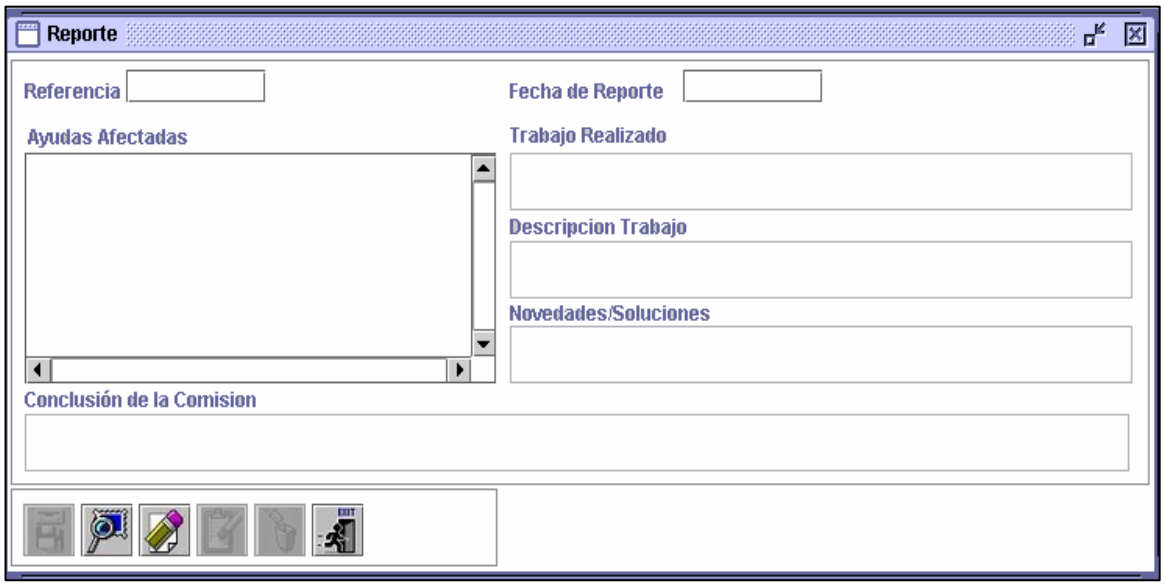


Vehículo

Comisión


Comision
Número
ALN-
Referencia
Aviso
Fecha Salida
Fecha Retorno
Materiales
Responsable
Asignados
Jefe
Vehiculo
Asignados
Boya
Faro
Farolete
Baliza
Enfilada
Ayudas
Asignados
>>
<<

Reporte



Reporte de Avisos Diarios

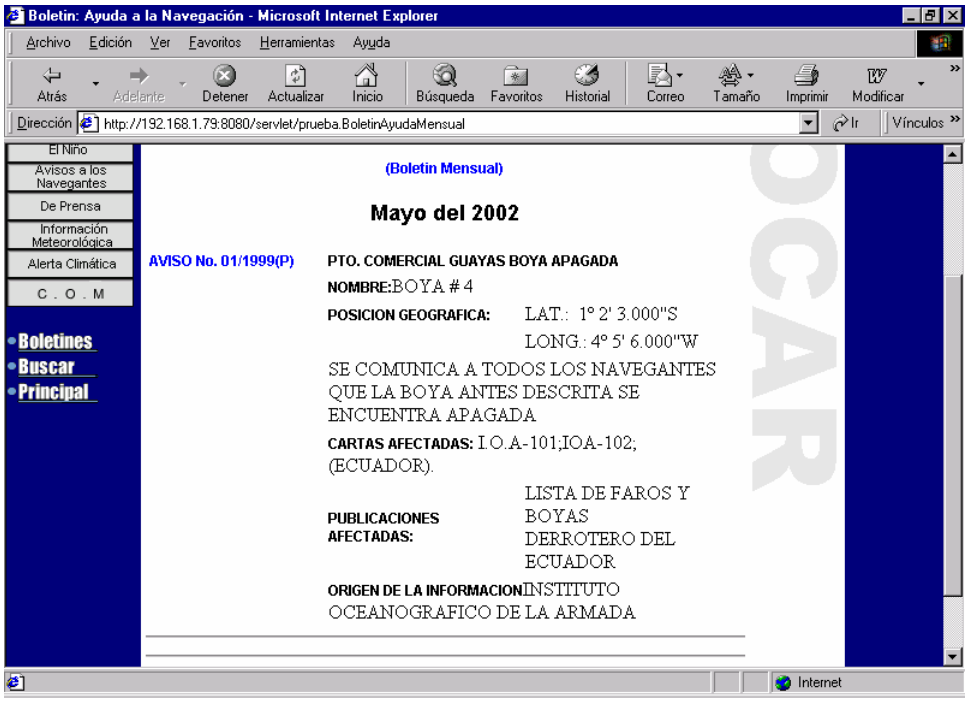
Boletines: Avisos a los Navegantes:Ayudas a la Navegación

(Avisos Diarios)

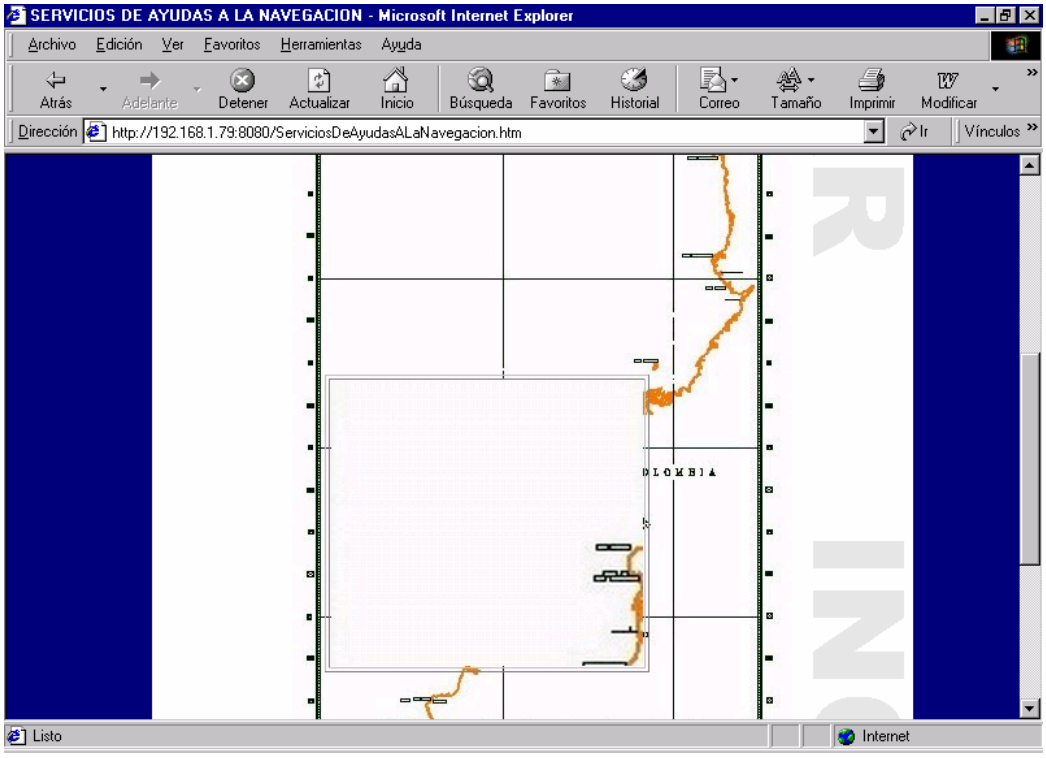
04 de Mayo del 2002

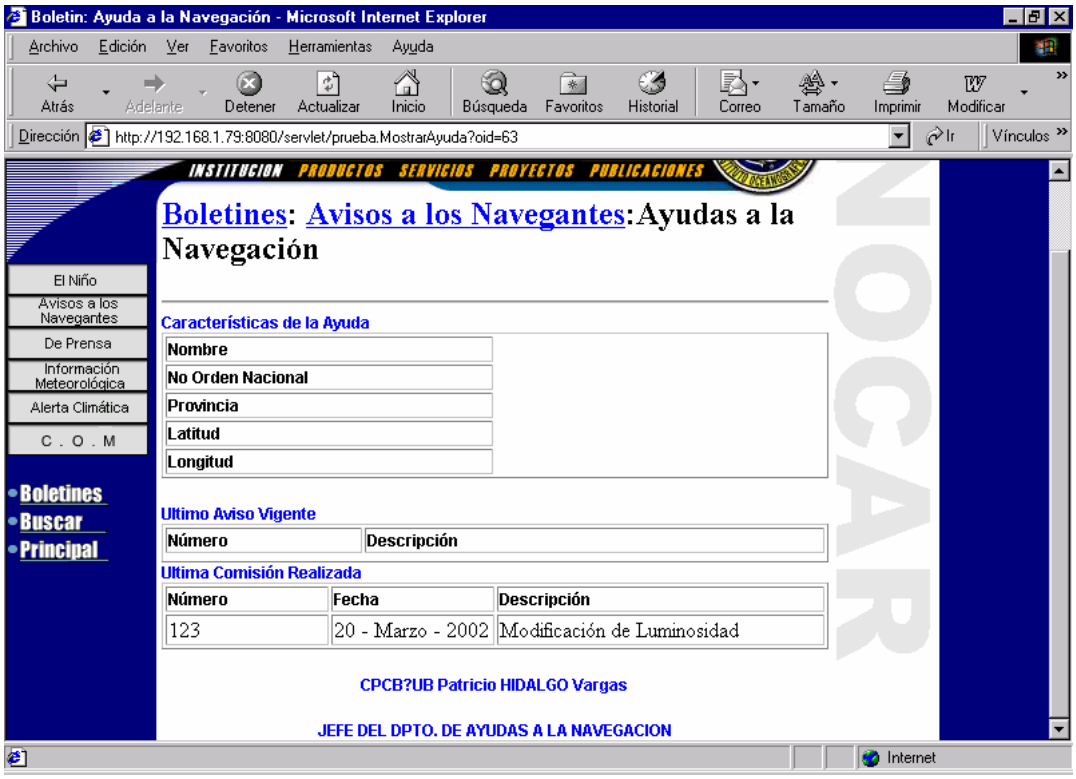
Tipo de Avisos	PROVINCIAS SITIO	AYUDAS	POSICION GEOGRAFICA		NOVEDAD	CARTAS Y PUBLICACIONES AFECTADAS
			LATITUD	LONGITUD		
(P.)	PTO. COMERCIAL-GUAYAS	BOYA # 4	1° 2' 3.000"S	4° 5' 6.000"W	BOYA APAGADA	I.O.A-101;IOA-102; (Ecuador)

Reporte de Avisos Mensual



Reporte de Ayudas





7. Plan de Pruebas

Usuarios de Ayudas

Creación de Usuarios de Ayudas

Se de desea crear el Usuario de Ayuda con las siguientes características:
Numero de cédula: 0914201015
Nombre : PEDRO
Apellido: SILVA
Titulo: EMCI.
Cargo: PUBLICACION DE AVISOS
User : psilva
Password: psilva

Configuración del sistema:
El usuario deberá hacer un click en el menú “Usuario” submenú “Usuario Ayuda”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Identificación	0914201015	15
Tipo de Identificación	CEDULA	
Nombre	PEDRO	30
Apellido	SILVA	30
Titulo	EMCI	30
Cargo	PUBLICACION DE AVISOS	30
User	Psilva	30
Password	Psilva	30

Búsqueda de Usuario de Ayuda

El usuario ingresara el numero de identificación y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Usuario Ayuda

Después de buscar el usuario el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Usuario Ayuda

Después de buscar el usuario el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Usuarios Comisión

Creación de Usuarios Comisión

Se de desea crear el Usuario de Comisión con las siguientes características:
Numero de cédula: 0910211015
Nombre : JOSE
Apellido: RODRIGUEZ
Titulo: EMCI.
Cargo: MANTENIMIENTO FAROS

Configuración del sistema:
El usuario deberá hacer un click en el menú “Usuario” submenú “Usuario Comisión”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Identificación	0910211015	15
Tipo de Identificación	CEDULA	
Nombre	JOSE	30
Apellido	RODRIGUEZ	30
Titulo	EMCI	30
Cargo	MANTENIMIENTO FAROS	30

Búsqueda de Usuario Comisión

El usuario ingresara el numero de identificación y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Usuario Comisión

Después de buscar el usuario el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Usuario Comisión

Después de buscar el usuario el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Usuarios Reportes

Creación de Usuarios Reporte

Se de desea crear el Usuario de Comisión con las siguientes características:
Numero de cédula: 0910211015
Nombre : MONICA
Apellido: VERA
Titulo: EMCI
Cargo: SECRETARIA
Email: movera@hotmail.com
Beeper:
Pin:
Fax: 2448879

Configuración del sistema:
El usuario deberá hacer un click en el menú “Usuario” submenú “Usuario Reporte”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Identificación	0910211015	15
Tipo de Identificación	CEDULA	
Nombre	MONICA	30
Apellido	VERA	30
Titulo	EMCI	30
Cargo	SECRETARIA	30
Email	movera@hotmail.com	30
Beeper		30
Pin		30
Fax	2448879	30

Búsqueda de Usuario Reporte

El usuario ingresara el numero de identificación y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Usuario Reporte

Después de buscar el usuario el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Usuario Reporte

Después de buscar el usuario el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Provincias

Creación de Provincia

Código: 001
Sigla: GY
Nombre: GUAYAS
Descripción: PROVINCIA DEL GUAYAS
Latitud máxima:1* 25’34.5’’ S
Latitud mínima: 0* 1’ 3.5’’ S
Longitud máxima: 78* 56’24.6’’W
Longitud mínima: 75* 5’4.6’’W

Configuración del sistema:
El usuario deberá hacer un click en el menú “Ingreso” submenú “Provincia”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Código	0910211015	15
Sigla	GY	15
Nombre	GUAYAS	30
Descripción	PROVINCIA DEL GUAYAS	100
Latitud máxima	1* 25’34.5’’ S	
Latitud mínima	0* 1’ 3.5’’ S	
Longitud maxima	78* 56’24.6’’W	
Longitud mínima	75* 5’4.6’’W	

Búsqueda de Provincia

El usuario ingresara el código y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Provincia

Después de buscar la provincia el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Provincia

Después de buscar la provincia el usuario procederá a eliminar la provincia después de presionar el botón eliminar

Sector

Creación de Sector

Código: 101
Nombre : PTO.PETROLERO DE LA LIBERTAD
Provincia: GUAYAS

Configuración del sistema:
El usuario deberá hacer un click en el menú “Ingreso” submenú “Sector”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Código	101	30
Nombre	PTO.PETROLERO DE LA LIBERTAD	50
Provincia	GUAYAS	

Búsqueda de Sector

El usuario ingresara el código y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Sector

Después de buscar el sector el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Sector

Después de buscar el sector el usuario procederá a eliminar el sector después de presionar el botón eliminar

Reparto

Creación de Reparto

Identificación: 1020365
Sigla : CAPUIL
Nombre: CAPITANIA DE GUAYAQUIL
Descripción CAPITANIA DEL PUERTO

Configuración del sistema:
El usuario deberá hacer un click en el menú “Ingreso” submenú “Reparto”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Identificación	1020365	15
Sigla	CAPUIL	10
Nombre	CAPITANIA DE GUAYAQUIL	50
Descripción	CAPITANIA DEL PUERTO	300

Búsqueda de Reparto

El usuario ingresara el numero de identificación y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Reparto

Después de buscar el reparto el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Reparto

Después de buscar el reparto el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Carta

Creación de Carta

Código : I.O.A.105
Nombre : CARTA IOA105
Latitud máxima:1* 25’34.5’’ S
Latitud mínima: 0* 1’ 3.5’’ S
Longitud máxima: 78* 56’24.6’’W
Longitud mínima: 75* 5’4.6’’W

Configuración del sistema:
El usuario deberá hacer un click en el menú “Ingreso” submenú “Carta”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Código	I.O.A.105	15
Nombre	CARTA IOA105	30
Latitud máxima	1* 25’34.5’’ S	
Latitud mínima	0* 1’ 3.5’’ S	
Longitud máxima	78* 56’24.6’’W	
Longitud mínima	75* 5’4.6’’W	

Búsqueda de Carta

El usuario ingresara el código y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Carta

Después de buscar la carta el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Carta

Después de buscar la carta el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Vehículo

Creación de Vehículo

Código: ARE-1020
Descripción: CAMIONETA LUV(50)

Configuración del sistema:
El usuario deberá hacer un click en el menú “Ingreso” submenú “Vehículo”

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Código	ARE-1020	15
Descripción	CAMIONETA LUV	50

Búsqueda de Vehículo

El usuario ingresara el código y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Modificación de Vehículo

Después de buscar el vehículo el usuario procederá a modificar los datos después de presionar el botón modificar

Eliminación de Vehículo

Después de buscar el vehículo el usuario procederá a eliminar el usuario después de presionar el botón eliminar

Ayuda
Creación de Ayuda

Numero de Orden Nacional: 1063
Numero de Orden Internacional: G-3058
Nombre: Boya Juan Bautista
Año: 1977
Modificación: 1986
Latitud: 2º12'30''
Longitud: 80º54'3.6''
Altura al nivel del mar: 4
Altura física: 4
Descripción: LINTERNA ELECTRICA SOBRE ESTRUCTURA CILINDRICA METALICA CON FRANJAS HORIZONTALES COLOR ROJO Y NEGRAS
Observación: AINW DEL BUQUE HUNDIDO
Alcance Nominal: 4
Alcance Geográfico: 7
Grupo D(2):
Des 1.0s
Ecl. 2.0s
Des 1.0s
Ecl 6.0s
Periodo 10
Luminosidad: 45 Cd.

Configuración del sistema:
El usuario deberá hacer un click en el menú "Ingreso" submenú "Ayuda"

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Numero de Orden Nacional	1063	15
Numero de Orden Internacional	G-3058	15
Nombre	Boya Juan Bautista	50
Año	1977	4
Modificación	1986	4
Latitud	2º12'30''	
Longitud	80º54'3.6''	
Altura al nivel del mar	4	10
Altura física	4	10
Descripción	LINTERNA ELECTRICA SOBRE ESTRUCTURA CILINDRICA METALICA CON FRANJAS HORIZONTALES COLOR ROJO Y NEGRAS	300
Observación	AINW DEL BUQUE HUNDIDO	300
Alcance Nominal	4	10
Alcance Geográfico	7	10
Grupo D(2)	2	10
Des	1.0s	
Ecl	2.0s	

Des	1.0s	
Ecl	6.0s	
Periodo	10	
Luminosidad	45 Cd	10

Aviso

Creación de Avisos

Aviso No.01/2002 (T) ECUADOR –GUAYAS PUERTO COMERCIAL BOYA APAGADA
NOMBRE : BOYA JUAN BAUTISTA
POSICION GEOGRAFICA Latitud: 2º12'30''
Longitud 80º54'3.6''
SE COMUNICA A LOS NAVEGANTES EN GENERAL QUE LA BOYA ANTES DESCRITA ESTA APAGADA TEMPORALMENTE
CARTAS AFECTADAS IOA105-IOA1052-IOA10520
ORIGEN DE LA INFORMACION CAPUIL

Configuración del sistema:
El usuario deberá hacer un click en el menú "Ingreso" submenú "Aviso"

Nombre visual del Campo	Valor a Ingresar	Tamaño del campo
Aviso	No.01/2002	15
Nombre	BOYA JUAN BAUTISTA	50
Año	1977	4
Latitud	2º12'30''	
Longitud	80º54'3.6''	
Descripción	SE COMUNICA A LOS NAVEGANTES EN GENERAL QUE LA BOYA ANTES DESCRITA ESTA APAGADA TEMPORALMENTE	300
Luminosidad	45 Cd	10

Búsqueda de Avisos

El usuario ingresara el numero de Aviso y podrá presionar el botón de Buscar y podrá proceder a modificar o eliminar

Consulta de Avisos

El usuario podrá consultar los avisos vigentes

APÉNDICE I

MANUAL DE USUARIO DE SISNAV

1. Barra de ingresos, modificación, búsqueda, limpiar y eliminación

Esta barra es común en todas las pantallas del sistema y permite realizar las modificaciones, ingresos, eliminaciones, búsquedas y limpieza de pantalla.

.- Permite Grabar la Información de la aplicación.

.- Permite realizar las búsquedas por el campo de identificación de cada aplicación.

.- Permite limpiar los campos de la aplicación.

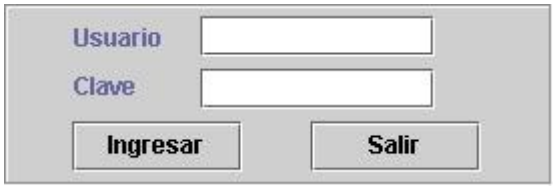
.- Permite realizar las modificaciones después de haber hecho la búsqueda.

.- Permite realizar las eliminaciones después de haber hecho la búsqueda.

.- Permite salir de la aplicación.

Pantalla Usuario Y Clave

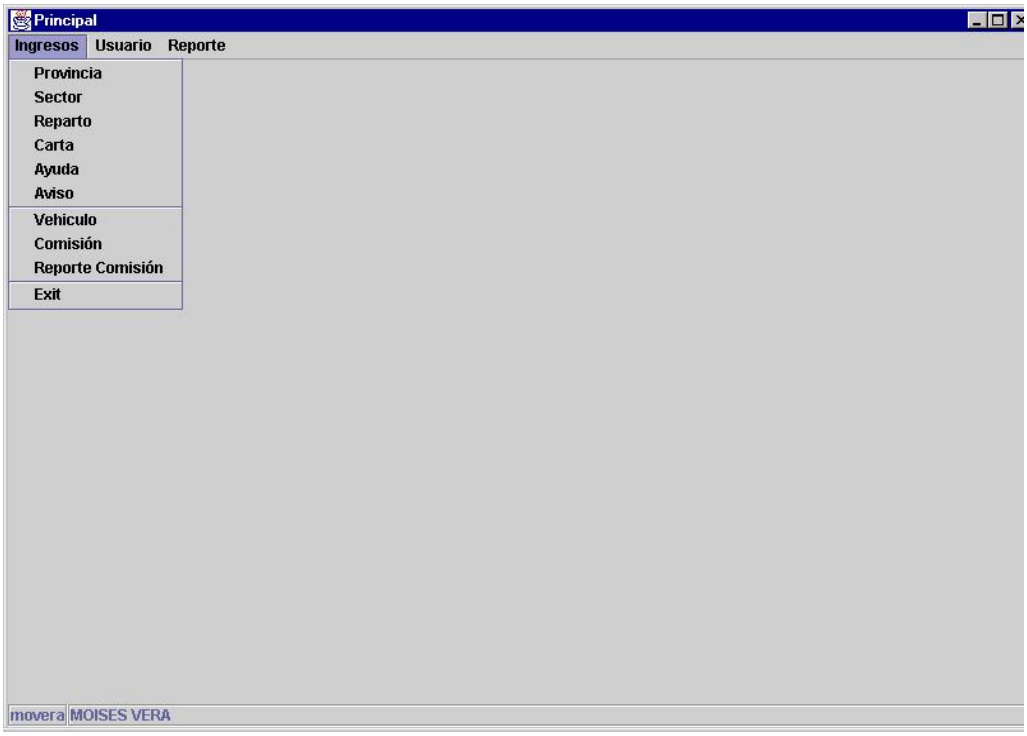
En esta pantalla es la primera en salir al comenzar el sistema en la cual se ingresan datos de autentificación del usuario tales como usuario y clave.



Menú Ingresos

En este menú se podrán los ingresos y mantenimientos para:

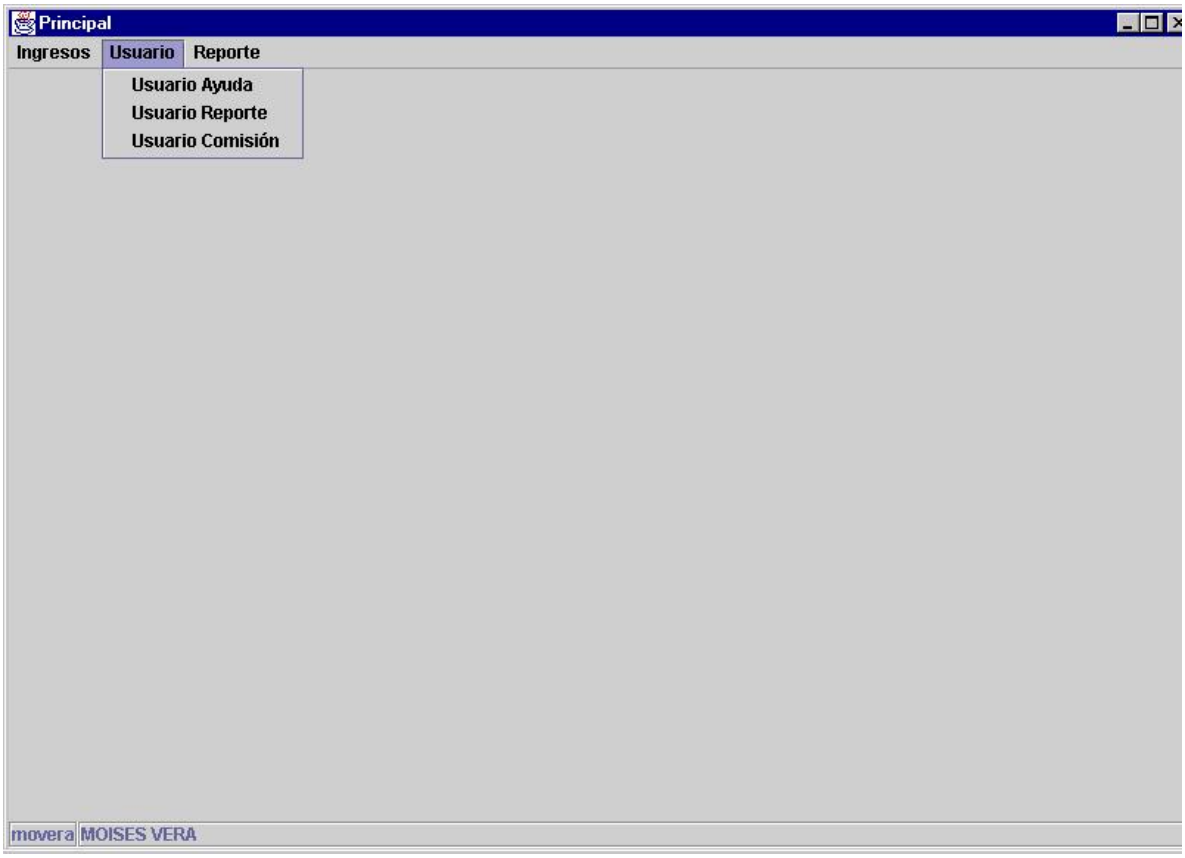
- Provincia
- Sector
- Reparto
- Carta
- Ayuda
- Aviso
- Vehículo
- Comisión
- Reporte Comisión



Menú Usuarios

En este menú se podrán los ingresos y mantenimientos para los usuarios:

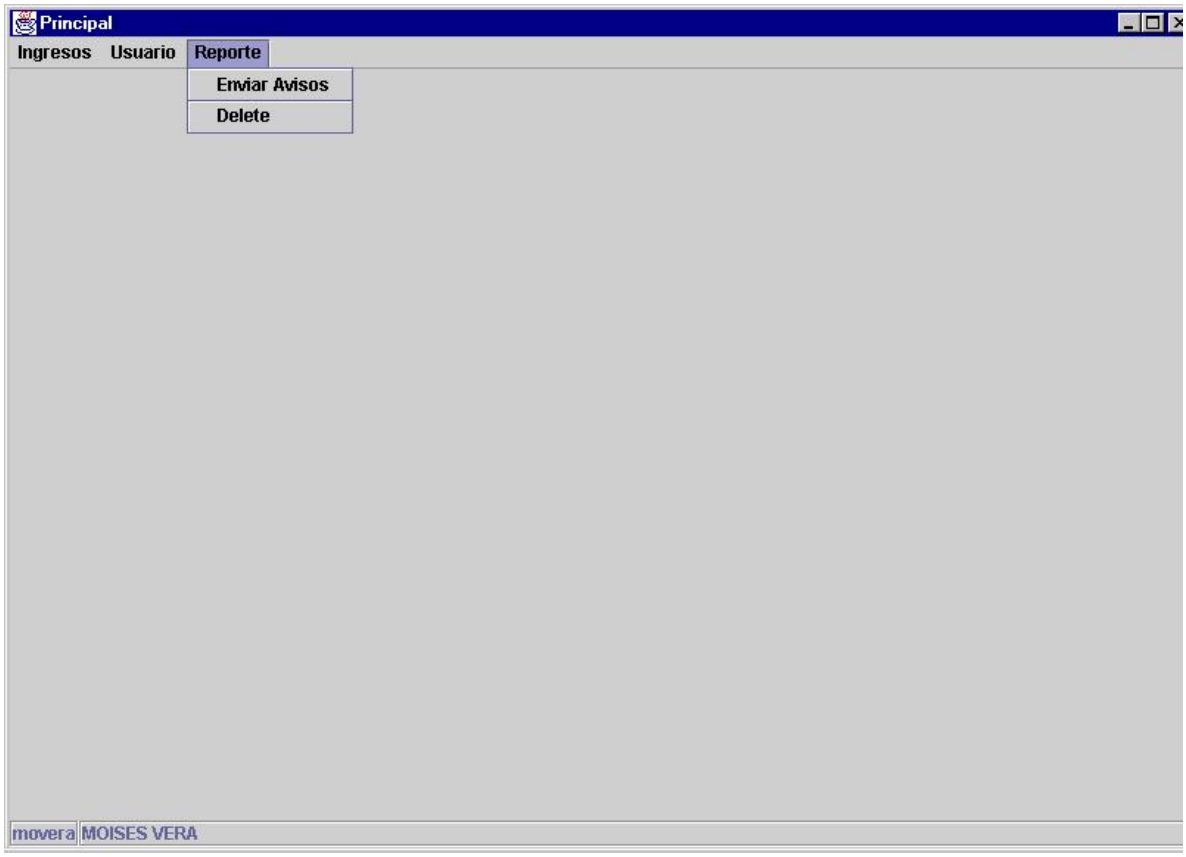
- Usuario Ayuda
- Usuario Reporte
- Usuario Comisión



Menú Reporte

En este menú se podrán los envíos de los avisos:

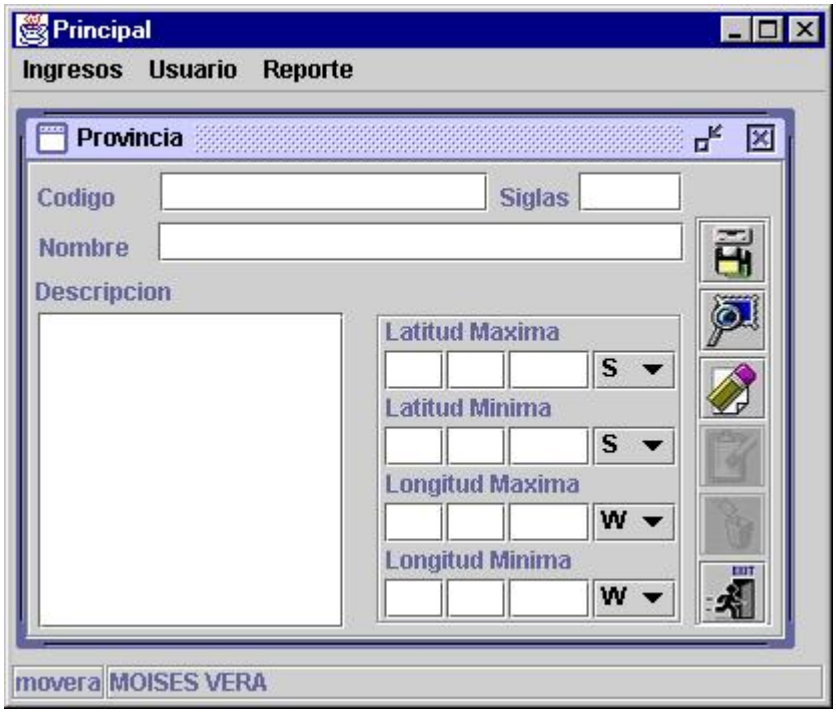
- Enviar avisos
- Delete



Provincia

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de la provincia. En esta pantalla se podrá ingresar información como:
Código.- Este campo contendrá el código correspondiente para la provincia designada el mismo que es único.
Siglas.- En este campo se almacenara las siglas con que se identificara a la provincia.
Nombre.- En este campo se almacenara el nombre de la provincia a ser ingresado.
Descripción.- Contendrá información adicional de la provincia que se ingrese.
Latitud Máxima.- Ubicación geográfica de la latitud máxima de la provincia en grados minutos y segundos.
Latitud Mínima.- Ubicación geográfica de la latitud mínima de la provincia en grados minutos y segundos.

Longitud Máxima.- Ubicación geográfica de la longitud máxima de la provincia en grados minutos y segundos.
Longitud Mínima.- Ubicación geográfica de la longitud mínima de la provincia en grados minutos y segundos.



Sector

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los sectores que se encuentran inmersos en una provincia. En esta pantalla se podrá ingresar información como:
Código.- Este campo contendrá el código correspondiente para el sector que se encuentre en la provincia correspondiente, este código es único.
Nombre.- Este campo contendrá el nombre del sector.
Provincia.- en este campo se escogerá a la provincia que contenga a dicho sector.

Ayudas

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de las ayudas que se puedan ingresar las misma que pueden ser Boya, Faro, Farolote, Baliza o Enfilada. En esta pantalla se podrá ingresar información para cualquiera de las ayudas antes mencionadas tales como:

Número de Orden Nacional.- Número de la orden nacional que se relaciona con la ayuda.

Número de Orden Internacional.- Número de la orden internacional que se relaciona con la ayuda.

Nombre.- Nombre que representa a la ayuda.

Sector.- Permite escoger el sector que se encontrara la ayuda en este campo a su ves permitirá ver a que provincia corresponde dicho sector.

Carta.- Esta lista permite escoger todas las cartas náuticas en donde se encuentran las ayudas, se pueden seleccionar varia a la ves con solo las teclas control + el clic del Mouse

Fecha de construcción.- Corresponde a la fecha de construcción de la ayuda.

Fecha de última modificación.- Corresponde a la fecha en que se realizo la ultima modificación o mantenimiento a la ayuda.

Latitud.- Ubicación geográfica de la latitud de la ayuda en grados minutos y segundos.

Longitud.- Ubicación geográfica de la longitud de la ayuda en grados minutos y segundos.

Altura física.- Información sobre la altura de la ayuda en metros.

Altura nivel del mar.- Información sobre la altura sobre el nivel del mar de la ayuda en metros.

Alcance geográfico.- Alcance geográfico de la ayuda en millas.

Alcance nominal.- Alcance nominal de la ayuda en millas.

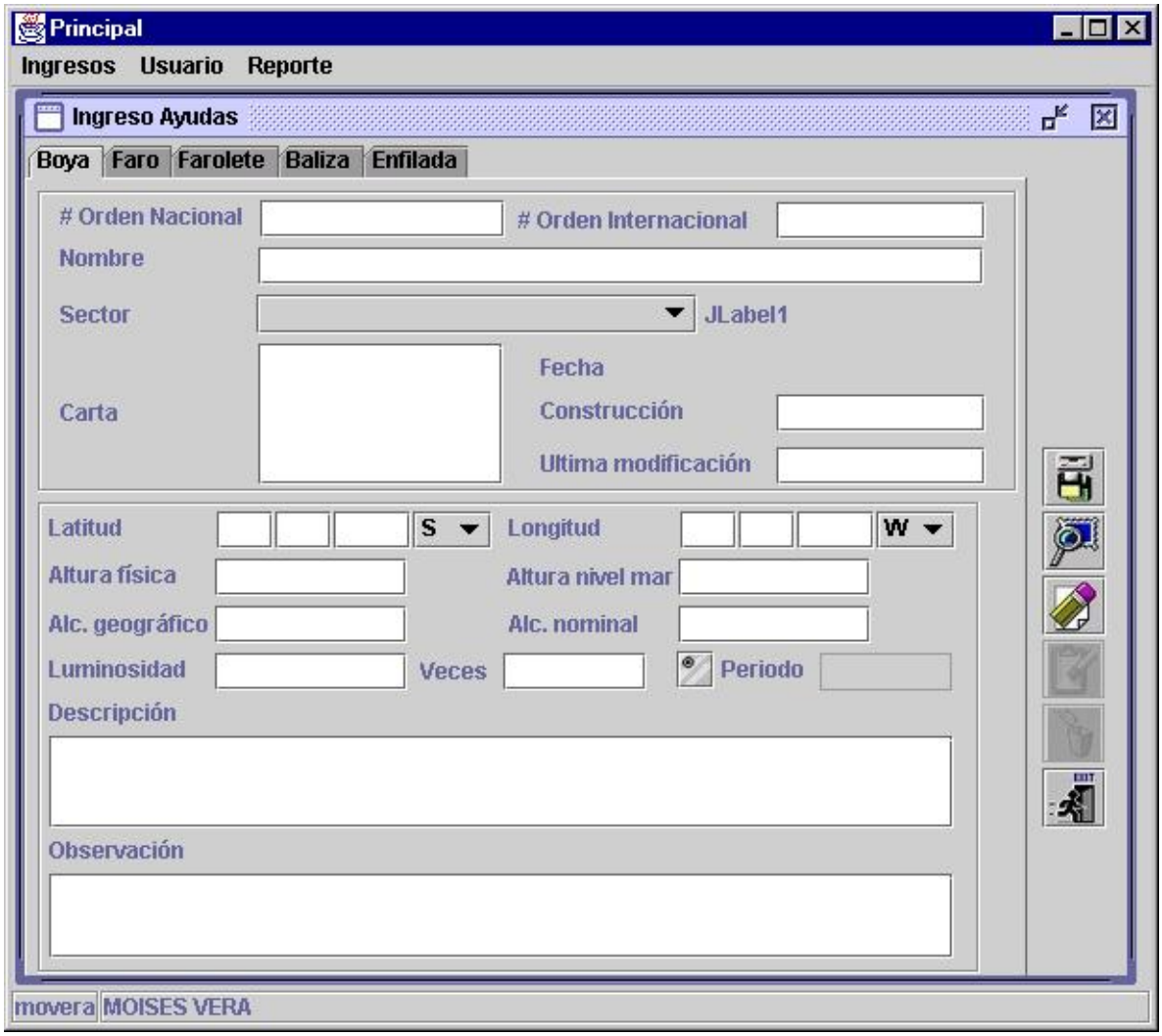
Luminosidad.- Información sobre la luminosidad de la ayuda.

Veces.- Número de veces que se repiten datos como el destello, eclipse y esta información adicional se ingresa aplastando el botón a lado del campo veces el cual preemitirá hacer el ingreso de la misma.

Periodo.- Este campo se llena de manera automática con la información ingresada anteriormente.

Descripción.- Información adicional sobre la ayuda ingresada.

Observación.- Información adicional sobre la ayuda ingresada es decir tipos de materiales.



Carta

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de las cartas náuticas en donde se encuentran localizadas las ayudas. En esta pantalla se podrá ingresar información tales como:

Código.- Este campo contendrá el código correspondiente para la carta el cual mismo que comenzara con I.O.A-, este código es único.

Nombre.- Nombre de la carta náutica a ser ingresada.

Latitud Máxima.- Ubicación geográfica de la latitud máxima de la carta en grados minutos y segundos.

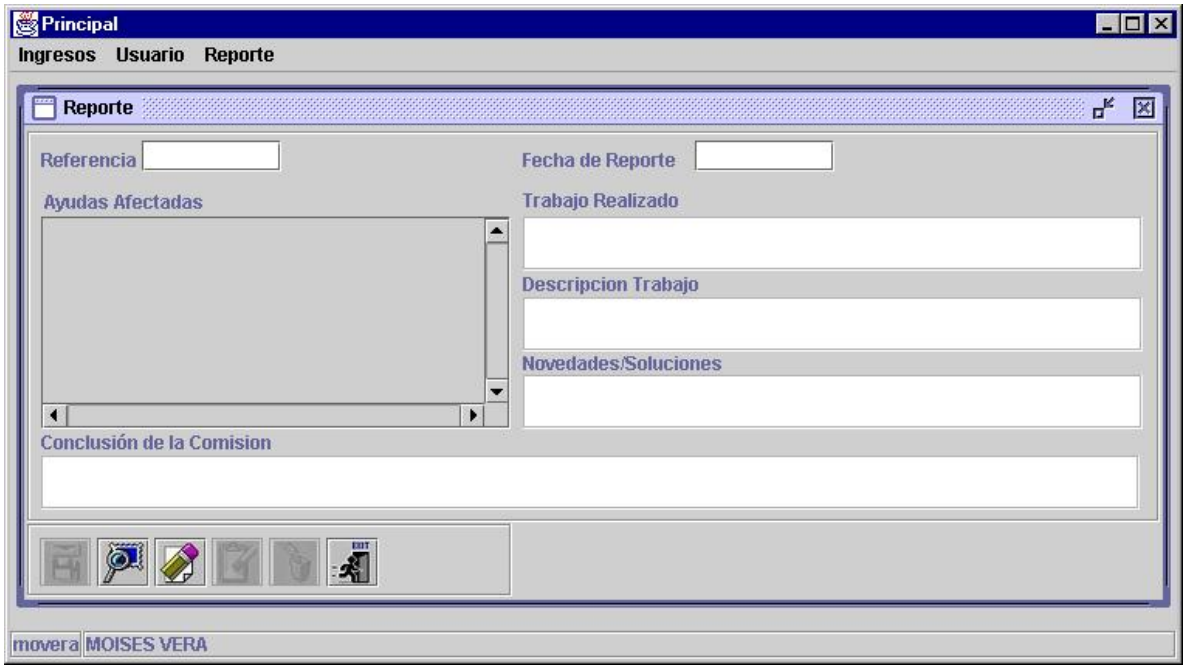
Latitud Mínima.- Ubicación geográfica de la latitud mínima de la carta en grados minutos y segundos.

Longitud Máxima.- Ubicación geográfica de la longitud máxima de la carta en grados minutos y segundos.

Longitud Mínima.- Ubicación geográfica de la longitud mínima de la carta en grados minutos y segundos.

Reporte

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los reportes. En esta pantalla se podrá ingresar información como:
Referencia.- Código de la referencia.
Fecha de Reporte.- Fecha en que se ingresa el reporte.
Trabajo Realizado.- Información sobre el trabajo que se realizo.
Descripción del Trabajo.- Que tipo de trabajo se realizo en el mantenimiento.
Novedades/Soluciones.- Que tipo de soluciones se implantaron y la novedades presentadas.
Conclusión de la comisión.- Que es lo que se obtuvo y logro en la misma.
Ayudas Afectadas.- Las ayuda que están inmersas en este reporte.



Vehículo

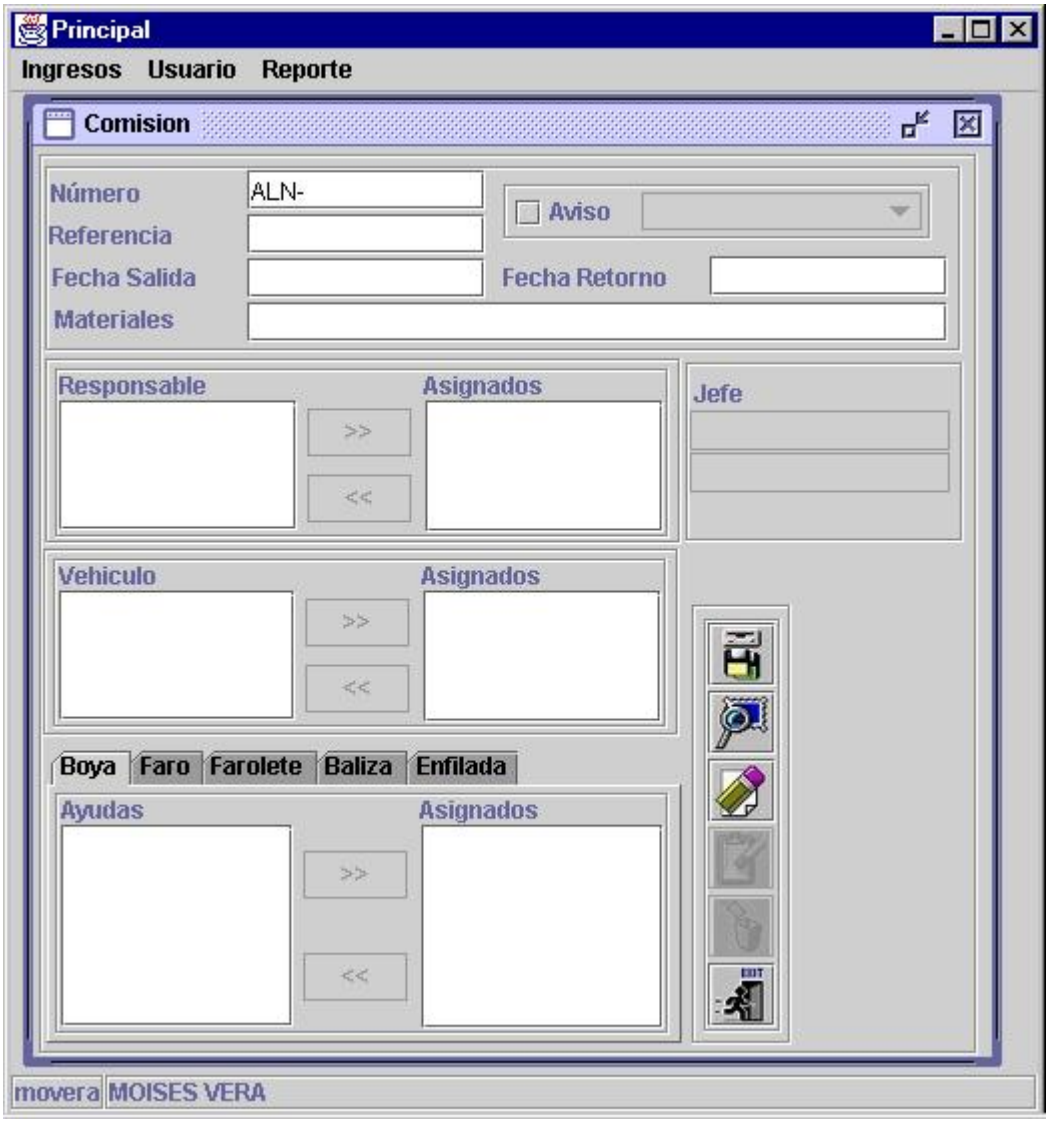
En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los vehículos. En esta pantalla se podrá ingresar información como:

Código.- Este campo contendrá el código correspondiente para el vehículos que se utilicen en los mantenimientos y varios el mismo que es único.

Descripción.- Información adicional sobre el vehículo.

Comisión

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de las comisiones que se crean para el mantenimiento o reparación de las ayudas. En esta pantalla se podrá ingresar información como:
Número.- El número de la comisión el mismo que será único y comenzara con las letras ALN-.
Referencia.- El numero de referencia con que se relaciona la comisión.
Aviso.- Este capo es opcional y me indicara si esta afecta algún aviso o no y si es así se escogerá al que afecta.
Fecha de Salida.- Contiene la fecha de salida de la comisión para la ayuda.
Fecha de Retorno.- Contiene la fecha de retorno de la comisión para la ayuda.
Materiales.- Información sobre los materiales que se utilizaron en la comisión.
Responsables.- En esta lista se podrá escoger a las personas que intervendrán en la comisión, esto se realiza seleccionando a las personas que intervendrán en la comisión agradándolos al lado de la lista de asignados.
Jefe.- Este campo se llena de manera automática con el nombre que se seleccione de la lista de asignados de los escogidos de la lista de responsables.
Vehículo.- En esta lista se podrá escoger a los vehículos que intervendrán en la comisión, esto se realiza seleccionando a los vehículos que intervendrán en la comisión agradándolos al lado de la lista de asignados.
Ayudas.- Aquí se podrán escoger las ayudas que serán atendidas por la comisión, y estas pueden ser faro, farolote, boya, baliza y enfilada, para lo cual se debe escogerlas y pasarlas a lado de la lista de asignados.



Usuario Ayuda

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los usuarios Ayuda que se crean para el mantenimiento de todos los datos, en esta pantalla estar información de las personas que podrán manipular el sistema. En esta pantalla se podrá ingresar información como:
Identificación.- Se almacenara el número de identificación de la persona a ser ingresada.
Tipo Identificación.- Permite escoger el tipo de identificación a ser ingresada.
Nombre.- El nombre de la persona a ser ingresada.
Apellido.- El apellido de la persona a ser ingresada.
Titulo.- El titulo de la persona a ser ingresada.
Cargo.- El cargo de la persona a ser ingresada.
User.- El usuario con que se va ha identificar a la persona a ser ingresada a la hora de el mismo hacer uso del sistema.

Password.- La clave de usuario con que se va ha identificar a la persona a ser ingresada a la hora de el mismo hacer uso del sistema.

Usuario Reporte

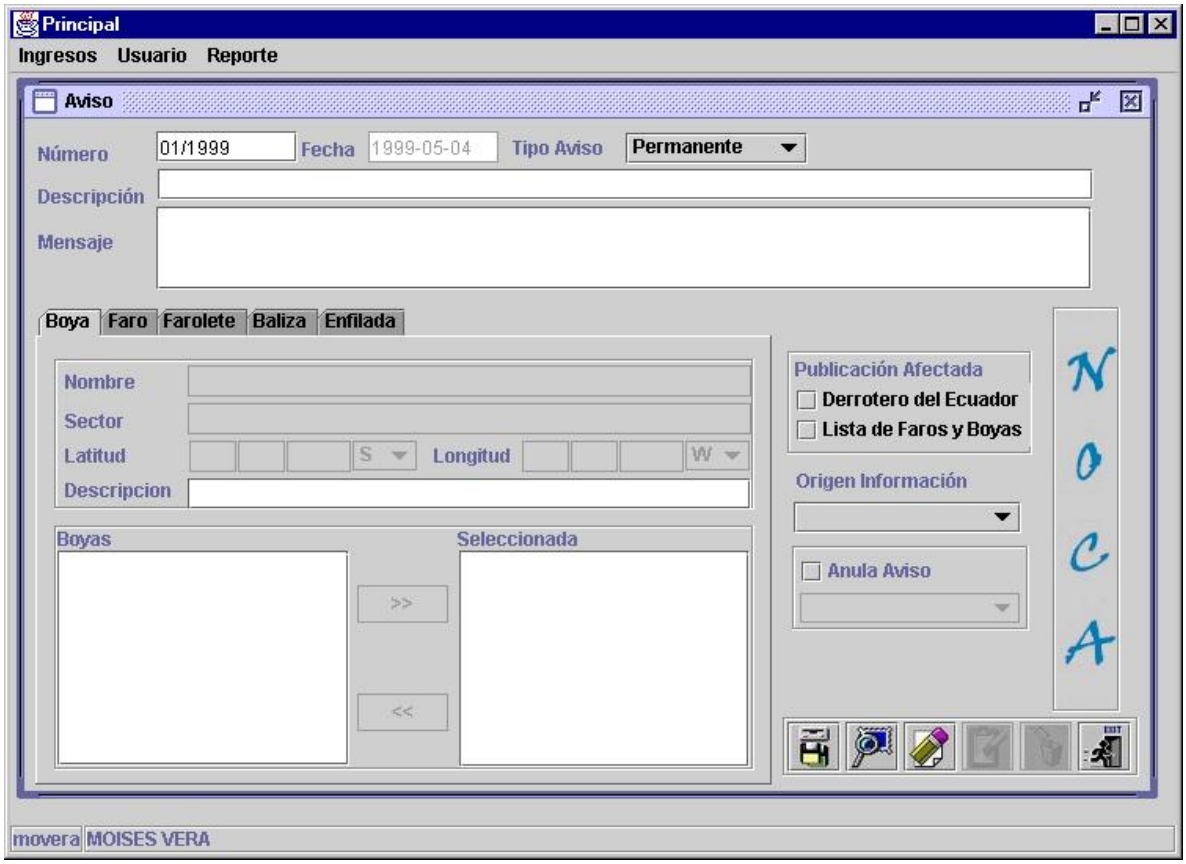
En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los usuarios reporte que se crean para el mantenimiento de todos los datos, en esta pantalla estar información de las personas a la que se les debe enviar información de los reportes. En esta pantalla se podrá ingresar información como:
Identificación.- Se almacenara el número de identificación de la persona a ser ingresada.
Tipo Identificación.- Permite escoger el tipo de identificación a ser ingresada.
Nombre.- El nombre de la persona a ser ingresada.
Apellido.- El apellido de la persona a ser ingresada.
Titulo.- El titulo de la persona a ser ingresada.
Cargo.- El cargo de la persona a ser ingresada.
Email.- Dirección de correo electrónico.
Beeper.- Número de Beeper sobre beeper.
Pin.- Pin del Beeper.
Fax.- Número de fax.
Servicio.- Tipo de servicio.

Usuario Responsable

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los usuarios que puedan participar en una comisión. En esta pantalla se podrá ingresar información como:
Identificación.- Se almacenara el número de identificación de la persona a ser ingresada.
Tipo Identificación.- Permite escoger el tipo de identificación a ser ingresada.
Nombre.- El nombre de la persona a ser ingresada.
Apellido.- El apellido de la persona a ser ingresada.
Titulo.- El titulo de la persona a ser ingresada.
Cargo.- El cargo de la persona a ser ingresada.

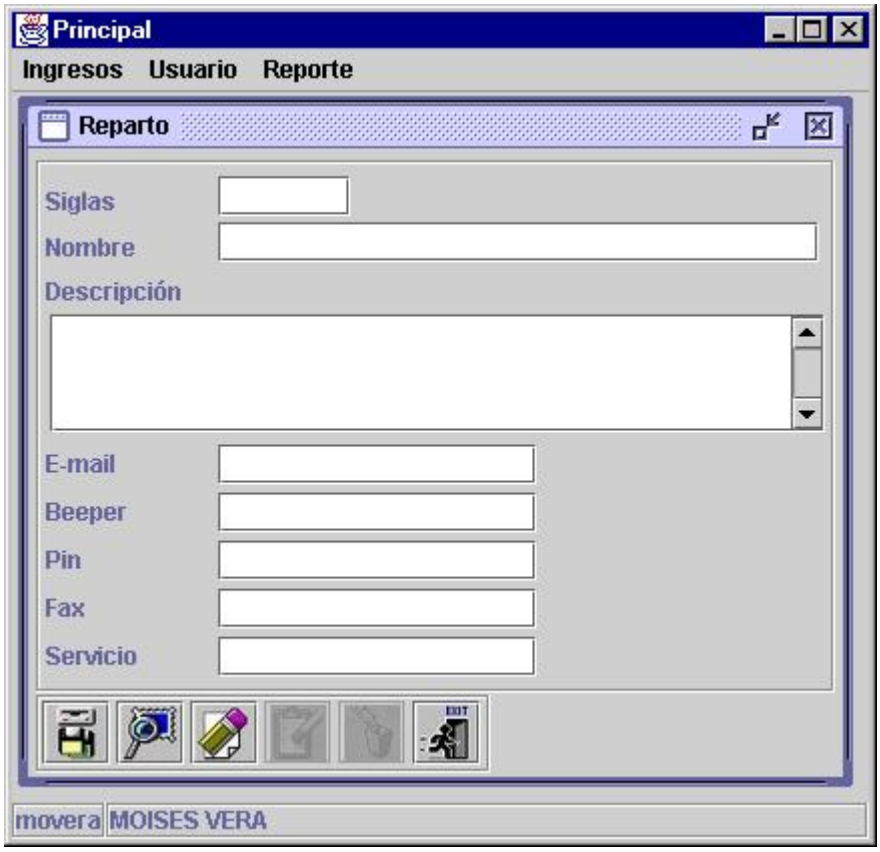
Aviso

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los avisos que generan para las diferentes ayudas. En esta pantalla se podrá ingresar información como:
Número.- Número del aviso el mismo que se genera de manera automática.
Fecha.- Fecha del aviso.
Tipo de Aviso.- Se podrá escoger entre tipo de aviso permanente o temporales.
Descripción.- Información sobre el aviso.
Mensaje.- El mensaje que contiene el aviso.
Ayudas(faro/farolote/boya/enfilada/baliza).- Aquí se podrá escoger a las ayudas que se afecta con dicho aviso, para lo cual solo hay que pasarlas a la lista de seleccionadas, al hacer esto me permite mostrar información con respecto a la ayudas seleccionadas (nombre, sector, latitud, longitud) e ingresar una pequeña descripción para cada una.
Publicación Afectada.- Escoger a que publicación afecta ya sea Derroteros del Ecuador, Lista de Faros y Boyas o ha ambas.
Origen de información.- Permite escoger de donde se origina la información.
Anula Aviso.- Permite escoger si este aviso a nula alguno anterior y escoger a cual.



Reparto

En esta pantalla se podrá realizar los correspondientes ingresos y mantenimientos a los datos de los Repartos que hay en el país. En esta pantalla se podrá ingresar información como:
Siglas.- Las siglas con que se representan al reparto.
Nombre.- El nombre del reparto.
Descripción.- Información sobre el reparto.
Email.- Dirección de correo electrónico.
Beeper.- Número de Beeper sobre beeper.
Pin.- Pin del Beeper.
Fax.- Número de fax.
Servicio.- Tipo de servicio.


Principal
Ingresos
Usuario
Reporte
Reparto
Siglas
Nombre
Descripción
E-mail
Beeper
Pin
Fax
Servicio
movera
MOISES VERA