ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO DE UN SISTEMA DE INFORMACIÓN PARA GESTIONAR LA IMPLANTACIÓN, MANTENIMIENTO Y MEJORA CONTINUA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013"

TESIS DE GRADO

Previa a la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por

MAYRA LORENA MAHECHA GUZMÁN

GABRIEL RICARDO COELLO FALCONES

Guayaquil – Ecuador

2016

AGRADECIMIENTO

A Dios porque sé que en su misteriosa forma de mover los hilos permitió que llegásemos hasta aquí.

A mi madre y a mi hermana por su gran apoyo mientras estudiábamos y desarrollábamos el presente trabajo.

A nuestro tutor Lenin por su ayuda y guía desde el inicio del proyecto. A ellos Eternamente gracias.

Lorena.

Gracias Dios por darnos fortaleza para alcanzar las metas.

Gracias a nuestras familias que nos dieron animó y apoyo.

Gracias a nuestros maestros que compartieron sus conocimientos y experiencia.

Gabriel.

DEDICATORIA

A Sebas mi niño amado, que muchas noches no quiso ir a dormir por acompañarnos mientras trabajábamos en este proyecto, por ser mi inspiración para ser cada día mejor en todos los aspectos de mi vida. Espero con este logro sembrar una certeza en su futuro: que todo lo que él se proponga lo conseguirá si lo hace con convicción y responsabilidad.

A Gabriel, mi amor, mi amigo y mi compañero de fórmula en tantos otros proyectos; su pertinaz guía, paciencia y complicidad facilitaron el camino. Los amo.

Lorena

A Lorena y Sebastián que juntos caminamos este sendero con amor y comprensión y Dios nos guie de la mano para seguir adelante y guiar a otros con creatividad y ejemplo.

Gabriel.

TRIBUNAL DE SUSTENTACIÓN

_____
Ing. Lenin Freire
PRESIDENTE
DIRECTOR DEL PROYECTO DE GRADUACIÓN

_____
Mgs. Nestor Arreaga
MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

RESUMEN

En el capítulo 1 se analiza el contexto general y los antecedentes de la solución propuesta que basada en la experiencia de sus autores sugiere que gestionar la implantación y mantenimiento de un SGSI debería ser más ágil con la ayuda de un sistema de información que automatice la gestión de los activos de información y sus riesgos.

En el capítulo 2 se presenta el marco teórico de la seguridad de la información y la Norma ISO 27001, se explican también los conceptos relacionados a un SGSI como activo de información, amenaza, vulnerabilidad, riesgo y la estrecha relación del SGSI con el ciclo de PHVA. Se expone además el enfoque y la nueva estructura de la norma en la versión 2013 así como también una comparativa con la versión del 2008 para verificar los cambios más sustanciales.

En el capítulo 3 Se realiza un levantamiento completo de los factores que tienen algún tipo de incidencia sobre los proyectos de Sistemas de Gestión de Seguridad de la Información en las organizaciones de Ecuador. Se revisan las iniciativas de estado como el Esquema Gubernamental de la Seguridad de la Información y la resolución de la Junta Bancaria que dan obligatoriedad a las organizaciones del sector público y bancario - financiero de implementar SGSI y Continuidad del Negocio respectivamente. Se revisan también las estadísticas de acreditación de la norma obtenidas del sitio web oficial de la organización ISO a nivel país y de la región. Todos los factores analizados convergen para presentar a ASTINAVE EP, la organización a la cual se le hace la implementación, conocer un poco de sus procesos y de su experiencia con otras normativas de ISO. Al final se hace una revisión del software que se usa actualmente para gestionar un SGSI; se describen y comparan entre sí 4 de los más conocidos.

En el capítulo 4 se muestra el análisis y diseño del sistema de información en base a los requerimientos de la norma y del contexto organizacional. Se explican detalladamente las decisiones de la metodología de desarrollo, la arquitectura de la solución, el uso de las herramientas a utilizarse tanto en el modelado como en la codificación del software. Asimismo los módulos

funcionales se exponen desde los modelos de datos físicos y los casos de usos correspondientes. Se establece la metodología de gestión de activos y de sus respectivos riesgos en función de la norma ISO 27005; las reglas de negocio de los módulos funcionales se programan en base a esto al igual que las escalas de impacto y las zonas de riesgo.

En el capítulo 5 se dan detalles de la implementación del sistema de información y su puesta en producción exponiendo las consideraciones para el servidor web, de base de datos y de reportes. Entre esas consideraciones, al igual que se lo hace en fase de diseño, se da espacio para relevar la integración con SharePoint, el ERP y el directorio activo de la organización. Se hacen pruebas de la aplicación del software y su uso para cada uno de sus módulos funcionales.

En el capítulo 6 se presentan los resultados de las pruebas de la solución propuesta una vez que se completan con éxito cada una de las fases planteadas en función de los objetivos propuestos y del uso del sistema per se.

ÍNDICE GENERAL

ABREVIATURAS

ASMX	:	Active Server Method File
ASP	:	Active Server Page
ASTINAVE EP	:	Empresa Publica Astilleros Navales Ecuatorianos
CRUD	:	Create, Read, Update and Delete
DAL	:	Data Access Layer
DBMS	:	Database Management System
DIRECTORIO ACTIVO	:	Es el servicio de directorio en una red distribuída de Microsoft
EGSI	:	Esquema Gubernamental de Seguridad de la Información
ERP	:	Enterprise Resource Planning
ESET	:	Es una compañía dedicada a desarrollar productos de seguridad informática
FRAMEWORK	:	Conjunto de módulos que dan una funcionalidad particular
FRAMEWORK .NET	:	Es un FRAMEWORK provisto por Microsoft para ayudar a los desarrolladores a escribir aplicaciones WEB más rápidamente
GPR	:	Sistema de Gestión por Resultados
HTML	:	Hypertext Markup Language
IDE	:	Integrated Development Environment
IIS	:	Internet Information Server
INEC	:	Instituto Nacional de Estadística y Censos
ISO	:	International Organization for Standardization
LINKED SERVER	:	Característica que permite realizar operaciones entre servidores remotos de base de datos

OHSAS	:	Occupational Health and Safety Management System Certification
ORM	:	Object-relational mapping
PHP	:	Pre Hypertext -processor
PHVA	:	Ciclo de Deming, Planificar - Hacer - Verificar - Actuar
RSCM	:	Reporting Services Configuration Manager
SGSI	:	Sistema de Gestión de la Seguridad de la Información
SHAREPOINT	:	plataforma de colaboración empresarial de Microsoft orientado a la WEB
SIG	:	Sistema Integrado de Gestión
SMTP	:	Simple Mail Transfer Protocol
SNAP	:	Secretaría Nacional de la Administración Pública
SO	:	Sistema Operativo
SOA	:	Statement of Applicability
SQL	:	Structured Query Language
SSDT	:	Sql Server Data Tools
SSRS	:	SQL Server Reporting Services
STORED PROCEDURES	:	Es un programa almacenado y ejecutado directamente en una base de datos
RDL	:	Report Document Language
TIC	:	Tecnologías de la información y la comunicación
UI	:	User Interface
URL	:	Uniform Resource Locator
WCF	:	Windows Communication Foundation
WEB	:	World Wide Web

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La adopción de estándares y buenas prácticas está muy en auge entre las organizaciones con el fin de destacar de la competencia, para ello las normas ISO son unas de las alternativas más aceptadas a la hora de estandarizar procesos; van muy a la vanguardia de los estándares de calidad con la ISO 9001, en seguridad y salud ocupacional con la OHSAS 18001, en ambiente con la 14001, en gestión de servicios de TI con la 20000, en continuidad del negocio con 223001 y en seguridad de la información con la 27001 que, aunque rezagada, terminará convirtiéndose en medular si se considera que en la actualidad la información y el uso de tecnologías para su gestión son un activo estratégico en cada organización.

No obstante, si el enfoque es sobre la ISO 27001, ha de tenerse en cuenta que la implantación de un Sistema de Gestión de la Seguridad de la Información que sea dinámico y que incluso pueda articularse con otros sistemas ya implementados en una organización es una tarea con

alta carga administrativa en la que para cada activo de información que se desea proteger se deberán identificar vulnerabilidades, amenazas y con esto realizar un análisis muy sesudo para la evaluación y tratamiento de los riesgos correspondientes, estas son actividades que se repiten dentro de una esquema de mejora continua en donde se deberían guardar todos los cambios que se realizan en función de la aplicación de los controles operacionales pertinentes, el panorama se complica más cuando en la mayoría de los casos el seguimiento se realiza manualmente sin dar garantías de una traza verificable en el tiempo para las tareas realizadas. Definitivamente ahí existe un problema que no se puede subestimar, así que la gestión de la seguridad de la información en base al estándar ISO 27001 bien podría optimizarse con el uso de un sistema de información que permita la gestión de los activos de información así como la gestión de sus riesgos; apoyarse en un software contribuiría a tener catálogos centralizados de activos, de amenazas, de vulnerabilidades, generar de forma automática la declaración de aplicabilidad, guardar la valoración del impacto de los activos en la organización, referenciar los documentos generados por la organización y, lo mejor de todo, mantener los riesgos sin perder la trazabilidad de los planes de acción pudiendo verificar en todo momento si los controles que se están aplicando dan un riesgo residual disminuido con respecto al inherente.

En vista del escenario descrito y con miras a poder sortearlo de una mejor forma, el presente trabajo de titulación realizará un análisis del contexto de implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información para en base a ello desarrollar un software que facilite las tareas propias de la adopción del estándar ISO 27001:2013.

CAPÍTULO 1

GENERALIDADES

1.1 Antecedente

Los maestrantes autores del presente trabajo de Tesis han estado involucrados con proyectos de la seguridad de la información desde el 2013, en base a esta experiencia han podido asimilar lo positivo en la adopción normas como la ISO 27001, así como también las dificultades a la hora de gestionar, sin la ayuda de un sistema informático, un volumen considerable de datos desde la fase de inicio con el fin de dar cumplimiento a lo indicado en dicha Norma.

De acuerdo a la definición dada por la organización ISO; “El uso de la familia de normas ISO 27000 ayuda a las organizaciones a administrar la seguridad de su información más valiosa, tales como información

financiera, la propiedad intelectual, detalles de los empleados o la información confiada por terceros. Para ello la ISO / IEC 27001 es el estándar más conocido que proporciona requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI)" [1].

Por su parte un SGSI es el proceso sistemático, en lo posible documentado y sobretodo conocido y asumido por toda la organización, a través del cual se da garantías del cumplimiento de la Norma ISO 27001 para asegurar los activos de información en función de su confidencialidad, disponibilidad e integridad. Lo que no se indica en ningún lado es que las acciones para definir, registrar y mantener los procesos, activos, amenazas y riesgos son realmente demandantes de tiempo y esfuerzo; en ocasionales es casi imposible dar la trazabilidad correcta a los acontecimientos relacionados así como a la evidencia documental de cada caso.

De lo experimentado con la implantación del estándar indicado por la ISO 27001 se tiene que gestionar el ciclo de vida de un SGSI de manera totalmente manual, le agrega un factor más de complicación a esta tarea y de allí surgió la necesidad de desarrollar un sistema de información modular que agilite la gestión de la seguridad de la información y se integre con los sistemas existentes en la organización.

1.2 Descripción del Problema

La Seguridad de la Información en Ecuador todavía no consigue los niveles de reconocimiento a nivel empresarial que tienen otras normas de la misma familia, ISO 9001 y 14001 por ejemplo, sin embargo, se puede destacar que el gobierno ha tenido una iniciativa interesante al respecto: la promulgación del Acuerdo Ministerial 166 de la Secretaría Nacional de la Administración Pública (SNAP) que fija las actividades principales que las entidades y empresas públicas deben cumplir para implementar el Esquema Gubernamental de Seguridad de la Información, el cual está basado en la Norma ISO 27001:2005. En el sector financiero la resolución 3066 de la Junta Bancaria también propugna la implantación de Sistemas para Gestión de la Seguridad de la Información (SGSI) y garantías para la Continuidad del Negocio en el marco de la gestión de riesgos corporativos.

Por otro lado el sector privado, aunque de manera incipiente, también empieza a interesarse en destacar que en sus procesos se tiene un buen manejo de la confidencialidad de la información que maneja, así que la expectativa en el corto y mediano plazo es que exista un aumento de la demanda de organizaciones que buscarán certificarse en la Norma ISO 27001.

No seguir estándares probados dificulta la identificación, seguimiento y control de riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los activos de información. Otros problemas son que los esfuerzos en temas de seguridad se diluyen al no buscar objetivos específicos que vayan en sintonía con la misión de la entidad, esto acarrea el desperdicio de recursos humanos, técnicos y económicos.

Bajo este contexto se tiene que las actividades propias de la planificación, ejecución y monitoreo del SGSI por lo general se realizan manualmente y guardando expedientes en papel arriesgándose a no dejar la traza real de lo que ocurre, una de las causas bien pudiera ser que en el mercado de las soluciones informáticas no hay muchas ofertas para cubrir de manera automatizada los procesos propios de la norma y de las pocas que hay, las más reconocidas como ISO TOOLS y GLOBALSUITE son costosas, más aun si se las quiere bajo el esquema on premise, es decir, pagando un valor por adquirir licencias a perpetuidad y con instalación y configuración en servidores propios de la organización. Por lo tanto un desarrollo como el propuesto sería una muy buena alternativa para cubrir esa brecha.

1.3 Solución Propuesta

La solución planteada es el desarrollo de un sistema de información que permita administrar todas las fases y todos los objetos involucrados de un Sistema de Gestión de la Seguridad de la Información.

El sistema es un aplicativo web accesible desde la intranet de la organización considerando también la gestión de permisos y la integración con otros módulos empresariales como registro de bienes, empleados, documentos y otros archivos desde el gestor documental del SGSI. En resumen se propone automatizar las siguientes funcionalidades:

1. Mantener el Inventario de activos de información.
2. Catalogar los procesos de la organización.
3. Gestionar el catálogo de amenazas y vulnerabilidades.
4. Calcular la tasación de activos de información.
5. Registrar y mantener la identificación de riesgos.
6. Gestionar la evaluación de riesgos.
7. Gestionar la asignación de responsables de seguimiento y de las acciones para el tratamiento de riesgos.

8. Registrar la asociación de evidencia documental.

9. Generar reportes y consultas de seguimiento para la gestión de controles de la Norma.

10. Generar la declaración de aplicabilidad.

El principal beneficio del uso del sistema de información propuesto es visibilizar el progreso de la implementación de la Norma, aportando un mayor control de forma sistematizada que permite tomar acciones oportunas cuando existan contratiempos. La automatización de las actividades requeridas en la Norma impacta en el tiempo de implementación, la productividad de los involucrados y en el control de recursos lo cual aporta para una eficaz puesta en marcha de la Norma. También permite tener al día toda la información requerida por las entidades de control como el SNAP actuando como un repositorio central de indicadores y documentación establecidos en la Norma.

La herramienta da al usuario acceso a sus diferentes módulos mediante un portal web, desarrollado en ASP.NET. La infraestructura mínima necesaria es de un servidor de aplicaciones web, una base de datos SQL SERVER con servicio de reportería y espacio para almacenamiento de documentos, por lo cual la inversión necesaria es baja para los beneficios del uso de la herramienta, más aun si se cuenta

con una infraestructura que permite virtualización puesto que se reduce también el costo del hardware.

Si bien este sistema está diseñado para cubrir las necesidades de cualquier tipo de organización en el escenario en que se desarrolla el presente trabajo surge el reto de integrar este nuevo sistema de información a otros sistemas puestos ya en producción como el ERP, el gestor documental, la intranet, etc. Tener una experiencia previa con sistemas integrados de gestión (SIG) brindaría una ventaja significativa con cara a la implantación del SGSI primordialmente por tener procesos definidos y documentados, para la organización a la cual se le desarrollará este software, dicha documentación se mantiene en el marco de un esquema de gestión documental que se soporta en SHAREPOINT 2013 y se deberá garantizar la referencia de documentación siempre actualizada.

1.4 Objetivo General

Desarrollar un sistema de información para gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001:2013.

1.5 Objetivo Específicos

Los objetivos específicos para este trabajo son:

1. Dar el contexto general que sustenta el presente trabajo.

2. Presentar el marco teórico de la seguridad de la información y la Norma ISO 27001.

3. Dar a conocer la situación actual y los requerimientos con respecto al SGSI de la organización donde se propone la implementación.

4. Mostrar el análisis y diseño del sistema de información en base a los requerimientos de la norma y del contexto organizacional.

5. Detallar la implementación del sistema de información y su puesta en producción.

6. Listar los resultados de las pruebas del sistema.

1.6 Metodología

La metodología se rige a las buenas prácticas estipuladas en el estándar ISO 27001:2013 donde se dan las directrices para la correcta implantación de un SGSI. De forma específica el diseño del sistema está basado en las buenas prácticas de implementación hechas por la Norma ISO 27002 y la metodología de gestión de riesgos implementada en base a lo establecido por la ISO 27005. Por último, se consideran todas las demás recomendaciones que influyen en cada uno de los objetivos específicos de la sección anterior.

Cabe resaltar que este proyecto es una propuesta estandarizada y adaptable a cualquier tipo de organización sin que importe el grupo de procesos cuyos activos de información se quieran asegurar.

CAPÍTULO 2

MARCO TEÓRICO

2.1 Seguridad de la Información

La información en los tiempos actuales es seguramente el bien más valioso, el activo con más valor para cualquier organización, en este contexto se podría hablar de patentes, experiencia, conocimiento del mercado, fórmulas secretas, información de clientes, contratos, nómina de empleados, etc. Esta información es la que marca la identidad de las empresas y le da su ventaja competitiva respecto de otras, y en manos incorrectas puede poner en riesgo las operaciones que en el peor de los casos puede significar el fin del negocio. Lo mismo ocurre a nivel gubernamental donde los planes económicos, de seguridad pública, de seguridad territorial, información de inteligencia, negociaciones

diplomáticas en la mayoría de los casos se consideran como información secreta y confidencial y su revelación supone un riesgo para la seguridad del estado. A nivel personal algo tan simple como enviar un mensaje a un familiar indicando el momento que sale de un lugar puede ser usado por delincuentes para ejecutar un secuestro, un caso muy común es el robo de los datos por tarjeta de crédito entre otros delitos informáticos que vienen en aumento como lo muestran datos de la fiscalía ecuatoriana [2].

La seguridad de la información entonces comprende todo lo relacionado con la protección de la información perteneciente a las organizaciones y las personas. Esto incluye medidas tecnológicas, organizacionales, regulatorias y legales que permitan asegurar la confidencialidad, disponibilidad e integridad de la información que justamente quiere protegerse.

2.1.1 Activos de Información

Toda aquella información que es procesada por sistemas tecnológicos, almacenada en medios portátiles o granjas de servidores y que circula por redes de telecomunicaciones puede estar en constante riesgo de ser violentadas con las posibles consecuencias mencionadas en la sección anterior. Cada uno de estos componentes; información, sistemas, medios, equipos,

archivos físicos y digitales se catalogan como activos de información. En algunos casos incluso el potencial humano (las personas) también se lo puede considerar como activo de información, en especial quienes producen y manejan estratégicamente la información. En una organización con un SGSI implantado los activos de información son identificados y codificados para evaluar y tratar los posibles riesgos con el objetivo de 'hacerlos más seguros'.

2.1.2 Amenazas de la seguridad de la información

Los riesgos que eventualmente ocasionan que un activo de información se vea afectado en su confidencialidad, disponibilidad o integridad, provienen de amenazas internas y externas a la organización, hay muchas amenazas conocidas que van desde virus, piratas informáticos, averías de hardware, incluso desastres naturales que si se materializan puede destruir la información o dejar los sistemas fuera de línea. En el marco de un SGSI para los activos de información se deben identificar las amenazas a las cuales están expuestos, para así tomar acciones que eviten o minimicen las consecuencias cuando ocurra un evento que ponga en riesgo la seguridad de la información.

En resumen, las amenazas son las situaciones que potencialmente podrían desencadenar un incidente en la seguridad de la información explotando debilidades (vulnerabilidades) de los activos de información.

2.1.3 Objetivos de la Seguridad de la Información

La seguridad de la información se resume en acciones que persiguen objetivos medibles con respecto a la protección de los activos de información. Existen 3 pilares básicos en la seguridad de la información que ya se habían mencionado: disponibilidad, confidencialidad e integridad de la información. Por lo tanto, los objetivos primordiales de la seguridad de la información son:

1. Asegurar que la información esté disponible para quienes están autorizados en el momento que la requieran a través de los medios o sistemas destinos para ellos.

2. Asegurar que la información solo pueda ser vista por las personas autorizadas y mantener registro de acceso a esta información.

3. Asegurar que la información solo pueda ser modificada por las personas autorizadas y tener mecanismos para identificar si ocurren modificaciones no autorizadas.

Es necesario que estos objetivos se persigan de forma organizada y metodológica, varias organizaciones han realizado esfuerzos para recoger, organizar y validar las mejores prácticas tomadas de la experiencia de profesionales y entidades en materia de seguridad de la información. La forma más práctica es aplicar algún estándar con muchos casos de éxito comprobados.

2.2 ISO 27001

Los primeros esfuerzos para reunir las mejores prácticas en temas de seguridad de la información datan de 1989 cuando varias empresas británicas empezaron a compartir sus experiencias en busca de mecanismos claves para proteger la información de forma eficaz. Este conjunto de buenas prácticas se conoció como estándar BS 7799.

La Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) a través de comisiones técnicas y fundamentándose en otras normas, como ISO/IEC 17799:2005, la serie ISO 13335, ISO/IEC TR 18044:2004, elaboraron la Norma Internacional ISO/IEC 27001, la cual se ha mantenido

evolucionando desde la versión ISO/IEC 27001:2005 a la más actual la ISO/IEC 27001:2013 logrando así ser el estándar más conocido que proporciona requisitos para un sistema de gestión de seguridad de la información.

En la Tabla 1 se listan más normas de la misma familia que dan acompañamiento a la gestión de la seguridad de la información.

Tabla 1 Normas para la gestión de la seguridad de la información.

Código	Descripción
27002	Guía de buenas prácticas
27003	Guía para el diseño e implementación del SGSI
27004	Métricas para determinar la eficacia de un SGSI
27005	Gestión de riesgos
27006	Guía para la auditoría de un SGSI
27007	Gobernanza de la Seguridad de la Información
27008	Guía de auditoría de los controles seleccionados en la implantación de un SGSI
27009	Guía sobre el uso y aplicación de la ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte.
27010	Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores
27011	Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005
27013	Guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
27014	Guía de gobierno corporativo de la seguridad de la información.
27015	Guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.
27017	Guía de seguridad para computación en la nube alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
27018	Código de buenas prácticas en controles de protección de datos para servicios de computación en computación en la nube.
27042	Guía con directrices para el análisis e interpretación de las evidencias digitales.
27043	Principios y procesos de investigación para la recopilación de evidencias digitales.
27044	Gestión de eventos y de la seguridad de la información (SIEM)

2.2.1 Enfoque de la Norma

La ISO 27001 adopta un enfoque a procesos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el sistema de gestión de seguridad de la información de una organización. En el enfoque dado en la versión 2013 de la norma se incluye el ciclo de Deming que consiste en Planificar-Hacer-Verificar-Actuar (PHVA), presentado en la Figura 2.1 Ciclo de Deming., y puede ser aplicado a todos los procesos como una buena práctica para los ejercicios de mejora continua.

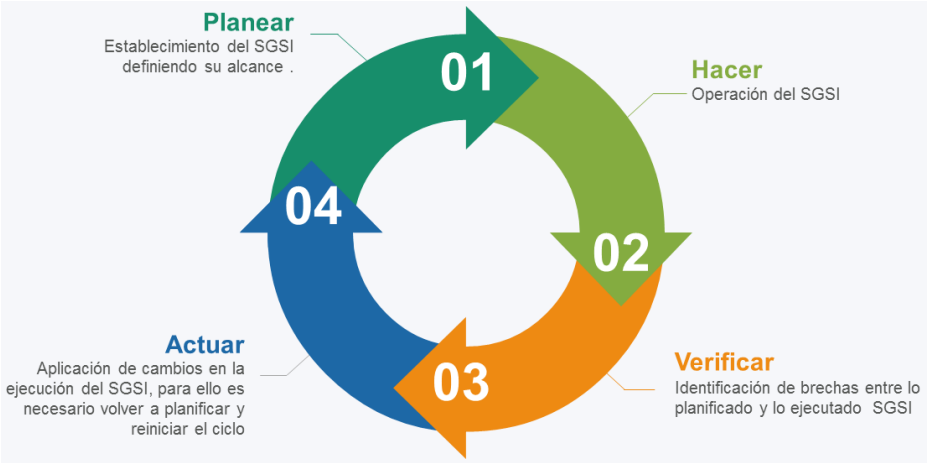


Figura 2.1 Ciclo de Deming.

Planear

Las actividades dentro de la planeación en el ciclo de Deming dan como consecuencia el establecimiento del SGSI definiendo su alcance en función de la organización, el negocio, los

procesos, interesados, etc. En esta fase también se contemplan otras actividades como:

1. Definición de políticas y directrices de la seguridad de la información.

2. Definición dela metodología de la evaluación de riesgos.

3. Identificación de riesgos.

4. Análisis y evaluación de riesgos.

5. Tratamiento de riesgos.

6. Selección de objetivos de controles y aplicación de los controles del anexo A de la norma.

7. Aprobación por parte de la dirección de riesgos y la implementación del SGSI.

8. Declaración de aplicabilidad (SOA).

Hacer

Las actividades dentro de la operación o ejecución en el ciclo de Deming dan como consecuencia la operatividad del SGSI, las actividades con mayor relevancia en esta fase son:

1. Implantación del plan de tratamiento de riesgos.

2. Implementación de los controles seleccionados en la fase de planificación.

3. Definición de un sistema de métricas/indicadores para la medición eficaz de los controles implementados.

4. Ejecución de campañas y programas de formación y concienciación en relación a la seguridad de la información para toda la organización

5. Gestión de las operaciones del SGSI.

6. Gestión de los recursos asignados al SGSI.

7. Implantación de procedimientos y controles preventivos, de detección y correctivos ante los incidentes de seguridad de la información.

Verificar

Las actividades dentro de la verificación o monitoreo en el ciclo de Deming dan como consecuencia la identificación de brechas entre lo planificado y lo ejecutado en el SGSI, las actividades con mayor importancia en esta fase son:

1. Ejecución de procedimientos de monitoreo.

2. Detección de errores en el procesamiento de la información.

3. Identificación de brechas e incidentes de seguridad.

4. Detección y prevención de eventos e incidentes de seguridad mediante el uso de indicadores.

5. Revisión regular de la efectividad del SGSI en función del cumplimiento de los objetivos.

6. Medición de la efectividad de los controles implementados.

7. Revisión regular en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables.

8. Realización periódica de auditorías internas del SGSI en lapsos planificados.

9. Revisión periódica del SGSI por parte de la dirección para garantizar que el alcance definido y las mejoras del SGSI son los adecuados.

10. Actualización de los planes de seguridad en función de las resultados y los nuevos Hallazgos en el monitoreo.

11. Registra de acciones y eventos de seguridad para analizar el impacto de estos en el SGSI.

Actuar

Las actividades dentro de la mejora continua en el ciclo de Deming dan como consecuencia la aplicación de cambios en la ejecución del SGSI, para ello es necesario volver a planificar y reiniciar el ciclo, las actividades con mayor importancia en esta fase son:

1. Implantación de las mejoras identificadas en el SGSI.

2. Ejecución de las acciones preventivas y correctivas adecuadas en función de lecciones aprendidas.

3. Comunicación de las acciones y mejoras a todas las partes interesadas con el nivel de detalle y los canales adecuados.

4. Verificación de que las mejoras planteadas alcanzarán los objetivos previstos.

2.2.2 Estructura de la Norma

Desde el 2012 se estable para todos los estándares ISO el Anexo SL el mismo que es una estructura de alto nivel para

tener un esquema unificado que permita la sintonía entre los diferentes sistemas de Gestión que se implementan en una empresa.

Por tanto, la norma ISO 27001:2013 evoluciona en estructura, contenido y se basa en este Anexo SL alineado al desarrollo documental de un Sistema de Gestión de Seguridad de la Información con lo que se consigue compatibilidad con todos marcos de referencia y normas relacionadas. En esta versión la estructura queda de la siguiente forma:

0.- Introducción: con respecto a la versión anterior si bien desaparece la sección “Enfoque del proceso” que describía el modelo PHVA, este sigue siendo la esencia del Sistema de Gestión de Seguridad de la Información (SGSI), tal como se definió en la sección anterior.

1.- Objeto y campo de aplicación: “en la norma ISO 27001:2013 se establece como obligatorio el cumplimiento de los requisitos especificados entre los capítulos 4 a 10 de dicho documentos, para poder obtener una conformidad de cumplimiento y así poder certificase” [3].

2.- Normas para consulta: La norma ISO 27001:2013 es una referencia normativa obligatoria y única, puesto que contiene todos los nuevos términos y definiciones utilizados.

3.- Términos y definiciones: Agrupa una consistente guía de términos y definiciones.

4.- Contexto de la organización: el objetivo de esta cláusula es identificar todos los problemas externos e internos que afectan a la empresa:

1. “Se intuyen todos los requisitos para definir el contexto del SGSI sin importar el tipo de empresa que sea y el alcance que tenga” [4].

2. “Se introduce una nueva figura como un elemento primordial para definir el alcance del SGSI” [4].

3. “Se establece la prioridad de identificar y definir todas las necesidades de las partes interesadas con relación a la seguridad de la información y las expectativas creadas por el SGSI ya que esto determinará las políticas de Seguridad de la Información y todos los objetivos a seguir para el proceso de gestión de riesgos” [4].

5.- Liderazgo: Se abarca el importante rol y compromiso que debe tener la alta dirección con el establecimiento del Sistema de Gestión de Seguridad de la Información, esto lo logra garantizando los siguientes puntos:

1. “Que los objetivos del SGSI y la política de seguridad de la información, antes se conocía como la política del SGSI” [4].

2. “La disponibilidad de todos los recursos para la implantación del SGSI” [4].

3. “Que los roles y las responsabilidades para la seguridad de la información se asignan y se comunican de forma adecuada” [4].

6.- Planeación: Los objetivos de seguridad se deben definir claramente y contar con planes específicos para conseguirlos los mismos. En el proceso de evaluación de riesgos podemos resaltar que:

1. “La metodología se enfoca con el objetivo de identificar todos los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información” [4].

2. “El nivel de riesgos se determina con base a toda probabilidad de que ocurra un riego y las consecuencias generadas, si el riesgo se materializa” [4].

7.- Soporte: comprende los recursos, personal competente, concienciación y comunicación de todas las partes interesadas.

Aparece el término “información documentada”, donde se estable el proceso de documentar, mantener, controlar y conservar la documentación que corresponde al SGSI.

8.- Operación: “Establece todos los requisitos para medir el funcionamiento del SGSI, todas las expectativas de la gerencia de la organización y la retroalimentación sobre estas, además de cumplir con la norma ISO 27001:2013” [4].

“Además, la organización plantea y controla las operaciones y los requisitos de seguridad, el pilar de este proceso se centra en realizar las evaluaciones de riesgos de seguridad de la información de forma periódica por medio de un programa elegido” [4].

“Todos los activos de información, las vulnerabilidades y las amenazas ya no son la base principal de la evaluación de riesgos; Solo se requieren para realizar la identificación de los

riesgos, que están asociados a la confidencialidad, la integridad y la disponibilidad” [4].

9.- Evaluación del desempeño: “La base para poder realizar la identificación y la medición de la eficiencia y el desempeño que realiza el SGSI continúan siendo las auditorías internas” [4].

“Se tiene que considerar el estado en el que se encuentran los planes de acción para poder atender las no conformidades como es debido, además se establece la necesidad de definir quién y cuándo realiza las evaluaciones, además de quien tiene que analizar la información que se ha recolectado” [4].

10.- Mejora: “El principal elemento del proceso de mejora son las no conformidades identificadas, las cuales tiene que contabilizarse y compararse con las acciones correctivas para asegurarse de que no se repitan” [4].

Lo indicado en párrafos anteriores se resume en la siguiente figura:

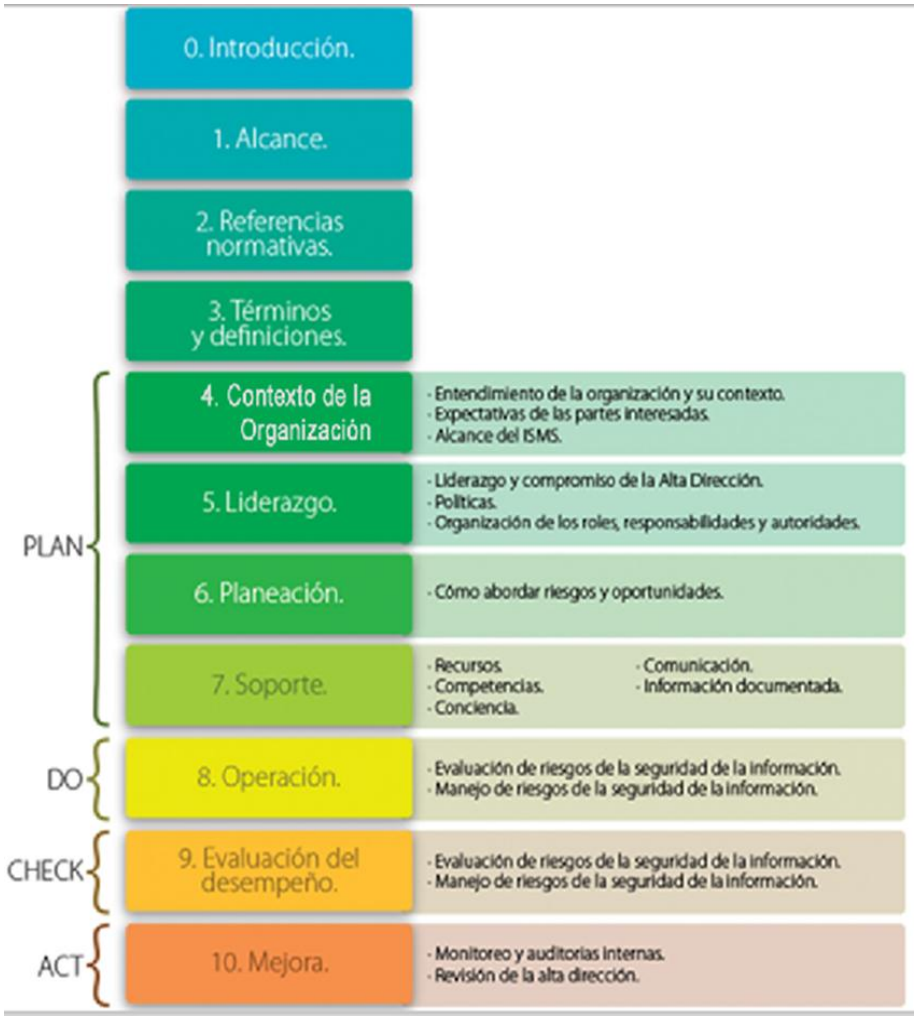


Figura 2.2 Anexo SL aplicado a ISO 27001:2013 [5].

Además de las cláusulas, en el Anexo de la norma se incluyen 114 controles cuyo cumplimiento se establece en la declaración de Aplicabilidad. Los dominios de acción que agrupan a dichos controles son:

A.5 Políticas de seguridad de la información.

A.6 Organización de la seguridad de la información.

A.7 Seguridad relativa a los recursos humanos.

A.8 Gestión de activos.

A.9 Control de acceso.

A.10 Criptografía.

A.11 Seguridad física y medioambiental.

A.12 Seguridad de las operaciones.

A.13 Seguridad de las comunicaciones.

A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.

A.15 Relación con proveedores.

A.16 Gestión de incidentes de seguridad de la información.

A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio.

A.18 Cumplimiento.

2.2.3 Cambios de ISO 27001:2005 a ISO 27001:2013

Una vez que la organización ISO realiza el esfuerzo de homologar las normas a través del Anexo SL definiendo así la estructura y el formato común para todas las nuevas normas de sistemas de gestión ISO y revisiones de las normas existentes, se asegura el texto común entre cada norma de sistemas de gestión y se logra una homologación de títulos de las cláusulas, secuencia de títulos, texto y definiciones.

Es necesario entonces revisar los cambios que existen entre la versión 2005 y la versión 2013 de la norma ISO 27001, sobre todo en los controles descritos en el anexo A. A continuación el resumen de los cambios que deberían considerarse para una migración del SGSI, como se muestra en la Tabla 2, Tabla 3, Tabla 4 y Figura 2.3 Mapeo de cambios a nivel de cláusulas..

Tabla 2 Resumen de cambios entre las versiones.

Versión 2005	Versión 2013
5 Cláusulas.	7 Cláusulas.
	En Capitulo Introducción se elimina la sección “Enfoque del proceso”.
Los términos y las definiciones en la ISO 27001:2005.	Pasan a la sección 3 en “Fundamento y vocabulario”.
El anexo A tiene 11 categorías de control (del 5 al 15) → 133 controles.	El anexo A tiene 14 categorías de control (del 5 al 18) →114 controles.
Se manejaba el rol propietario de los activos.	Se considera el rol propietario de los riesgos.
	“El proceso para evaluar los riesgos ya no se encuentra enfocado a los activos, las vulnerabilidades y las amenazas” [4].
	“Se elimina el término propietario del activo y se adopta el término propietario del riesgo” [4].
No menciona la ISO 31000 u otro estándar.	Menciona a la ISO 31000 en la cláusula 6.1 Acciones para la dirección de riesgos y oportunidades

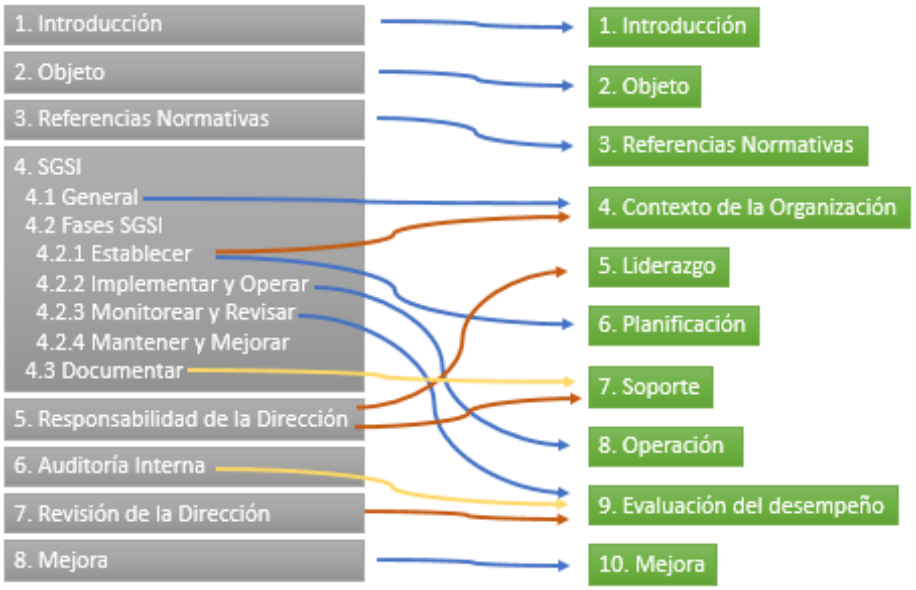


Figura 2.3 Mapeo de cambios a nivel de cláusulas.

Tabla 3 Controles retirados en la versión 2013 [5].

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.6.1.1	Comité de gestión para la seguridad de la información	Roles de la seguridad de la información y responsabilidades	A.6.1.3 y A.8.1.1
A.6.1.2	Coordinación de seguridad de la información	Contacto con autoridades	A.6.1.6
A.6.1.4	Procesos de autorización para instalaciones para procesamiento de información	Seguridad de la información en la gestión de proyectos	
A.6.2.1	Identificación de riesgos relacionados con agentes externos	Política de dispositivo móvil	A.11.7.1
A.6.2.2	Direccionamiento de seguridad al tratar con clientes	Trabajo a distancia	A.11.7.2

Control	Descripción	Cambia por	Incluye los controles de la ISO 27001:2005
A.10.2.1	Entrega del servicio		
A.10.7.4	Seguridad del sistema de documentos		
A.10.8.5	Sistema de información de negocios		
A.10.10.2	Seguimiento al uso de sistema		
A.10.10.5	Falla en el registro		
A.11.4.2	Autenticación de usuarios para conexiones externas		
A.11.4.3	Identificación de equipos		
A.11.4.4	Puerto remoto de diagnóstico y configuración de protección		
A.11.4.6	Control para la conexión de redes		
A.11.6.2	Aislamiento del sistema sensible		
A.12.2.1	Validación de datos de entrada	Controles contra *malware*	A.10.4.1
A.12.2.2	Control de procesamiento interno		
A.12.2.3	Integridad de mensaje		
A.12.2.4	Validación de datos de salida		
A.12.5.4	Filtración de la información		
A.15.1.5	Prevención del uso indebido de las instalaciones para el procesamiento de información		
A.15.3.2	Protección de las herramientas de auditoría de sistemas de información		

Tabla 4 Nuevos Controles en la versión [5].

Control	Descripción	Absorbe los controles de la ISO 27001:2005
A.6.1.4	Seguridad de la información en la gestión de proyectos	
A.12.6.2	Restricciones en la instalación de software	
A.14.2.1	Política de desarrollo de seguridad	
A.14.2.5	Desarrollo de procedimientos para el sistema	
A.14.2.6	Desarrollo de un entorno seguro	
A.14.2.8	Sistema de prueba de seguridad	
A.15.1.1	Información de seguridad para las relaciones de proveedores	A.6.2.3
A.15.1.3	Cadena de suministro ICT	
A.16.1.4	Evaluación y decisión de los eventos de seguridad de la información	
A.16.1.5	Respuesta a incidentes de seguridad de la información	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	
A.17.2.1	Disponibilidad de las instalaciones para procesamiento de información.	

A medida que se investiga más sobre los cambios entre a versión 2013 de la ISO 27001 y su inmediata sucesora, muchos auditores, consultores, implementadores y entendidos en el tema coinciden en que esta nueva versión refleja una mayor

flexibilidad para su implantación en las organizaciones sin importar su tamaño, así como la necesidad de adaptarse mejor a la exigencia de las nuevas tecnologías.

2.2.4 Sistema de Gestión de la Seguridad de la Información (SGSI).

"El SGSI es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información" [6].

El SGSI preserva la confiabilidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y le da confianza a las partes interesadas de que los riesgos son manejados adecuadamente. Esto es aplicable a cualquier organización, independientemente del tipo, tamaño y giro de negocio.

"El desarrollo de un SGSI representa un enfoque proactivo, sistemático, y lógico para resolver los problemas de seguridad de la información en lugar del enfoque reactivo para la identificación de brechas de seguridad" [3].

Establecer y operar un SGSI

El establecimiento y operación de un SGSI, necesariamente resultará en una reducción inmediata en los riesgos de seguridad de la información. Esencialmente, un SGSI es una herramienta que permite a una organización lograr y controlar sistemáticamente el nivel de desempeño de seguridad de información que se ha fijado.

De manera concreta, el SGSI debe proporcionar beneficios económicos como:

1. Reducción del tiempo de investigación de violaciones de seguridad.

2. Reducción del tiempo en el proceso de formación de personal nuevo.

3. Reducción de litigios, gastos legales.

4. Posibles reducciones en primas de seguros.

5. Mejoramiento en la percepción de la imagen comercial.

6. Protección de los activos de información.

7. Incremento en los niveles de concienciación con respecto a la seguridad de la información

8. Mejoras en el proceso de contratación del personal.

9. Aumentar la confianza con los clientes y demás partes interesadas.

Dado que el SGSI incorpora el ciclo PHVA dentro de cada actividad, la ejecución del mismo ya no se convierte en una actividad de fiscalización aislada si no en una parte integral del negocio. Así que la implementación y operación del SGSI está basado en la gestión de los riesgos para la seguridad de la información, es decir, la implementación de controles para llevar dichos riesgos a niveles aceptables.

Documentación SGSI

La documentación de una organización se estructura en función del tamaño, tipo de actividades, alcance del SGSI, la complejidad de los requisitos en seguridad de la información y el sistema de gestión.

Un documento es prácticamente cualquier cosa que proporciona información, puede ser un registro, procedimiento, especificación, gráfico o informe. La información puede

presentarse en papel, cinta magnética, disco de computadora, fotografía, muestras de maestros o una combinación de éstos.

El enfoque flexible de la norma trata de relevar la implementación, mantenimiento y mejora del SGSI, por ello la organización debe decidir sobre la estructura y el formato de la documentación que se necesita para soportar al SGSI. Toda información documentada tiene que ser controlada; los siguientes criterios son esenciales para el control de un documento:

1. Título.
2. Número.
3. Estado.
4. Número de página; total de número de páginas.
5. Revisión.
6. Aprobación.
7. Fecha de Emisión.

En las siguientes tablas (Tabla 5, Tabla 6 y Tabla 7) se mencionan los documentos que son revisados y aquellos que se recomiendan tener en una auditoría del SGSI:

Tabla 5 Información documentada en SGSI.

Documento	Cláusula/Anexo
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento de riesgos6.1.2	
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del riesgo	6.1.3 e), 6.2
Informe de evaluación de riesgos	8.2
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI *	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1

Tabla 6 Otra documentación en el SGSI.

Documentos	Cláusula/Anexo
Procedimiento para control de documentos	7.5
Controles para gestión de registros	7.5
Procedimiento para auditoría interna	9.2
Procedimiento para medidas correctivas	10.1
Política Trae tu propio dispositivo (BYOD)	A.6.2.1
Política sobre dispositivos móviles y tele-trabajo	A.6.2.1
Política de clasificación de la información	A.8.2.1, A.8.2.2, A.8.2.3
Política de claves	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1,A.9.4.3
Política de eliminación y destrucción	A.8.3.2, A.11.2.7
Procedimiento para trabajo en áreas seguras	A.11.1.5
Política de pantalla y escritorio limpio	A.11.2.9
Política de gestión de cambio	A.12.1.2, A.14.2.4
Política de creación de copias de seguridad	A.12.3.1
Política de transferencia de la información	A.13.2.1, A.13.2.2, A.13.2.3
Análisis del impacto en el negocio	A.17.1.1
Plan de prueba y verificación	A.17.1.3
Plan de mantenimiento y revisión	A.17.1.3
Estrategia de la continuidad del negocio	A.17.2.1

Tabla 7 Registros y formatos de evidencias.

Registros	Cláusula/Anexo
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.2
Resultados de las auditorías internas	9.2
Resultados de la revisión por parte de la dirección	9.3
Informe de evaluación de riesgos	8.2
Resultados de acciones correctivas	10.1
Registros sobre actividades de los usuarios, excepciones y eventos de seguridad	A.12.4.1, A.12.4

En esta última tabla se hacía referencia a la información documentada como evidencias (registros). El estándar ISO 27001 define un registro como una: “declaración de resultados o evidencia de actividades realizadas”, es decir, la organización debería mantener registros para proporcionar evidencias de conformidad y cumplimiento de los requisitos y para determinar la eficacia del SGSI.

Los registros (físicos o digitales) deben ser simples, legibles, fácilmente identificables y recuperables. Ellos deben proporcionar administración con información útil para la mejora continua. De allí la importancia de que la gestión de documentos y registros tenga un esquema de fácil trazabilidad,

de preferencia a través de un aplicativo de gestión documental que permita la consulta y recuperación de los documentos.

Auditoria Interna

La auditoría interna del SGSI es un examen sistemático, objetivo e independiente de los procesos, actividades, operaciones y resultados de la organización, así mismo permite emitir juicios basados en evidencias sobre los aspectos más importantes de la gestión, los resultados obtenidos y la satisfacción de los diferentes grupos de interés.

Con respecto a un SGSI, se recomiendan los siguientes pasos para la organización de las auditorías:

1. **Planificación.-** se define el programa de auditoría para el año incluyendo áreas y responsables. Se seleccionan auditores y se prepara la información necesaria para la ejecución (revisión documental y en sitio). Se define el plan de trabajo general.

2. **Revisión documental.-** se realiza la revisión de los procesos de gestión de seguridad de la información recopilando los registros mínimos con los cuales debe contar el SGSI. Aún no se revisan controles.

3. **Revisión en sitio.-** se revisan los controles de seguridad de la información y su evidencia (registros). El plan de trabajo de auditoría debe incluir el enfoque de revisión (ej. número de muestras a realizar, atributos de control a verificar - suelen estar en las políticas y procedimientos).

4. **Análisis de resultado.-** se comparan los resultados obtenidos contra lo establecido en las políticas y procedimientos tanto para procesos como controles de seguridad de la información. Se determinan si existieron desviaciones, se confirman con los auditados.

5. **Elaboración de registros.-** se elaboran los registros mínimos de este proceso: Plan de Auditoría diligenciado e Informe de Resultados.

6. **Presentación de resultados.-** para esta tarea la solución propuesta también permite registrar las trazas de los informes de auditoría y de los formatos de acciones correctivas.

Este proceso de la operación y mejora del SGSI es uno en los que la solución propuesta contribuirá enormemente a que gane agilidad al permitir que la revisión de las referencias documentales (políticas, procedimientos, instructivos, manuales,

registros, etc.) se realizase en línea y previamente asociados a los controles implementados.

2.2.5 Administración del Riesgo

Para la implementación del SGSI, desde su planificación se debe definir una metodología para la administración de los riesgos la cual describirá los procesos generales para:

1. Identificación de activos.
2. Identificación de amenazas y vulnerabilidades.
3. Análisis y evaluación de los riesgos.
4. Tratamiento de los riesgos.
5. Aplicación de controles.
6. Monitoreo de riesgos.

La siguiente figura resume el ciclo de la gestión de los riesgos en ISO 27001:

Figura 2.4 Ciclo de la gestión de los riesgos [6].

El análisis de riesgos de los activos de información permite identificar, analizar, evaluar y definir el manejo de los riesgos, para así apoyar el cumplimiento de los objetivos de la organización, y disminuir a un nivel aceptable el impacto de la materialización de dichos riesgos; la gestión de riesgos permite que los responsables de los procesos conozcan los riesgos de sus activos de información y acompañen de manera más efectiva la implementación de los controles y acciones de mejora.

El enfoque de riesgos definido se basa en la identificación de las amenazas y vulnerabilidades presentes en los activos a analizar; el cálculo de la probabilidad y el impacto de

materialización de los riesgos y cómo pueden afectar las actividades impidiendo el logro de los objetivos.

Con base en los estándares NTC/ISO 27005 el desarrollo de este procedimiento consta de los siguientes puntos, según la Tabla 8:

Tabla 8 Gestión de riesgo según la ISO 27005.

Valoración	Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables teniendo en cuenta la metodología aplicada en la organización.
Planificación	1. Definir el equipo metodológico que será encargado de apoyar la actividad de identificación de riesgo. 2. Seleccionar los activos fijos sujetos al análisis de riesgos
Identificación	1. Describir el riesgo. 2. Identificar las causas (mapeos de amenaza-vulnerabilidad). 3. Identificación de los controles existentes.
Análisis y Evaluación	1. Estimar los niveles de los riesgos. a. Identificación de la probabilidad. b. Identificación del impacto. 2. Evaluar e Identificar las opciones para el tratamiento de los riesgos. 3. Seleccionar los controles para el tratamiento de los riesgos.

La norma ISO/IEC 27005 es una directriz que contiene los lineamientos metodológicos que se deben cumplir para la evaluación de riesgos de seguridad de la información. Es muy importante señalar que esta norma no es una metodología en

sí, sin embargo, lo que propone es un proceso para gestionar riesgos de la seguridad de la información, lo cual implica que, al ser un proceso, la evaluación de riesgos podrá ser sometida a una mejora continua (de nuevo se puede aplicar el ciclo de Deming).

Independientemente de la metodología, los riesgos a gestionarse serán de 2 tipos:

1. **Riesgo inherente.-** es aquel que existe sobre los activos de información en ausencia de controles.

2. **Riesgo residual.-** es aquel que permanece después de que la organización haya implementado controles.

En cualquiera de los 2 casos la fórmula del riesgo estará en función de:

1. **Impacto.-** es la afectación que un proceso, considerado en el alcance del SGSI, tendría si un riesgo llegara a materializarse.

2. **Vulnerabilidad.-** nivel de exposición que los activos de información tendrían ante determinado escenario de riesgo debido a una falla o carencia de controles.

3. **Probabilidad.-** es el atributo que hace referencia a la posibilidad de que un riesgo se materialice, se entiende que mientras el activo de información es más vulnerable, la probabilidad de ocurrencia del riesgo será mayor.

Con base en los conceptos descritos, la fórmula del riesgo es la siguiente:

Riesgo (valor) = Probabilidad x Impacto (4.1)

En la Figura 2.5 Flujo básico de la gestión del Riesgo. se puede apreciar un flujo básico para la gestión de riesgos en donde se resalta la obtención de los valores para cada riesgo.

Figura 2.5 Flujo básico de la gestión del Riesgo.

El valor de un riesgo justamente es el que se aprecia como parámetro de salida en el método de evaluación de riesgos que se defina en la organización, dicho método de evaluación puede ser cualitativo o cuantitativo. En ambos métodos se define impacto y probabilidad.

En el caso de la evaluación cualitativa los niveles de riesgo por niveles de importancia, como "Alto", "Medio" y "Bajo" son el resultado de combinar el impacto y probabilidad tal como se

aprecia en la Figura 2.6 Método Cualitativo para la gestión de Riesgos..

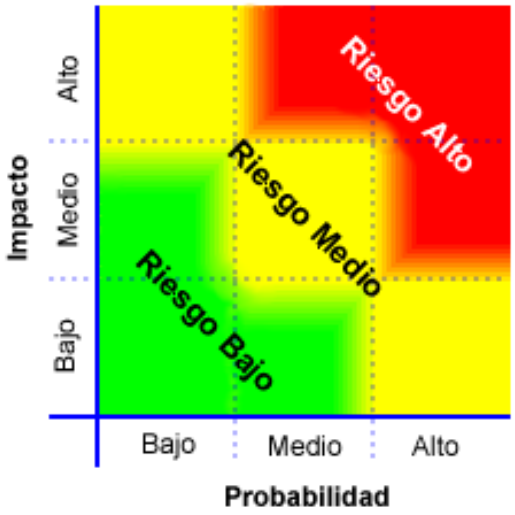


Figura 2.6 Método Cualitativo para la gestión de Riesgos.

En la evaluación cuantitativa se estiman valores prácticos de impacto y probabilidad, y se producen valores del nivel de riesgo en unidades específicas. Llevar a cabo un análisis cuantitativo completo no siempre es posible o deseable debido a la falta de información sobre los activos de información, amenazas y vulnerabilidades que se está analizando, falta de datos confiables, influencia de los factores humanos, falta de justificación del esfuerzo de análisis cuantitativo, etc. En tales escenarios, la aplicación del método cualitativo de riesgos bajo el juicio de expertos con conocimientos en sus respectivos campos, puede ser eficaz.

En la Figura 2.7 Método Cuantitativo para la gestión de Riesgos se presenta un ejemplo de los niveles de impacto y probabilidad y el nivel de riesgo resultante por cada combinación a través de un método cuantitativo:

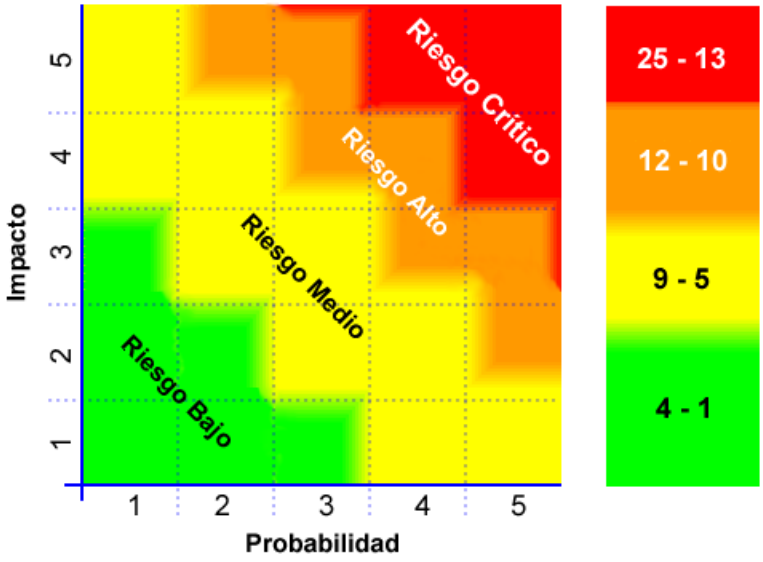


Figura 2.7 Método Cuantitativo para la gestión de Riesgos.

Usando cualquiera de los métodos para la evaluación de riesgos, si el resultado de este cálculo no está dentro de los parámetros aceptables en concordancia con el apetito de riesgo definido por la organización, es decir, el resultado del riesgo dentro de la matriz térmica o de un mapa de calor está en el cuadrante rojo, el riego debe ser tratado mediante controles.

En el capítulo 4 se dará más detalle de como la solución propuesta con el Módulo de Gestión de Riesgos

correspondiente ayuda al equipo metodológico involucrado en la implementación del SGSI con los Riesgos.

2.2.6 Controles

De acuerdo a lo descrito en el apartado anterior sobre la gestión de riesgos, la norma indica que el tratamiento de los mismos debe hacérselo a través del establecimiento de controles, indicado con la flecha roja en la Figura 2.8.

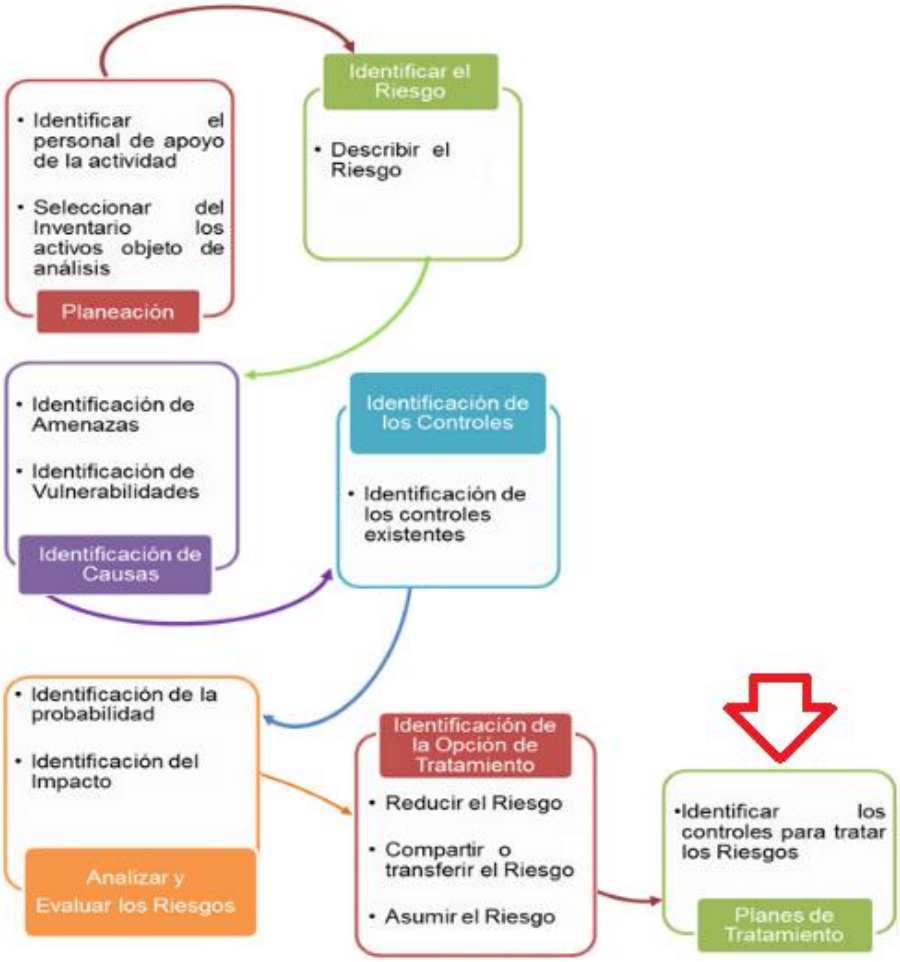


Figura 2.8 Actividades de la gestión de Riesgos [7].

Los controles deben ser definidos en función del par amenaza vulnerabilidad que se estableció como causa en el análisis del riesgo evaluado, para la selección de controles se puede tener en cuenta el Anexo A de la norma ISO 27001. La naturaleza de dichos controles puede hacer que sean preventivos o correctivos, a saber:

1. **Controles Preventivos**.- Los controles preventivos son aquellos que están enfocados en la mitigación de las causas (amenaza - vulnerabilidad) para evitar su materialización.

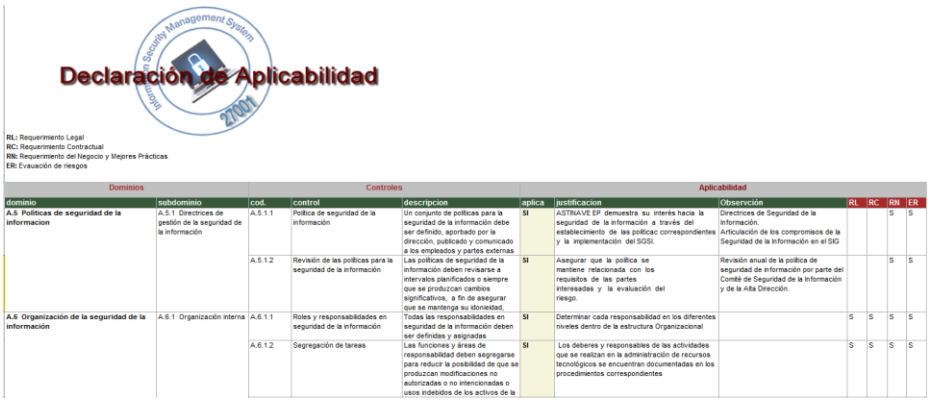
2. **Controles Correctivos**.- Los controles correctivos están enfocados en la recuperación de los activos luego de la materialización del riesgo.

Declaración de aplicabilidad

La Declaración de Aplicabilidad (SoA: Statement of Applicability por sus siglas en inglés), es un requisito y se lo incluye en la documentación obligatoria indicada por la norma ISO 27001 que contribuye a mantener el registro y control de las medidas en seguridad de la información que son aplicadas por la organización.

En este documento se enlistan los 114 controles establecidos en el Anexo A que sirven como una referencia para la implementación de medidas de protección de la información; se indica si el control estará considerado en el SGSI y la correspondiente justificación sea que esté incluído o descartado (ver Figura 2.9). Los controles a ser implementados se sobreentienden como objetivo de control, no obstante, la declaración de aplicabilidad no se restringe a los controles del

anexo ya que pueden constar otros controles operacionales propios quizás de un sistema integrado de gestión o de un marco de buenas prácticas ya aplicados en la organización donde se quiera implantar el SGSI.



Declaración de Aplicabilidad

RL: Requerimiento Legal
RC: Requerimiento Contractual
RN: Requerimiento del Negocio y Mejores Prácticas
ER: Evaluación de riesgos

Dominios		Controles			Aplicabilidad						
dominio	subdominio	cod.	control	descripcion	aplica	justificacion	Observción	RL	RC	RN	ER
A.5 Políticas de seguridad de la informacion	A.5.1 Directrices de gestión de la seguridad de la información	A.5.1.1	Política de seguridad de la información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas	SI	ASTINAVE EP demuestra su interés hacia la seguridad de la información a través del establecimiento de las políticas correspondientes y la implementación del SGSI.	Directrices de Seguridad de la Información. Articulación de los compromisos de la Seguridad de la Información en el SIG			S	S
		A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de la información deben revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad.	SI	Asegurar que la política se mantiene relacionada con los requisitos de las partes interesadas y la evaluación del riesgo.	Revisión anual de la política de seguridad de información por parte del Comité de Seguridad de la Información y de la Alta Dirección.			S	S
A.6 Organización de la seguridad de la información	A.6.1 Organización interna	A.6.1.1	Roles y responsabilidades en seguridad de la información	Todas las responsabilidades en seguridad de la información deben ser definidas y asignadas	SI	Determinar cada responsabilidad en los diferentes niveles dentro de la estructura Organizacional		S	S	S	S
		A.6.1.2	Segregación de tareas	Las funciones y áreas de responsabilidad deben segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la	SI	Los deberes y responsables de las actividades que se realizan en la administración de recursos tecnológicos se encuentran documentadas en los procedimientos correspondientes		S	S	S	S

Figura 2.9 Vista de la declaración de aplicabilidad generada desde el sistema.

Monitoreo

Seguido a la validación del plan para gestionar los riesgos, incluyendo matriz y mapa de riesgos, es necesario que estos riesgos sean monitoreados considerando que las amenazas no desaparecen para la organización.

“El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficacia en su implementación adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden

estar influyendo en la aplicación de las acciones preventivas” [7].

“A partir del análisis y calificación de riesgos, se debe formular un plan para el tratamiento de riesgos que identifique la gestión apropiada, los recursos, responsabilidad y prioridades para manejar los riesgos de la seguridad de la información” [7].

“La organización debe ejecutar procedimientos de seguimiento y revisión para detectar oportunamente los errores en los procesamientos e identificar con prontitud incidentes e intentos de violación de seguridad, así como determinar si las ac tomadas para solucionar un problema de seguridad fueron eficaces” [7].

Justamente en la administración de los riesgos y su ciclo de mejora continua es en donde se encuentra el mayor esfuerzo de carga administrativa, incluso logística para mantener actualizados los cambios, asociar documentación, registrar planes y acciones y sobre todo dejar trazabilidad, así que donde el sistema de información propuesto hará su contribución a la gestión de un SGSI.

CAPÍTULO 3

SITUACIÓN ACTUAL Y LEVANTAMIENTO DE NECESIDADES

3.1 Esquema Gubernamental de Seguridad de la Información (EGSI)

Para las entidades del estado las Tecnologías de Información y Comunicación (TIC) son herramientas fundamentales para el cumplimiento de sus objetivos, por tanto, cuentan con activos informáticos que están expuestos a riesgos como sea visto en capítulos anteriores.

Bajo esta premisa la Secretaría Nacional de la Administración Pública (SNAP) con el propósito de generar confianza en la ciudadanía acerca

de la administración de estos activos informáticos toma varias acciones reflejadas en acciones y normativas.

En el 2011 se conformó una comisión para la seguridad informática y de las tecnologías de la Información y Comunicación de las entidades públicas o dependientes de ellas. Esta comisión determinó las normas y procedimientos prioritarios que deben ser parte de la cultura y procesos de las entidades del Estado entregando en el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma INEC ISO/IEC 27002.

Se le da más fuerza a esta iniciativa con el Acuerdo Ministerial 166 del 25 de septiembre del 2013 donde se dispone a la Administración Pública, Institucional y dependiente de la Función Ejecutiva la Gestión de la Seguridad de la Información de forma obligatoria y basándose en las Normas Técnicas NTE INEN-ISO/IEC 27000 publicadas por el Instituto Ecuatoriano de Normalización INEN que se basan en las Normas Técnicas Internacionales ISO 27000.

De forma general, desde su publicación, cada entidad debe designar un Comité de Seguridad de la Información y un Oficial de Seguridad de la Información que encabezará el Comité en 30 días, el plazo de implementación es de 18 meses, sin embargo, se establecen algunos requerimientos que deben ser implementados en solo 6 meses.

La máxima autoridad de la misma entidad es la responsable de que se lleve el registro y organización de toda la documentación que evidencie la implementación del EGSI. También debe considerarse la Gestión de Riesgos según la Norma Técnica respectiva y cualquier excepción en la implementación o control que no esté definido en el EGSI debe ser comunicada y aprobada por la Secretaria Nacional Técnica de la Administración Pública.

Por su parte la Secretaría Nacional de la Administración Pública hará el seguimiento y control mediante el Sistema de Gestión por Resultados (GPR), la misma que se realizará de forma anual y cuando se den cambios importantes en la Norma. El Oficial de Seguridad de la Información de cada entidad es el representante de la misma para los temas de implementación y gestión de incidentes de seguridad de la información.

En el Anexo 1 de este acuerdo se detalla el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la norma INEC ISO/IEC 27002, conformado por una Introducción, un glosario de términos y los siguientes capítulos:

1. Política de seguridad de la información.

2. Organización de la seguridad de la información.

3. Gestión de los activos.

4. Seguridad de los recursos humanos.

5. Seguridad física y del entorno.

6. Gestión de comunicaciones y operaciones.

7. Control de acceso.

8. Adquisición, desarrollo y mantenimiento de sistemas de información.

9. Gestión de los incidentes de la seguridad de la información.

10. Gestión de la continuidad del negocio.

11. Cumplimiento.

El EGSI no se contrapone ni desplaza a la norma INEC ISO/IEC 27002 solo hace distinción en los hitos por capítulo que deber ser implementados de forma prioritaria y no prioritaria en la organización.

A la fecha el SNAP todavía sigue calificando el cumplimiento de hitos en el sector público y dando seguimiento a través de la herramienta en línea Gobierno Por Resultado (GPR) en la cual el EGSI fue registrado como un proyecto a finales del 2013. Con esta iniciativa se dio un gran paso para que las empresas del sector público dejaran el

desconocimiento de las buenas prácticas para la seguridad de la información, sin embargo, no se ha logrado una demanda masiva de certificaciones en la norma ISO 27001; sólo se destaca en solitario CNT con la certificación de un proceso muy puntual de uno de sus servicios en la ciudad de Quito. En este contexto no hay que olvidar tampoco que el EGSI se basa en la versión 2005 de la norma ISO 27001 y que el cambio de versión pudo haber repercutido (justo en el 2013) en que no se haya alcanzado el plazo de implementación de 18 meses a partir de la publicación del Acuerdo como se muestra en la Figura 3.1.

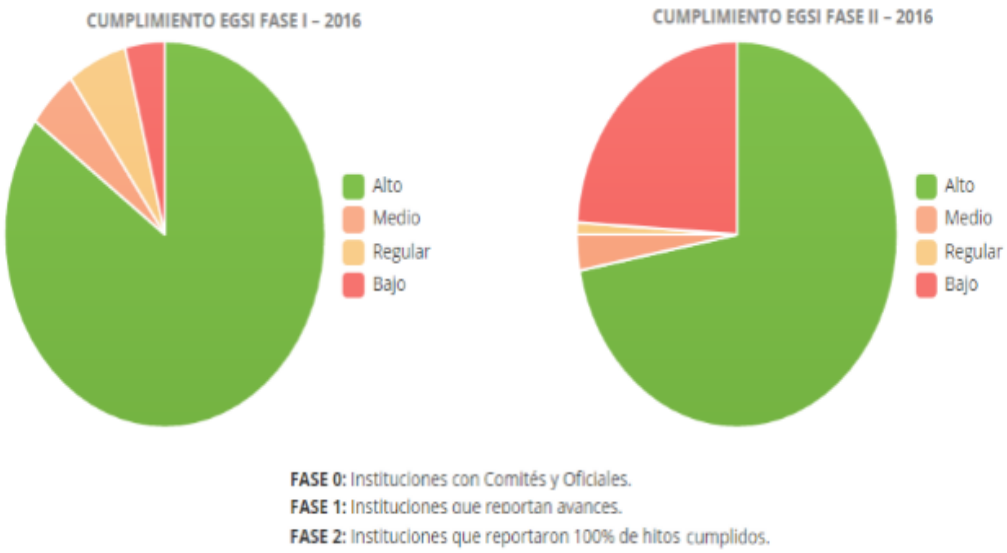


Figura 3.1 Indicares del cumplimiento del EGSI fase I y fase II [8].

3.2 Resolución de la Junta Bancaria 3066

En las resoluciones del año 2014 de la Junta Bancaria, se destaca la 3066 en la que se define la figura de un responsable de la información, incidentes de seguridad de la información, transacción, además se insta

a las instituciones del sector bancario y financiero a establecer al menos procedimientos para:

1. Gestión de incidentes
2. Inventario de la infraestructura tecnológica
3. Respaldo de información periódicos
4. Gestión del ciclo de vida de las aplicaciones
5. Separación de ambientes
6. Escaneo de vulnerabilidades
7. Control de cambios
8. Gestión de desempeño y capacidades de la infraestructura
9. Migración de plataforma tecnológica.

De manera explícita esta resolución dispone que las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio tomando como referencias el estándar ISO 22301, incluyendo a todas las actividades derivadas de tal proceso la incorporación de las gestión integral de riesgos.

Una de las secciones (la VII) se dedica de manera exclusiva a la seguridad de la información con el objeto de satisfacer las necesidades

de la entidad y salvaguardar la información contra uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones deben tomar como referencia la serie de estándares ISO/IEC 27000. Con ello las instituciones quedan obligadas a establecer, implementar, ejecutar, mantener y documentar un SGSI. Los artículos 21 y 22 dan detalles de lo exigido.

Esta resolución se aprobó en septiembre del 2014, provocando que al siguiente año hubiera un aumento de la demanda en las consultorías de implementación y auditorias de los sistemas integrados de gestión de los bancos incluyendo las requisitos de normas como ISO 22301, ISO 27001 e incluso la ISO 20000.

3.3 Estadísticas de seguridad de la información en Ecuador y la Región

Las razones por las cuales los especialistas en seguridad de la información piensan que habrá un repunte en la cantidad de organizaciones que acogerán el estándar ISO 27001 es porque justamente la seguridad de la información, con un énfasis muy marcado en la seguridad informática, es cada vez más importante y considerada dentro del engranaje empresarial, tanto así que cada vez más existe el espacio y recursos para los planes de seguridad dentro de la planificación estratégica de las empresas. En los siguientes puntos se

encontrarán las cifras que comprueban las tendencias en seguridad de la información en los 2 últimos años.

3.3.1 Delitos informáticos

De las muchas fuentes consultadas por los autores, se tomaron los datos obtenidos por los Laboratorios de ESET Latinoamérica que en sus informes del 2014 y 2015 señalan que el 50% del total de información que se filtra a nivel mundial corresponde a datos de empresas financieras.

Asimismo en el “I Foro Regional de Seguridad Informática: Malware y Cibercrimen en América Latina”, organizado por el mismo ESET. Los expertos afirmaron que en cuanto a seguridad informática, una de las tendencias más fuertes es el robo de información en el sector corporativo, por ejemplo, el coordinador del Laboratorio de ESET Latinoamérica indicó; “Según algunos registros, prácticamente el 50% de la información que se filtra en las empresas corresponden a empresas que se dedican a finanzas, entidades que tienen registros de compra, información de tarjetas de crédito y cuentas bancarias. Más allá de los ataques, es ver cuánta información recopilaron, por cuánto tiempo, de qué manera crecieron. En el 2014 los cibercriminales fueron más eficientes;

en solo seis meses, se robaron 500 millones de registros de usuarios. Más no es siempre mejor” [9].

Durante el 2014, se registraron menos ataques que en los dos años anteriores, en los cuales 2012 representó un pico, pero se afectó mucha más información; en solo dos ataques se vulneraron más de dos millones de registros. Los cibercriminales están apuntando a los empleados de estas empresas corporativas porque son los que tienen acceso a los sitios estratégicos, son los mismos que se encargan de asegurar a la empresa y desarrollar sistemas de protección. El objetivo final es robar contraseñas, que se consiguen en el 70% mientras que la filtración de usuarios se da en el 60% de acuerdo a los casos registrados en América Latina. En la siguiente Figura 3.2 se muestran los porcentajes de este tipo de incidentes por país:

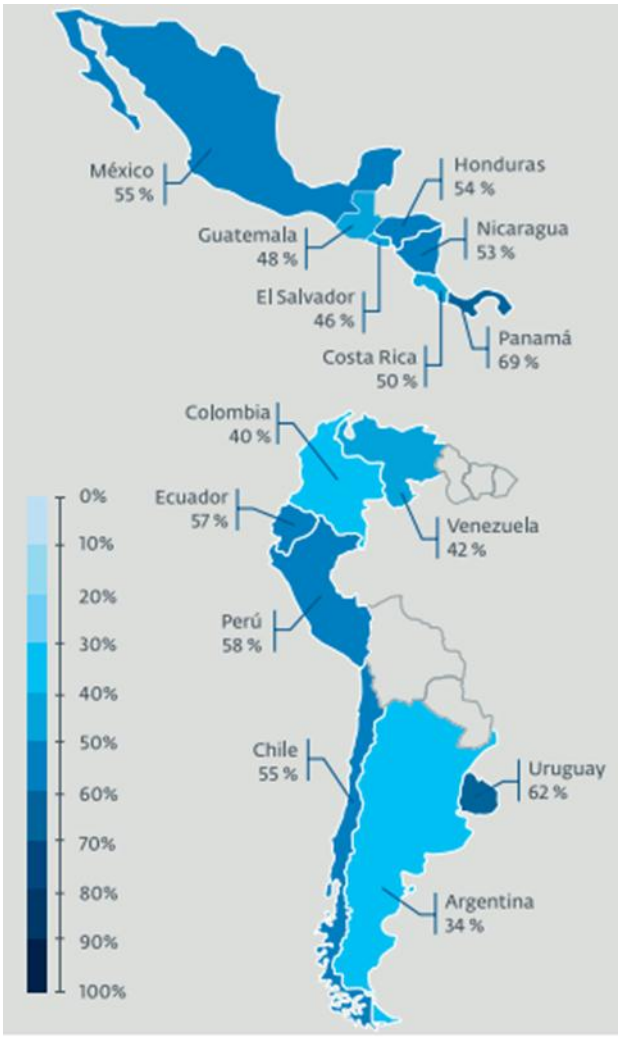


Figura 3.2 Porcentaje de empresa, por país que sufrieron incidentes relacionados con acceso indebido a aplicaciones y/o bases de datos [10].

En el “ESET Security Report, Latinoamérica 2015” se hizo una revisión completa de:

1. Las preocupaciones de las empresas en Latinoamérica (ver Figura 3.3).

2. Los incidentes ocurridos. (ver Figura 3.4).

3. Cómo se están protegiendo las empresas (ver Figura 3.5).

A más de ello se realizó un breve examen de la evolución del estado de la seguridad informática en los últimos 5 años. Las conclusiones arrojan que la percepción de seguridad de la información al igual que los incidentes que pueden sufrir no cambia mucho entre las organizaciones de diferentes tamaños.

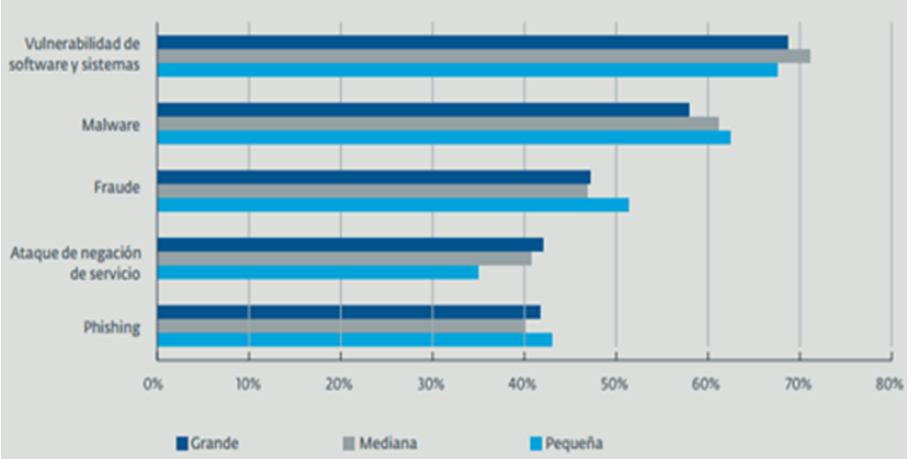


Figura 3.3 Preocupaciones de la seguridad de la información de las empresas de acuerdo a su tamaño [10].

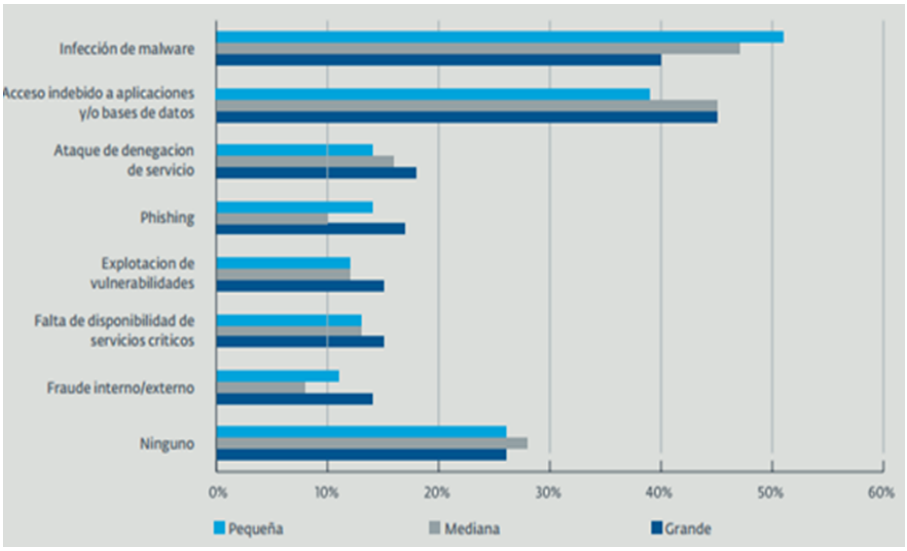


Figura 3.4 Incidentes ocurridos en empresas latinoamericanas [10].

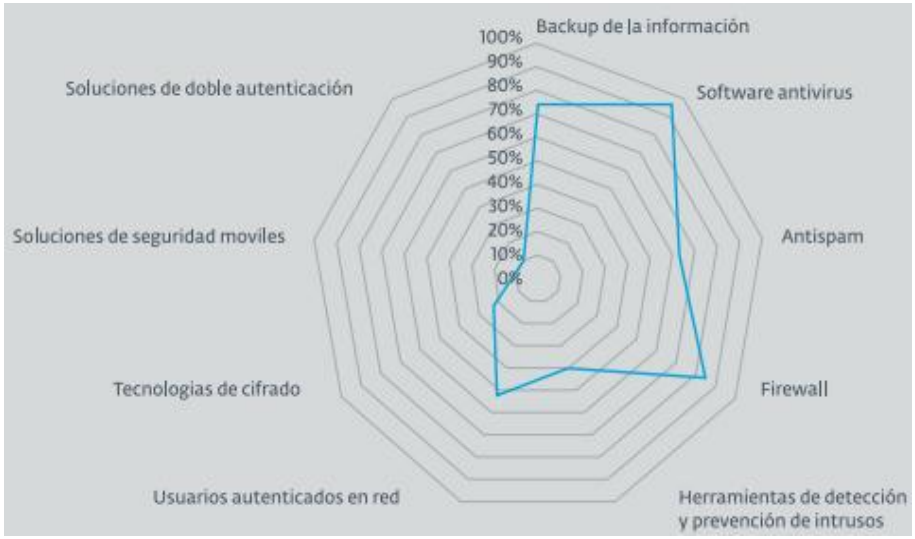


Figura 3.5 Porcentaje de empresas latinoamericanas que implementaron controles basado en tecnología [10].

Casos como Shellshock [11], Heartbleed [12] o Poodle [13] han abierto los ojos de muchos equipos de seguridad para considerar lo vulnerable que pueden llegar a estar si no se hace

la adecuada gestión de los controles de seguridad que están implementados. Además, con el tiempo se hace evidente que las Amenazas Persistentes Avanzadas (APTs) son cada vez más utilizadas, lo que implica que se debe pasar de la preocupación a la acción para garantizar el nivel de seguridad que la información requiere.

Se considera que es el momento más adecuado para que las empresas de la región comiencen a pensar en la gestión de la seguridad con una visión holística; no solamente con tener un antivirus, un firewall y políticas de seguridad en letra muerta se puede garantizar la Seguridad de la Información de forma más general. Es necesario expandir el análisis incluyendo nuevas tecnologías, no desconocer la diversidad de amenazas y, sobre todo, que todo los colaboradores de la organización estén al tanto de esta realidad; de esta se lograrán brindar los niveles de seguridad adecuados que permitan disfrutar de las posibilidades que la tecnología ofrece a las organizaciones.

Mientras más se lee sobre informes similares a los de ESET más queda en evidencia que el marco recomendado para orquestar el accionar en torno a la seguridad de la información es el estándar ISO 27001.

3.3.2 Empresas certificadas con ISO 27001

En la página oficial de la organización ISO se encuentran publicadas las estadísticas de organizaciones certificadas en el estándar ISO 27001.

.En la Figura 3.6, Figura 3.7 y la Tabla 9 se verifica que para Ecuador las iniciativas de certificación son muy escasas y que están muy por debajo de los líderes de la Región.

Figura 3.6 Certificaciones de ISO 27001 para Ecuador [1].

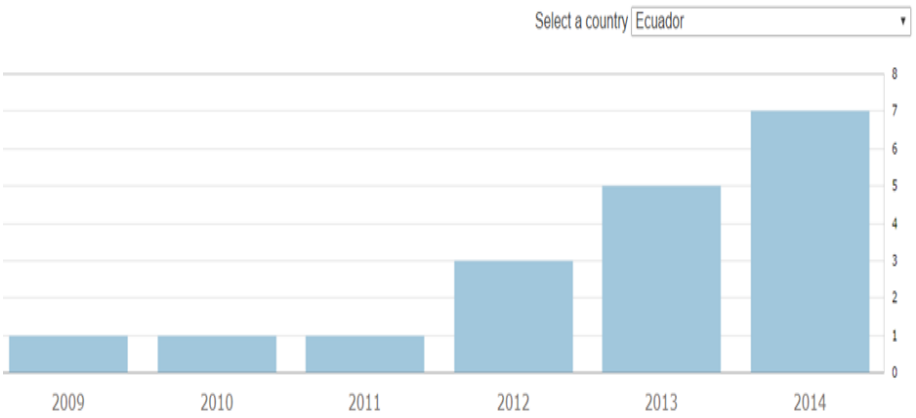


Figura 3.7 Cantidad de certificaciones ISO 27001 por año (Ecuador) [1].

Tabla 9 Cantidad de certificaciones ISO 27001 por año (Ecuador) [1].

ISO/IEC 27001 - Central / South America									
Year	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**
Country	**18**	**38**	**72**	**100**	**117**	**150**	**203**	**272**	**277**
Argentina	1	1	6	4	8	24	33	40	23
Barbados				1	1				
Bolivia				1	1	3	1	1	1
Brazil	10	25	40	48	41	50	53	82	86
Chile	2	3	7	10	13	18	23	24	25
Colombia	3	8	11	14	23	27	58	82	80
Costa Rica			2	5	6	7	7	10	22
Cuba			1	1	2			0	
Dominican Republic				1	1	2	3	4	3
Ecuador				1	1	1	3	5	7
El Salvador					1	1	1	1	1
Guatemala					1	1	1	2	3
Guyana				1	1			0	
Honduras						1	1	0	1
Jamaica				1	1			0	
Panama					1	1	2	1	
Peru	1	1	2	6	9	5	7	9	12
Puerto Rico			2	2	2	2	2	2	
Trinidad							1	1	1
Uruguay	1		1	4	4	7	7	8	11
Venezuela									1

El sitio oficial de la organización ISO no proporciona información sobre cuáles son las 7 empresas que en Ecuador están certificadas, sin embargo algunas de las que han dejado saber de su logro con este estándar son:

1. CNT
2. Telconet
3. Banco de Guayaquil
4. Movistar

No hay cifras oficiales de implantaciones de SGSI sin certificar, pero por EGSI y por la reglamentación de la Junta bancaria a las empresas del sector financiero, se debería esperar que bancos, cooperativas y sector público ya tengan implantados SGSI.

Lamentablemente Latinoamérica también está muy atrás de Asia y Europa los cuales lideran el ranking de certificación en este estándar, las siguientes figuras dan constancia de esta tendencia:

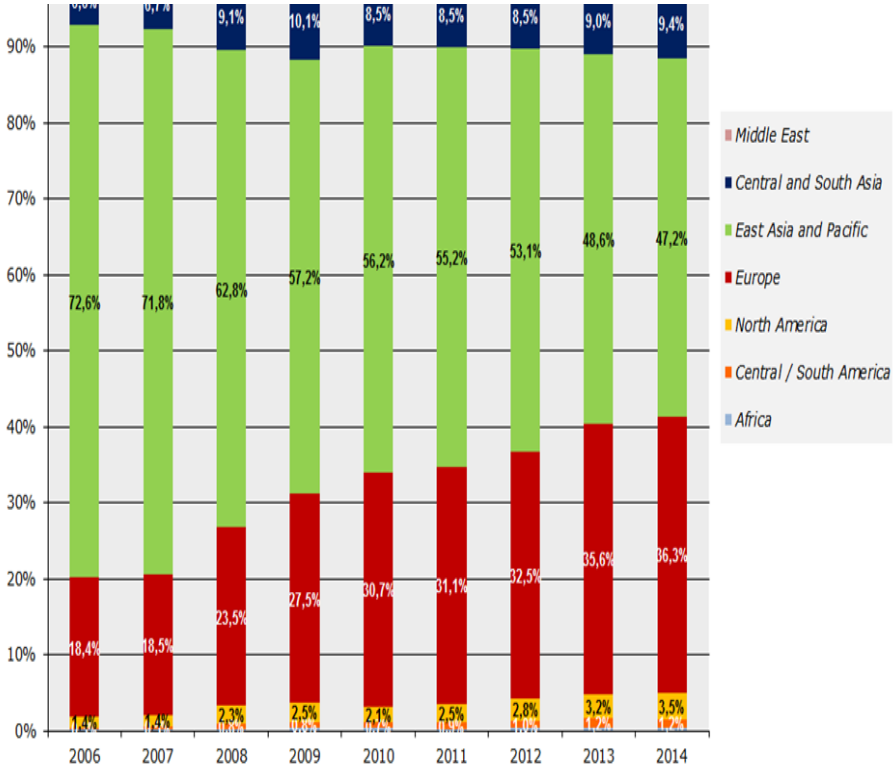


Figura 3.8 Porcentaje de certificaciones 27001 por región [1].

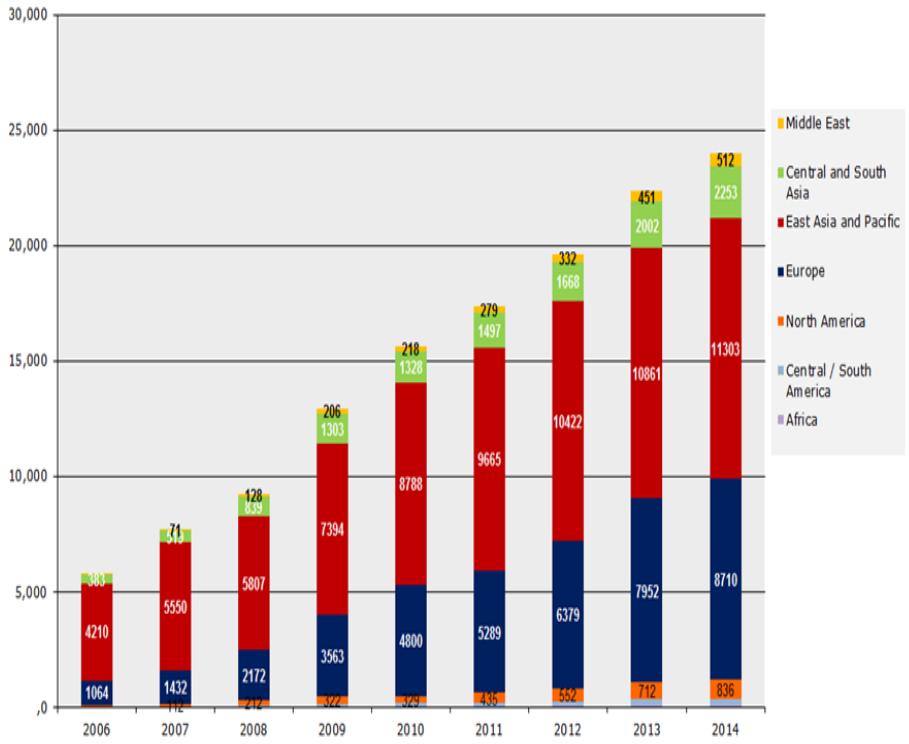


Figura 3.9 Cantidad de certificaciones 27001 por región [1].

En otros resultados se muestra la tendencia de adopción en la norma por región, el consolidado de la Tabla 10 permite notar que recién en el 2012 Latinoamérica consiguió llegar a 1%; de ahí el incremento de las organizaciones que se certifican es muy lento. De hecho llama la atención la contracción que se presenta Asia-Pacífico lo cual a la larga afecta la tendencia a nivel mundial; ver Figura 3.10.

Tabla 10 Porcentaje de adopción por región [1].

Año	2006	2007	2008	2009	2010	2011	2012	2013	2014
Total	100 %	100%	100%	100%	100%	100%	100%	100%	100%
Africa	0,1%	0,1%	0,2%	0,4%	0,3%	0,2%	0,3%	0,4%	0,3%
Central / South America	0,3%	0,5%	0,8%	0,8%	0,7%	0,9%	1,0%	1,2%	1,2%
North America	1,4%	1,4%	2,3%	2,5%	2,1%	2,5%	2,8%	3,2%	3,5%
Europe	18,4 %	18,5%	23,5%	27,5%	30,7%	31,1%	32,5%	35,6%	36,3%
East Asia and Pacific	72,6 %	71,8%	62,8%	57,2%	56,2%	55,2%	53,1%	48,6%	47,2%
Central and South Asia	6,6%	6,7%	9,1%	10,1%	8,5%	8,5%	8,5%	9,0%	9,4%
Middle East	0,6%	0,9%	1,4%	1,6%	1,4%	1,6%	1,7%	2,0%	2,1%

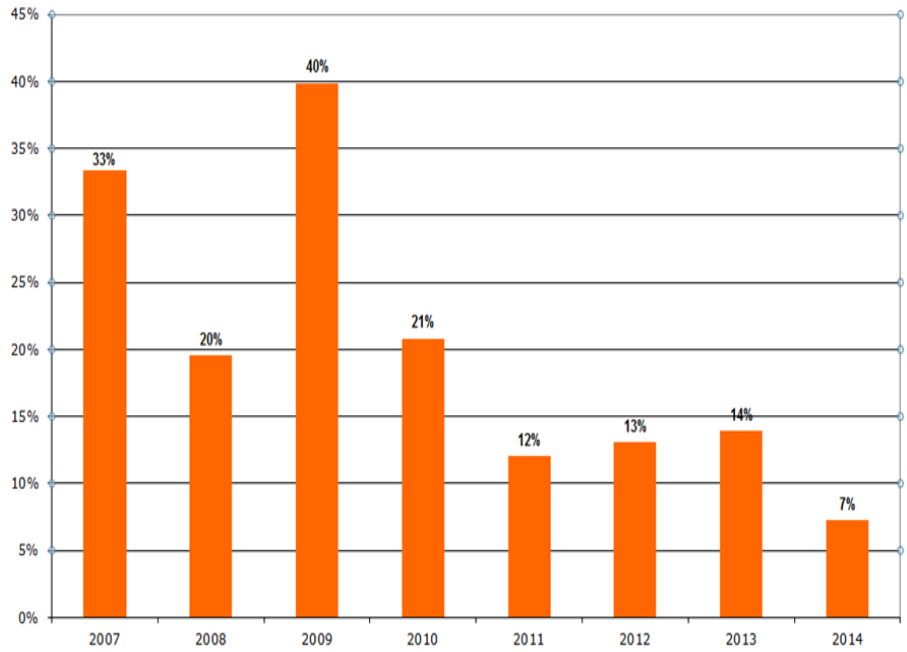


Figura 3.10 Cifras del Crecimiento y aceptación de la norma (anual) [1].

Las cifras dan evidencia de que las certificaciones en ISO 27001 no son tan demandadas como otras normas ISO (9001, 14001, 18001, etc.), situación que pudiera resultar paradójica considerando que la era digital le ha impuesto nuevos retos a las organizaciones incluyendo el aseguramiento de su información e infraestructura y que para nadie es un secreto que las amenazas avanzan de forma exponencial y que certificar el uso marcos estructurados para la gestión de la seguridad de la información puede ser un diferenciador en ventaja competitiva, cumplimiento, confianza y credibilidad y sobre todo disminución de costos imprevistos.

Se esperaría un repunte en estas cifras, pues pese a que existen otros marcos de buenas prácticas en la gestión de la seguridad de la información como COBIT 5 con su modelo BMIS e ITIL con su IT Security Management, solo por citar los más conocidos, el respaldo y la credibilidad de ISO deberían ser garantía suficiente para que las organizaciones se sientan más atraídas por implementar su estándar. En tanto deberá esperarse la próxima publicación de estadísticas oficiales de esta norma a nivel mundial y verificar las tendencias correspondientes en cada región y país.

3.4 Software para la gestión de ISO 27001

Los autores hicieron una investigación primero en la web y luego contactando los proveedores respectivos a fin de recabar información sobre el software disponible para facilitar los procesos de planificación, ejecución y mejora continua de un SGSI. Para la realización de una comparativa sencilla (ver Tabla 11 y Tabla 12) se consideraron las siguientes herramientas:

1. Isotools
2. GlobalSuite
3. Isolucion

4. ePulpo

Tabla 11 Funcionalidades de software de gestion comerciales.

	Funcionalidad
Isotools	Evaluación de Seguridad de la Información Controles 27002 Salvaguardas Métricas e Indicadores Cuadro de Mando Objetivos y Metas Gestor documental Recursos Humanos Capacitación Procesos
globalsuite	Análisis diferencial (GAP Analysis) Defición de Servicios y Procesos Inventario de Activos Análisis y Gestión de Riesgos Gestión de Controles Configuración de las dimensiones de seguridad Con guración de metodologías para el cálculo de los riesgos Con guración de metodologías para la madurez de controles Declaración de aplicabilidad Gestión de Incidencias de Seguridad Publicación de Encuestas de Activos y Riesgos Cuadro de Mando Planes de Formación y Auditorías Gestor Documental Gestor de Informes Gestión de Proyectos Integración con los sistemas de la organización Interconexión con otros sistemas y software ya existentes en la organización Históricos y trazabilidad en el tiempo **Usada por Deloitte*
Isolucion	Gestión de activos getsión de SOA Administración de GAP Matriz de requisitos legales Administración de incidentes Indicadores Gestión de riesgos Documentación y políticas

Epulpo	Gestión de usuarios Inventario de Activos Gestión de Activos Análisis y Gestión de Riesgos(Magerit) Análisis de Impacto y Continuidad de Operaciones(basada en otra herrmaineta llamada PILAR) Gestión de Planes de Acción Cuadro de Mandos Gestión Documental(gestor documental propietario Formación

Tabla 12 Comparación de software de gestion comerciales.

	Isotools	**globalsuite**	**isolucion**	**epulpo**
Procedencia	España	España	Colombia	España
Integración con otras norma ISO	SI	SI	SI	NO
tiempo en el mercado (años)	10	10	7	5
costo (USD)	No se pudo obtener un aproximado	No se pudo obtener un aproximado	Aprox. 13000 USD	Aprox. 25000 USD
modalidad Implementación	Saas	Saas. On Premise	Saas. On Premise	Saas. On Premise
Tecnología	JAVA	JAVA	.NET	PHP
países (presencia)	15	15	8	No especificado

En el siguiente capítulo se podrá verificar que la solución propuesta da cobertura a muchas de las funcionalidades ofertadas por las herramientas informáticas líderes usadas en el SGSI.

3.5 ASTINAVE EP: empresa en la cual se desarrolló el Sistema de información para la gestión del SGSI.

En esta parte ya es momento de conocer un poco sobre la organización en la cual se realizó el desarrollo del software propuesto, se trata de ASTINAVE EP en donde además trabajan los autores (la Ing. Mahecha como Responsable de Seguridad de la Información y el Ing. Coello como implementador de proyectos para la defensa como criptografía, simuladores de vuelo y sistemas de mando y control), de allí que la iniciativa de ambos a más de presentar una propuesta para la titulación de cuarto nivel era también ofrecer una solución concreta para su entorno laboral más cercano.

Pues bien, Astilleros Navales Ecuatorianos – ASTINAVE EP es una empresa de más de cuarenta años de trayectoria en el mercado naval ecuatoriano que ha sobrellevado transiciones sujetas a cambios de razón social y del fortalecimiento hacia el marco jurídico público, permitiendo consolidar su accionar en el apoyo a la defensa y la seguridad nacional, al desarrollo industrial marítimo, al desarrollo y producción de tecnología.

Desde sus inicios, ASTINAVE EP ha buscado el crecimiento permanente para constituirse como un astillero de mayores capacidades productivas lo cual, involucra no sólo mantenerse dentro

del ámbito de la reparación de embarcaciones sino también fortalecerse como astillero constructor e innovador de soluciones integrales con el conocimiento, y la experticia dentro de estos ámbitos adquirida en todos los años de historia. El 26 de marzo de 2012, mediante Decreto Ejecutivo N° 1116 y, posteriormente reformado con el Decreto Ejecutivo 1169 del mismo año, ASTINAVE es consolidada como empresa pública del Sector de la Defensa.

El objeto social de ASTINAVE EP, comprende:

1. Reparación, mantenimiento, transformación, diseño y construcción de las unidades navales para el sector de la Defensa Nacional y para la actividad naviera privada nacional y extranjera.

2. Reparación, mantenimiento, diseño y construcción de varaderos con patio de transferencia y de diques para embarcaciones de la defensa y del sector privado.

3. Implementación de tecnologías existente o de punta; así se fomenta progresos en la creación de diseños, relacionados con la construcción naval y comercial.

4. Confección, mantenimiento y reparación de estructuras, silos, tanques, hélices, bocines, tuberías de acero y aluminio y procesos especiales metalúrgicos.

5. Mantenimiento y reparación de motores, bombas, válvulas y sistemas hidráulicos.

6. Construcción de plantas de tratamiento de agua y provisión de servicios para la actividad de transporte por agua e industria naviera.

7. Producción, comercialización, reparación y mantenimiento de sistemas electrónicos, informáticos y de inteligencia de aplicación naval, militar, aérea y civil, originados por Centros de Investigación y Desarrollo o propios.

8. Trabajos y prestación de servicios para la Industria metalúrgica en general del sector público y privado previstos en este artículo y otros nuevas que incursione, acorde a su capacidad operativa, técnica y económica.

3.5.1 Misión y Visión

Misión

Desarrollar, Producir y Mantener Soluciones para potenciar la Defensa, la Seguridad, y el Sector Industrial Marítimo.

Visión

Hasta el año 2017 ser la empresa líder en el país en apoyo a la Defensa, Seguridad y Desarrollo Industrial Marítimo.

3.5.2 Entorno organizacional

ASTINAVE EP orientada al enfoque a procesos empresariales ha formulado y establecido su estructura organizacional como se muestra en la Figura 3.11.

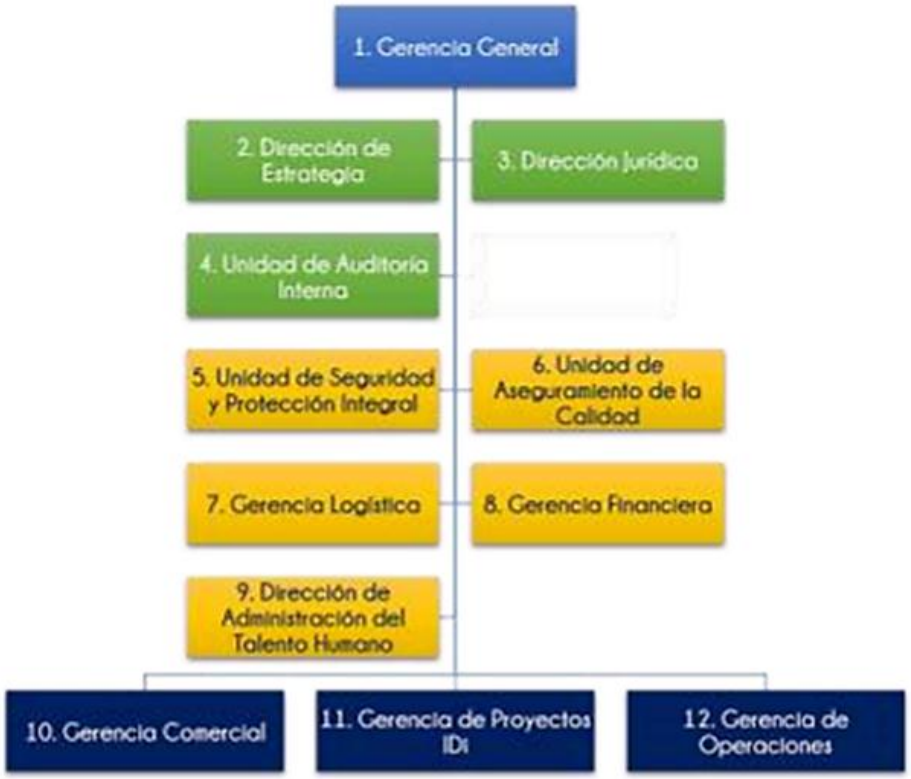


Figura 3.11 estructura organizacional de ASTINAVE EP.

De la Figura anterior se diferencian claramente 4 grupos de procesos:

1. Azul Claro: Procesos Gobernantes.- es la figura de la Gerencia General.

2. Azul Oscuro: Procesos de cadena de valor.- donde se producen los bienes y servicios ofertados por ASTINAVE EP.

3. Verde: Procesos habilitantes de asesoría.- brindan asesoría a los procesos anteriores con bases legales y técnicas.

4. Amarillo: Procesos habilitantes de apoyo.- brindan apoyo a los procesos productivos de la empresa.

Las líneas de negocio descritas en la Figura 3.12 mantienen la conceptualización de brindar soluciones integrales complementando así la operatividad de las actividades dentro de la empresa para el cliente. Esto demuestra, adicionalmente, la madurez que ha sido alcanzada en el pasar de los años fortaleciendo a ASTINAVE EP, y pasar de ser una empresa únicamente prestadora de servicios de mantenimientos de embarcaciones, a ser una empresa que brinda soluciones integrales en los ámbitos de embarcaciones, electrónica y costa afuera (off-shore).

Figura 3.12 Líneas de Negocio de ASTINAVE EP.

3.5.3 Procesos empresariales

Basada en la responsabilidad con la ciudadanía, los procesos de la organización han sido estructurados de modo que permitan una flexibilidad y adaptabilidad ante exigencias de los clientes, aplicabilidad de normativas gubernamentales y oportunidades de alcanzar una excelencia operativa, esto permite, establecer una estructura organizacional adecuada para el desarrollo de las actividades, tal como lo muestra la Figura 3.13.

Figura 3.13 Modelo de Gestión de ASTINAVE EP.

En ASTINAVE EP se ha procurado que la infraestructura productiva al igual que, aquella destinada a la administración de la empresa, esté acorde a las políticas de seguridad, salud ocupacional y medio ambiente, de modo que, los flujos de trabajo, se puedan realizar del mejor modo, mediante la optimización de los recursos y posibilitando que el capital humano se desempeñe y se desarrolle paralelamente.

En ASTINAVE EP la base del modelo de gestión fue fortalecido con temas inherentes al ámbito de la seguridad de la información haciendo inclusión de directrices, procedimientos e instructivos de trabajo que permiten gestionar apropiadamente

la información bajo estándares internacionales con todas las partes interesadas.

La propuesta de valor de ASTINAVE EP radica en ofrecer a sus clientes soluciones integrales en cada una de sus líneas de negocio, propuesta que está soportada en la filosofía de Gestión del Ciclo de Vida de los Productos. Bajo esta conceptualización, también formuló sus procesos internos posibilitando que los flujos de trabajo condujeran a la creación de los productos y servicios de acuerdo a las necesidades del cliente. La Figura 3.14 define el mapa de procesos correspondiente.

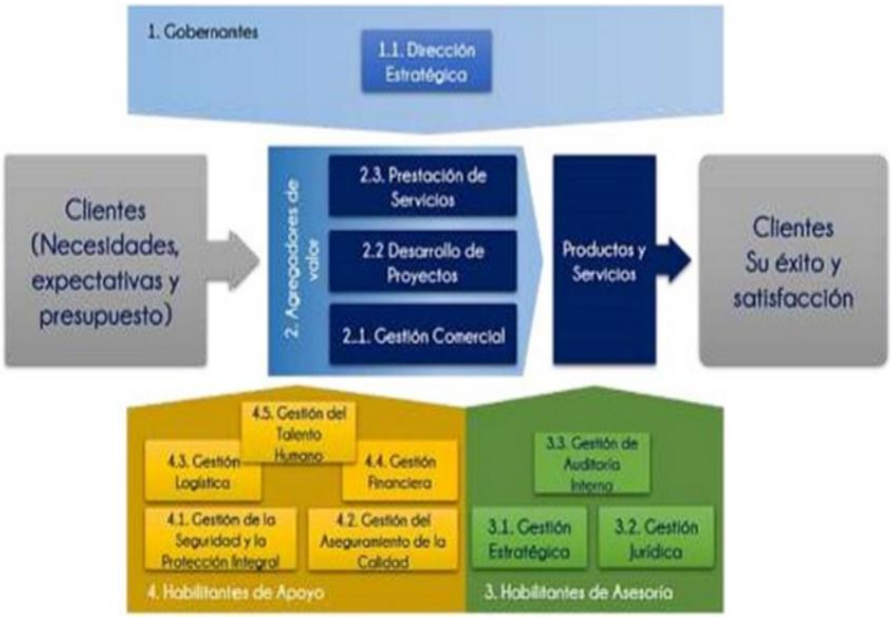


Figura 3.14 Mapa de Procesos de ASTINAVE EP.

3.5.4 Sistema integrado de Gestión

ASTINAVE EP con el firme compromiso de la mejora continua en cada uno de sus procesos ha implementado un Sistema Integrado de Gestión (SIG), que involucra la Gestión de Calidad, Gestión de Seguridad y Salud ocupacional; y Gestión Medio Ambiental.

Durante el primer trimestre del 2015 se dio inicio el proceso de Auditoría Externa de sistemas integrados de gestión. En cumplimiento con el proceso formal de Certificación del Sistema de Gestión, el Organismo de Certificación – SGS Ecuador, emitió la recomendación de certificación y registro de dicho sistema para ASTINAVE EP, conforme a los requisitos de la norma ISO 14001:2004- Environmental Management System Certification, ISO 9001:2008 – Quality Management System Certification, OHSAS 18001:2007 Occupational Health and Safety Management System Certification. Con esta certificación se lograron los siguientes avances:

1. Equipos de alta tecnología: seguridad y medio ambiente.

2. Personal capacitado en manejo de maquinarias y equipos de alto riesgo.

3. Personal comprometido con la estrategia empresarial.

4. Infraestructura y su operación adecuada para la operatividad y servicios.

5. Implementación de un sistema de gestión documental.

6. Organización orientada a procesos y optimización de recursos.

Además el SIG tiene los siguientes objetivos fundamentales:

1. Identificar, manejar y reducir los efectos de producto no conforme, reducir los efectos ambientales y los peligros de actividades de los trabajadores.

2. Obtener un mejor resultado empresarial gestionando las tres disciplinas de forma integrada, es decir, integrando los sistemas que las gestionan, los procesos que los soportan y las actividades que componen los procesos.

3. Capacitar al personal y asegurar su participación para la mejora continua del desempeño de la calidad, fomentar la seguridad y cuidar el medioambiente entre otras.

4. Realizar las actividades de forma consistente de acuerdo a las políticas establecidas por la empresa y su plan estratégico.

En base al trabajo realizado para alcanzar la certificación con el SIG, el siguiente objetivo de la organización es asegurar el buen uso de la información institucional y de las partes interesadas a través de los procedimientos organizacionales y de tecnologías de información y comunicación, comprometiéndose a:

1. Controlar, prevenir y/o mitigar los riesgos de seguridad de la información, en orden a asegurar la continuidad del negocio.

2. Incrementar la integración de la información de los diferentes procesos y servicios de la organización.

3. Incrementar la capacidad, el desarrollo y buen uso de las tecnologías de información y comunicación.

La implementación del SGSI en ASTINAVE EP arrancó en Febrero del 2016, la toma de requerimientos, análisis, diseño y desarrollo del software empezó en Noviembre del 2015, la puesta en producción ocurrió en Junio del 2016 y desde entonces ha venido haciéndose uso de él con bastante expectativa.

Los autores se sienten satisfechos de haber contribuido a que la organización para la cual trabajan siga dando pasos para ser de las pocas empresas en Ecuador con un Sistema de Gestión

Integrado con certificación en cuatro áreas: Calidad (ISO 9001), Ambiental (ISO 140001), Seguridad y Salud Ocupacional (OHSAS 18001) y Seguridad de Información (ISO 27001).

CAPÍTULO 4

ANÁLISIS Y DISEÑO

En este capítulo se tomaron los requerimientos que se desprendieron de los capítulos previos y se inició el análisis y diseño de la solución propuesta. Sobre todo se hizo un especial énfasis en que aunque la solución iba a ser desarrollada e implementada en ASTINAVE EP el software debería tener un enfoque lo más genérico posible de forma tal que la misma solución pudiera adaptarse en otra organización sin mayor complicación.

4.1 Herramientas seleccionadas para el modelamiento y desarrollo del Software.

La solución propuesta es una aplicación web que estará ejecutándose en un entorno de virtualización de Windows, en la Tabla 13 y Tabla 14

se encuentra el resumen de las herramientas usadas para la realización de modelos y codificación:

Tabla 13 Herramientas usadas para modelamiento y desarrollo.

	Selección	Descripción
DBMS	SQL SERVER 2014	Un Sistema de administración de bases de datos es una Interfaz que define un lenguaje para definición y manipulación de la base de datos. Acciones primordiales: 1.-**Definir la base de datos:** especificar tipos, estructuras y restricciones de datos. 2.-**Construir la base de datos:** guardar los datos en algún medio controlado por el mismo SGBD. 3.-**Manipular la base de datos:** realizar consultas, actualizarla, generar informes.
S.O	Windows 2012 + (IIS 7+)	Sistema Operativo que se ejecuta sobre el servidor web que publica la solución, en este caso, en la intranet de la organización
Lenguaje	ASP.NET, C#	"ASP.NET es un modelo de desarrollo Web unificado que incluye los servicios necesarios para crear aplicaciones Web empresariales con el código mínimo. ASP.NET forma parte de .NET Framework y al codificar las aplicaciones ASP.NET tiene acceso a las clases en .NET Framework." [14].
IDE	Visual Studio 2012	Un IDE (Integrated Development Environment) es una herramienta que ayuda al desarrollador para maximizar su productividad proporcionándole componentes muy unidos con interfaces de usuario similares. Generalmente, este programa suele ofrecer muchas características para la creación, modificación, compilación, implementación y depuración de software.

Cliente	HTML5, CSS3, Bootstrap (Responsive Design)	Bootstrap es un framework front end para crear páginas web que incluye una serie de recursos que simplifican el desarrollo de un proyecto web con html5, css3 y Jquery, de manera que simplifica mucho el trabajo a la hora de diseñar. Es adaptable a cualquier dispositivo.

Tabla 14 Otras Herramientas necesarias.

	Selección	Descripción
Framework	.NET 4.5	Un framework es un componente de software que puede ser añadido al sistema operativo Windows. Provee un extenso conjunto de soluciones predefinidas para necesidades generales de la programación de aplicaciones, y administra la ejecución de los programas escritos específicamente con la plataforma. En el caso del Framework .NET ya existen iniciativas para ejecutarlas también sobre plataformas Linux.
ORM	Entity Framework 5.0	Un ORM (Object Relational Mapping), es una técnica de programación para convertir datos entre el lenguaje de programación orientado a objetos utilizado y el sistema de base de datos relacional utilizado en el desarrollo de una aplicación. En este caso la herramienta usada está sustentada en el propio framework
Reportes	SSRS	El componente para presentar reportes empresariales, para este caso Sql Server Reporting Services, ofrece una gama completa de herramientas y servicios listos para usar que ayudan a crear, implementar y administrar informes para la organización.
Otros Controles	Telerik Q4 (UI ASP.NET AJAX)	Suite de controles de servidor para ASP.NET

4.2 Esquema de desarrollo.

El esquema de desarrollo elegido fue iterativo e incremental, es decir, la solución se planificó en diversas iteraciones que por lo general no superaban las 2 semanas. En cada iteración se proporcionaba un resultado completo de acuerdo a lo planificado sobre el proyecto total, de esta manera no se dejó para el final ninguna actividad relacionada con la entrega de requerimientos funcionales.

En cada iteración la solución propuesta fue evolucionando a partir de los resultados completados en las iteraciones anteriores y con los nuevos requerimientos.

Este esquema permitía además mejorar los requerimientos ya completados y priorizar el desarrollo funcional remanente. La Figura 4.1 se explica cómo funciona este esquema.

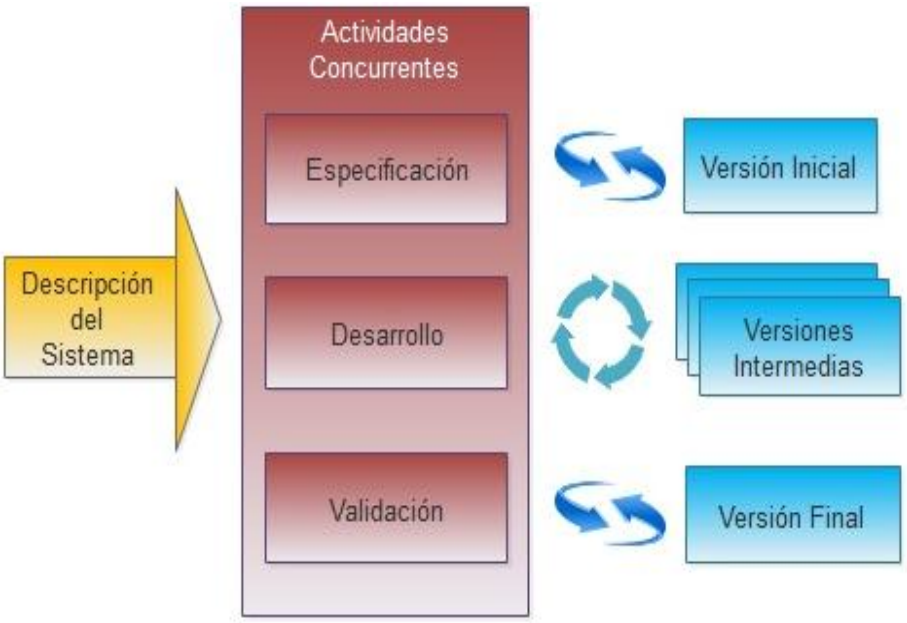


Figura 4.1 Esquema de desarrollo incremental.

4.3 Arquitectura de la solución.

Siendo ya una reconocida buena práctica en las fábricas de software, la arquitectura implementada es de tipo N-TIER, diferenciando las capas presentadas en la Figura 4.2 y listadas a continuación:

Figura 4.2 Arquitectura en capas

Acceso a datos

Conocida como Data Access Layer, esta capa es la encargada de la comunicación con la base de datos, en ella se programan todas las acciones y/o procedimientos CRUD (Create, Read, Update y Delete), es la única que conoce qué motor de base de datos se está empleando pero no conoce al Front End, es decir, que puede ser reusada para una interfaz web o de escritorio. Implícitamente contiene a lo que se denomina como Capa de Entidades, o sea, contiene todos aquellos objetos que representan la lógica del negocio, además recibe peticiones exclusivas de la capa de negocio.

Para mayor agilidad en la programación de esta capa se está usando el ORM Entity Framework; es una técnica de programación que mapea una base de datos relacional a una serie de objetos que pueden ser manipulados desde los lenguajes de programación orientados a objetos utilizados tradicionalmente hoy en día para el desarrollo. Lo que se persigue con los ORM es facilitar y automatizar el proceso de desarrollo manual. En la Figura 4.3 se puede ver el esquema básico de funcionamiento del mencionado ORM.

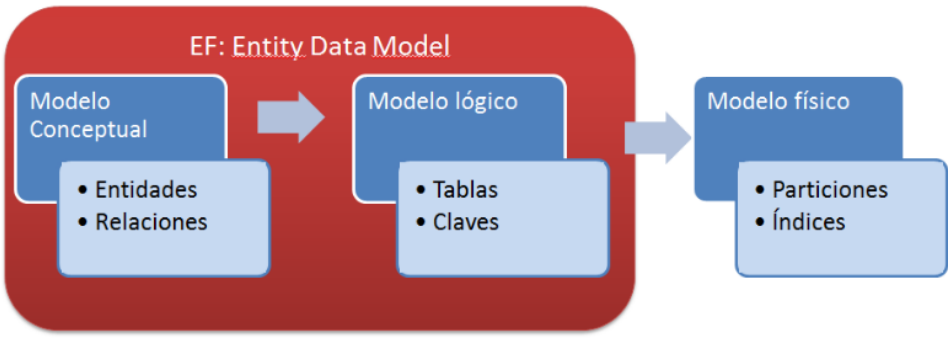


Figura 4.3 DAL usando como ORM a Entity Framework.

Negocio

Conocida como Capa de reglas de negocio, esta capa se encarga de implementar, la lógica del negocio, es decir, todo lo que el software debe de considerar antes de realizar una acción o el proceso que debe de seguir después de realizar una acción. Esto incluye validaciones, restricciones y demás acciones que deban programarse para cumplir con los requerimientos. Esta capa recibe de la Capa de Presentación las solicitudes, valida que las condiciones que establece el negocio se

cumplan antes de realizar dicha acción o de hacer la respectiva solicitud a la Capa de Acceso a Datos.

Presentación

Esta Capa es la encargada de interactuar con el usuario, es decir, es el conjunto de controles, ventanas, mensajes, cuadros de diálogos, páginas web o interfaces gráficas a través de las cuales el usuario realiza acciones en el software, comunicándose así con la aplicación, esta comunicación consiste en proporcionar parámetros de entrada y recibir datos como respuesta. Esta capa se comunica con la capa de Lógica de Negocio y también hace uso de las clases de la capa de Entidades.

La arquitectura de N-capas está caracterizada por la descomposición funcional de la aplicación, los componentes de servicio y su instalación distribuída. Mejorando la escalabilidad, disponibilidad, administración, y utilización de recursos. Cada capa es completamente independiente de las otras capas, excepto aquella que esta inmediatamente debajo de ella. La capa n solo necesita saber cómo manejar una solicitud de la capa n+1, como hacer la solicitud a la capa n-1 (si existe) y cómo manejar el resultado de la petición.

Dado que se está usando el Framework Net de Microsoft es bueno recomendar en este punto a la “Guía de Arquitectura N-Capas

Orientada al Dominio con NET 4.0”, a la que Microsoft Ibérica cataloga como patrón y modelo base (arquitectura marco) que puede ser personalizado por cada organización en función de necesidades concretas. De dicho documento se tiene el resumen de la Figura 4.4.

Estilo Arquitectural	**En Capas (*N-Layer*)**
Descripción	El estilo arquitectural en capas se basa en una distribución jerárquica de los roles y las responsabilidades para proporcionar una división efectiva de los problemas a resolver. Los roles indican el tipo y la forma de la interacción con otras capas y las responsabilidades la funcionalidad que implementan. 
Características	• Descomposición de los servicios de forma que la mayoría de interacciones ocurre solo entre capas vecinas. • Las capas de una aplicación pueden residir en la misma máquina o pueden estar distribuidos entre varios equipos. • Los componentes de cada capa se comunican con los componentes de otras capas a través de interfaces bien conocidos. • Cada nivel agrega las responsabilidades y abstracciones del nivel inferior.

Figura 4.4 Descripción y Característica de la Arquitectura N-Capas.

Entre las ventajas de esta arquitectura, se destacan:

1. Codificación concurrente

2. Aplicaciones más robustas debido al encapsulamiento

3. Mantenimiento y soporte más sencillo

4. Mayor flexibilidad

5. Alta escalabilidad. (Las capas de acceso a datos y de negocio pueden ser reusadas en una capa de presentación diferente)

El aplicativo web para gestionar el SGSI, fue agregado a un conjunto de funcionalidades desplegadas dentro de la intranet de ASTINAVE EP, la organización en base al esquema de la arquitectura de la solución en el IDE luce como se puede apreciar en las siguientes figuras:

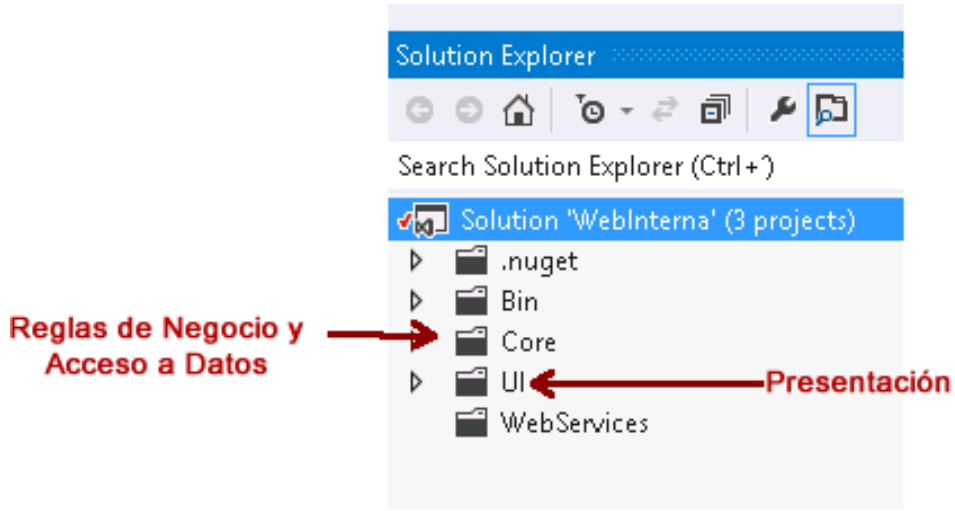


Figura 4.5 Vista de las n-capas desde la solución en Visual Studio 2012.

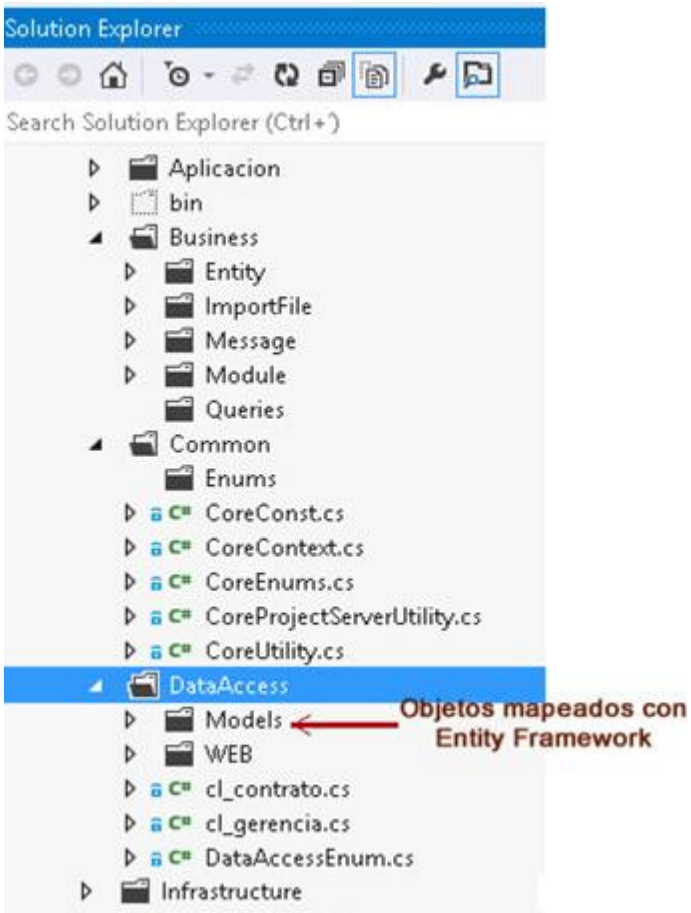


Figura 4.6 Detalles del Projecto Core en donde están los objetos, el acceso a datos, las reglas de negocio.

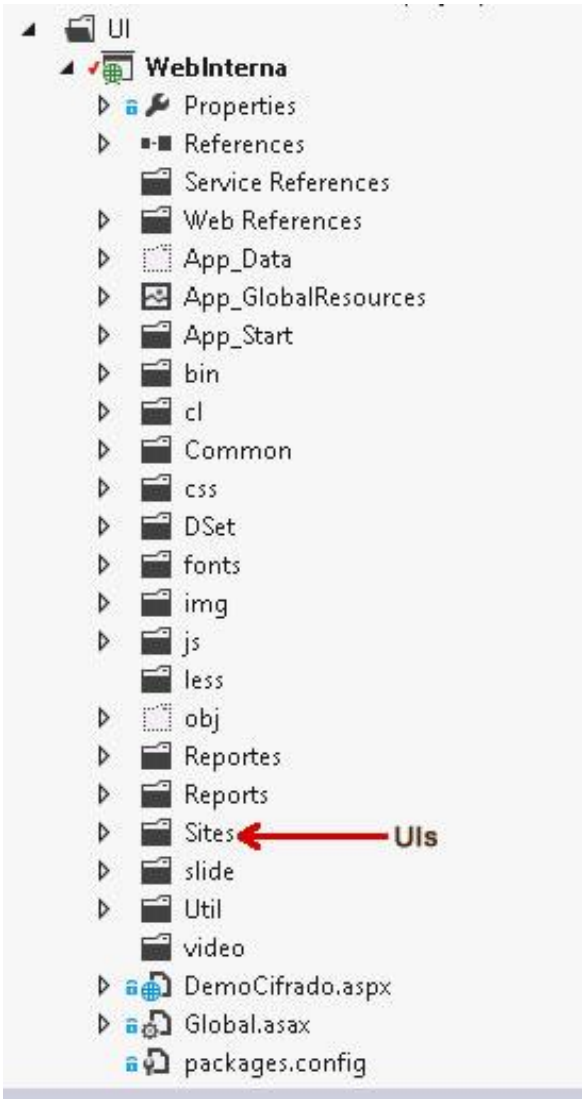


Figura 4.7 Detalle del Proyecto UI en donde se programan los artefacto de GUI.

4.4 Diseño de la solución.

En función de los requerimientos funcionales obtenidos a partir de lo establecido en la norma ISO 27001, así como de las consideraciones particulares de la organización para la cual se realizó la propuesta de

implementación del sistema, la solución inicialmente queda compuesta por los siguientes módulos funcionales, presentados en la Tabla 15:

Tabla 15 Resumen de módulo funcionales de la solución propuesta

Gestión de controles de la norma	1. Registro y mantenimiento de requisitos del anexo A. 2. Registro y mantenimiento de requisitos del anexo SL (Clausulas). 3. Asociación de documentos cuyo control de cambios es gestionado por Sharepoint. 4. Asignación de responsables de seguimiento por control. 5. Generación de declaración de aplicabilidad.
Gestión de activos de información	1. Registro y mantenimiento de procesos organizacionales. 2. Registro y Mantenimiento de clasificador único de activos. 3. Registro y mantenimiento de activos de información. 4. Tasación (valoración del impacto) de los activos de información. 5. Registro de encuestas para la valoración de los activos. 6. Votación para la valoración de los activos de información.
Gestión de riesgos	1. Registro y mantenimiento de amenazas a los activos de información. 2. Registro y mantenimiento de Vulnerabilidades de los activos de Información. 3. Asociación de par amenaza-vulnerabilidad (ISO 27005). 4. Definición de la probabilidad de las causas de riesgos para los activos de información. 5. Valoración del riesgo para los activos de información. 6. Registro y mantenimiento del tratamiento de riesgos. 7. Registro y mantenimiento de acciones de planes por riego. 8. Evolución del riesgo (inherente vs residual).

La interrelación de estos módulos funcionales con otros sistemas y subsistemas de la organización se puede apreciar en el diagrama mostrado en la Figura 4.8.

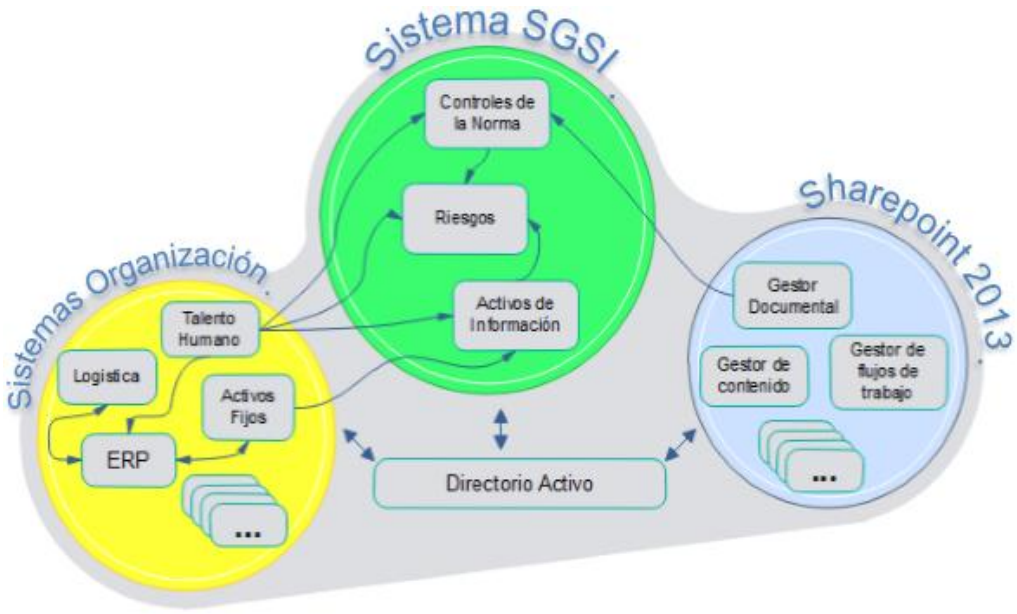


Figura 4.8 Diagrama de sistemas y subsistemas

En concordancia con el esquema modular establecido y la funcionalidad resumida en la Tabla 15, se verán más en detalle algunas consideraciones funcionales por cada módulo a continuación.

4.4.1 Gestión de los controles de la norma

Este módulo permitirá a los usuarios gestionar todo lo relativo con la norma y sus requisitos, es decir, que si la norma evoluciona hacia una siguiente versión, será en este módulo en donde se registrará la nueva norma, su versión y el año correspondiente, de la misma forma se procederá con el registro y mantenimiento de los nuevos controles definidos en esa norma.

Sin duda que su funcionalidad más importante es la generación de la declaración de aplicabilidad, ésta permitirá a los responsables del SGSI definir la aplicabilidad de los controles del Anexo A en la organización en función de los procesos cuyo alcance se quiera establecer. Este documento es el primer documento mandatorio de la norma ISO 27001.

El sistema permitirá, como evidencia de cumplimiento, asociar a cada control del Anexo A uno o varios documentos a través de los cuales la organización define directrices, procedimientos, manuales, instructivos, planes, etc. para articular y dar marco común a las iniciativas en seguridad de la información. En el caso particular de la empresa en la cual se realizó la propuesta de desarrollo, muchos de esos documentos apuntalan el sistema integrado de gestión. Para el desarrollo de la búsqueda de esos documentos es necesario programar pensando en la integración con el Sharepoint 2013 que en este caso es el gestor documental a través del cual se almacenan los documentos, se gestionan permisos, accesos y control de versión de los mismos.

Asimismo se permitirá que los miembros del equipo metodológico que se conforme para la administración del SGSI

puedan ser asignados para dar seguimiento al cumplimiento de controles, una gestión de auditoria interna si se quiere, para esta asignación también se deberá programar una búsqueda integrada con las bases de la Dirección de Talento Humano para mostrar aquellos colaboradores en estado activo.

4.4.2 Gestión de activos de información

En este módulo se tendrá la gestión completa de los activos de información, en el requerimiento funcional de la norma se establece la necesidad de que los activos asociados a la información y a los recursos para el tratamiento de la información deben estar claramente identificados y debe elaborarse y mantenerse un inventario. Para ello la solución propuesta define un esquema de clasificación único que incluso podrá ser cambiado, más detalle en la Tabla 16.

Tabla 16 Clasificación Única para los activos de Información.

cód.	Clasificación
1	**Información y Registros**
1.1	Físicos
1.2	Digitales
2	**Hardware**
2.1	Equipos Informáticos
2.2	Equipos de Telecomunicaciones
2.3	Dispositivos de Almacenamiento
2.4	Infraestructura Tecnológica
2.5	seguridad informática
3	**Software**
3.1	Propietario
3.2	De ASTINAVE EP
3.3	Licencias
4	**Activo Fijo**
4.2	Edificios
4.3	Activo Fijo
4.4	Bienes de Control
4.5	Vehículo
5	**Reputación e Imagen Corporativa**
5.1	Imagen
5.2	Patentes
5.3	Propiedad Intelectual
5.4	Derechos de Autoría
5.5	Méritos

De la misma manera el sistema permite administrar los procesos organizacionales, para el caso de ASTINAVE EP, se

tendrá la siguiente estructura administrable mostrada en la Tabla 17.

Tabla 17 Definición Procesos a los cuales se asociarán los activos de información.

cód.	Proceso
1	**GOBERNANTE**
1.1	DIRECCION DE ESTRATEGIA
2	**AGREGADOR DE VALOR**
2.1	GESTION COMERCIAL
2.1.1	MARKETING
2.1.2	VENTAS
2.2	DESARROLLO DE PROYECTOS
2.2.1	DESARROLLO DEL CONCEPTO DE SOLUCION
2.2.2	PREPARACION DE LA PROPUESTA DE SOLUCION
2.2.3	DESARROLLO DEL PROYECTO
2.2.4	EVALUACION Y CONTROL DEL PROYECTO
2.2.5	CIERRE DEL PROYECTO
2.3	PRESTACION DE SERVICIOS
2.3.1	EJECUCION CARENAMIENTO
2.3.2	MONITOREO-CONTROL-CIERRE
3	**HABILITANTE DE ASESORIA**
3.1	GESTION ESTRATEGICA
3.1.1	FORMULACION DE LA ESTRATEGIA
3.1.2	IMPLEMENTACIÓN ESTRATÉGICA
3.1.3	MEJORA DE LA GESTION INTEGRAL
3.1.4	ADMINISTRACIÓN DE PROYECTOS ORGANIZACIONALES
3.1.5	ADMINISTRACIÓN DEL CONOCIMIENTO
3.1.6	ADMINISTRACIÓN DE LA INFORMACIÓN
3.1.7	ADMINISTRACION TECNOLÓGICA
3.2	GESTION JURIDICA
3.2.1	ALINEAMIENTO LEGAL
3.2.2	PATROCINIO
3.2.3	ASESORÍA JURÍDICA
3.2.4	ADMINISTRACIÓN DE SEGUROS
4	**HABILITANTE DE APOYO**
4.1	GESTION DE LA SEGURIDAD Y LA PROTECCION INTEGRAL
4.1.1	ADMINISTRACION DE LA SEGURIDAD INDUSTRIAL
4.1.2	ADMINISTRACION DE LA SALUD OCUPACIONAL
4.1.3	GESTION AMBIENTAL
4.2	GESTIÓN DEL ASEGURAMIENTO DE LA CALIDAD
4.2.1	INSPECCIÓN EN LA RECEPCIÓN
4.2.2	EJECUCIÓN DE ENSAYOS

4.2.3	INSPECCIÓN Y PRUEBAS EN LA EJECUCIÓN
4.3	GESTION LOGISTICA
4.3.1	ADQUISICIÓN DE BIENES Y SERVICIOS U OBRAS
4.3.2	ADMINISTRACIÓN DEL TRANSPORTE
4.3.3	ADMINISTRACIÓN DE LOS SERVICIOS INSTITUCIONALES
4.3.4	ADMINISTRACIÓN DEL MANTENIMIENTO
4.4	GESTION FINANCIERA
4.4.1	ADMINISTRACIÓN PRESUPUESTARIA
4.4.2	ADMINISTRACIÓN CONTABLE
4.4.3	ADMINISTRACIÓN Y CONTROL DE ACTIVOS FIJOS
4.4.4	ANÁLISIS DE COSTOS
4.4.5	ADMINISTRACIÓN RECURSOS MONETARIOS
4.5	GESTION DEL TALENTO HUMANO
4.5.1	VINCULACIÓN DEL TALENTO HUMANO
4.5.2	EVALUACIÓN DEL DESEMPEÑO
4.5.3	ADMINISTRACIÓN DEL DESARROLLO PROFESIONAL
4.5.4	ADMINISTRACIÓN DEL SISTEMA REMUNERATIVO
4.5.5	DESVINCULACIÓN DEL TALENTO HUMANO

Una vez que se tiene un activo de la información controlado en el Catálogo Único, se garantiza que el mismo ya está pertinentemente clasificado, con propietario definido, asociado a uno o más procesos de la organización, lo siguiente es definir la valoración del impacto de esos activos de información.

Al proceso de valoración del Impacto de los Activos de Información de lo denomina Tasación, la metodología para definir tal tasación será la indicada por la Norma 27005, la misma que en su Anexo B brinda más detalles al respecto: “El paso siguiente a la identificación de los activos es pactar la escala que se va a utilizar y los criterios para la asignación de una ubicación particular en esa escala para cada uno de los

activos, con base en la valoración. Debido a la diversidad de activos que se encuentran en la mayoría de los organizaciones, es probable que algunos activos que tengan un valor monetario conocido sean valorados en la moneda local en donde están presentes, mientras otros que tiene un valor más cualitativo se les puede asignar un rango de valores, por ejemplo, desde 'muy bajo' hasta 'muy alto'. La decisión de utilizar una escala cuantitativa en lugar de una cualitativa es realmente un asunto de preferencia organizacional, pero debería ser pertinente para los activos que se están valorando.

Se recomienda reducir todas las valoraciones de los activos hasta una base común. Esto se puede hacer con la ayuda de criterios que se pueden utilizar para evaluar las consecuencias posibles resultantes de la pérdida de confidencialidad, integridad, disponibilidad, no repudio, responsabilidad, autenticidad o confiabilidad de los activos son:

1. Incumplimiento de la legislación y/o reglamentación.

2. Deterioro en el desempeño del negocio.

3. Pérdida del buen nombre/efecto negativo en la reputación.

4. Brechas asociadas con la información personal.

5. Efectos adversos en el cumplimiento de la ley.

6. Brechas en la confidencialidad.

7. Brechas de orden público.

8. Pérdida financiera.

9. Alteración de las actividades del negocio.

10. Hacer peligrar la seguridad ambiental.

En lo que respecta a la evaluación del impacto, para la 27005, un incidente en la seguridad de la información puede tener impacto en más de uno de los activos o únicamente en una parte de uno de los activos. El impacto se relaciona con el grado de éxito del incidente. En consecuencia, existe una diferencia importante entre el valor del activo y el impacto resultante de un incidente. Se considera que el impacto tiene un efecto inmediato (operacional) o un efecto futuro (en el negocio) que incluye consecuencias financieras y de mercado.

El sistema propondrá una valoración del impacto en función de la Confidencialidad, Disponibilidad e Integridad permitiendo además que la valoración la realicen los responsables de los activos y los dueños de los procesos guiados por un grupo

metodológico del SGSI. La escala predefinida en el sistema será la mostrada en la Tabla 18.

Tabla 18 Escala para la valoración del Impacto en los activos de información.

ESCALA DE IMPACTO					
Nivel	**Valor**	**Imagen**	**Operativo**	**Financiero**	**Legal**
Muy Bajo	**1**	Impacta negativamente la imagen de un rol	Impacta de forma leve la operación de un rol	Sin impacto financiero en organización o sus procesos	Impacta negativamente la posibilidad de recibir multas
Bajo	**2**	Impacta negativamente la imagen del proceso	Impacta importante la operación del proceso	Se pueden presentar sobrecostos (reprocesos) a nivel de proceso	Impacta negativamente la posibilidad recibir demandas
Medio	**3**	Impacta negativamente la imagen no sólo del proceso evaluado sino de otros procesos	Impacta negativamente no sólo la operación del proceso evaluado sino a otros procesos	Se pueden presentar sobrecostos (reprocesos) no sólo en el proceso evaluado sino a otros procesos	Impacta negativamente la posibilidad de recibir una investigación disciplinaria
Alto	**4**	Impacta negativamente la imagen de la organización	Impacta negativamente la operación de la UPTC ó sus objetivos	Se pueden presentar sobrecostos (reprocesos) significativos para la organización	Impacta negativamente la posibilidad de recibir una investigación fiscal
Muy Alto	**5**	Impacta negativamente la imagen de la organización	Impacta negativamente no solo la operación de la organización si no otras entidades conexas	Se pueden presentar sobrecostos (reprocesos) significativos para la organización	Impacta negativamente la posibilidad de recibir una intervención o sanción

La integración de este módulo funcional con otros sistemas y subsistemas ya existentes en la organización se rige al esquema expuesto en la Figura 4.8.

4.4.3 Gestión de Riesgos

La gestión de riesgos para los activos de información también se diseñó en función de las recomendaciones de la ISO 27005 y las especificaciones dadas en su correspondiente Anexo E. Para ello el sistema permitirá a los implementadores del SGSI registrar y mantener catálogos de Amenazas (Anexo C) y de Vulnerabilidades (Anexo D) para luego poder asociarlas y generar pares amenaza-vulnerabilidad. Sabiendo que una amenaza es una situación potencial que puede desencadenar un incidente en la seguridad de la información y que una vulnerabilidad es el punto débil de un activo que puede ser explotado por una amenaza, gestionar los pares amenaza-vulnerabilidad permitirá gestionar las causas de riesgos para los activos de información.

Para la definición del riesgo como **Riesgo = Impacto x Probabilidad (4.2)** se usará lo diseñado en las tasación de los activos (que será el Impacto) y se complementará con el cálculo promediado de las probabilidades de ocurrencia de un conjunto de pares amenaza-vulnerabilidad que a la larga definirán la causa del riesgo tal como se muestra en la Tabla 19.

Tabla 19 Ejemplo de cálculo probabilidad de ocurrencia de un conjunto de pares amenazas-vulnerabilidad.

Amenaza	Vulnerabilidad	Probabilidad
MAL FUNCIONAMIENTO DEL EQUIPO	MANTENIMIENTO INSUFICIENTE	2
	FALTA DE PRUEBA DEL ENVÍO O LA RECEPCIÓN DE MENSAJES	1
SATURACIÓN DEL SISTEMA DE INFORMACION	GESTIÓN INADECUADA DE LA RED (CAPACIDAD DE RECUPERACIÓN DEL ENRUTAMIENTO)	2
INCUMPLIMIENTO EN EL MANTENIMIENTO DEL SISTEMA DE INFORMACION	FALTA DE PROCEDIMIENTO DE CONTROL DE CAMBIOS	3
	Probabilidad Promedio	***2***

Una vez que ambos componentes (Impacto y probabilidad) se definan en el sistema, la valoración de cada riesgo también deberá poder ubicarse en una escala que guiará al usuario sobre la respuesta a darse a ese riesgo tal como se muestra en la Figura 4.9. La escala se definió en función del apetito de riesgo señalado por el Comité de Seguridad de Información de la organización.

Figura 4.9 Escala de Riesgos.

Para una gestión de riesgos basada en la metodología indicada en la ISO 27005 se debe dar cobertura a los procesos de evaluación, tratamiento y seguimiento de riesgos, en la Tabla 20 se resumen las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGSI, es decir, que la solución propuesta también deberá ofrecer al usuario un mecanismo para asociar planes de acción a cada riesgo y poder dar seguimiento a la realización de esas acciones. Estos planes de acción, dicho sea de paso, definirán una respuesta al riesgo en concordancia con lo definido en la norma: aceptar, mitigar, evitar, transferir y se permitirá relacionar la acción propuesta con uno o más controles del Anexo A.

Tabla 20 Alineamiento del SGSI y el proceso de Gestión del Riesgo en la Seguridad de la Información.

SGSI	Probabilidad
Planificar	Establecer el contexto Valoración del riesgo Planificación del tratamiento del riesgo Aceptación del riesgo
Hacer	Implementación del plan de tratamiento del riesgo
Verificar	Monitoreo y revisión continuos de los riesgos
Actuar	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Las alternativas pensadas para el seguimiento son matriz de riesgos, mapa de calor y una línea de tiempo que dejará ver la evolución de cada riesgo desde el fase inicial donde se lo considera inherente hasta cuando se lo asume residual por la aplicación de controles, el valor agregado de esta línea de tiempo es que permitirá revisar la traza completa de los controles operacionales implementados en el tratamiento de los riesgos.

Al igual que en los 2 módulos anteriores la integración de éste con otros sistemas y subsistemas ya existentes en la organización se rige al esquema expuesto en la Figura 4.8.

4.4.4 Seguridad y accesos

Como será una aplicación web que solo será accedida en la intranet de la organización por los usuarios del dominio correspondiente, la autenticación se hará contra Directorio Activo, es decir, que los usuarios se validarán contra la infraestructura del controlador de dominio de modo tal que accederán al sistema usando los mismos usuario y clave con los que ingresan a su equipo local.

Además la solución propuesta estará integrada al módulo de seguridad que gestiona los roles y los privilegios para los usuarios que acceden a diferentes módulos de la intranet en ASTINAVE EP. Algunos de los roles ya definidos con un esquema de privilegios simplificado (ver Figura 4.10) se pueden apreciar en las siguientes tablas (Tabla 21, Tabla 22 y Tabla 23).

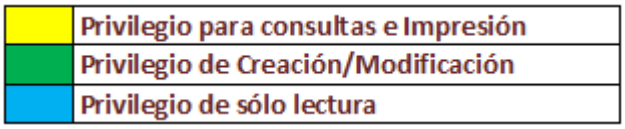


Figura 4.10 Privilegios para los roles.

Tabla 21 Privilegios de los Roles en Gestión de la norma.

	Gestión de la norma					
Rol	**1**	**2**	**3**	**4**	**5**	**6**
Oficial de Seguridad de la Información						
Responsable de Seguridad de la Información						
Gestor de Riesgos						
Revisor de Gestión						
Ejecutor de actividad de planes de acción						
1: Registrar y Mantener la norma						
2: Registrar requisitos de la norma						
3: Registrar y mantener declaración de aplicabilidad						
4: Asignar responsable de seguimiento de controles						
5: Asociar documento de SharePoint						
6: Verificar trazas de riesgo por control						

Tabla 22 Privilegios de los Roles en Gestión de Activos de información.

	Gestión de Activos Información						
Rol	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Oficial de Seguridad de la Información							
Responsable de Seguridad de la Información							
Gestor de Riesgos							
Revisor de Gestión							
Dueño de proceso							
Responsable de activo							
1: Registrar y Mantener procesos institucionales							
2: Registrar y mantener clasificación única de activos							
3: Registrar y mantener activos de Información							
4: Registrar tasación directa de los activos							
5: Registrar encuestas para valoración de impacto de los activos							
6: Realizar cálculos de la tasación de activos							
7: Responder encuestas							

Tabla 23 Privilegios de los Roles en Gestión de Riesgos.

	Gestión de Riesgos							
Rol	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Oficial de Seguridad de la Información								
Responsable de Seguridad de la Información								
Gestor de Riesgos								
Revisor de Gestión								
Dueño de proceso								
Responsable de activo								
Ejecutor de actividad de planes de acción								
1: Registrar y Mantener amenazas								
2: Registrar y mantener vulnerabilidades								
3: Asociar amenazas y vulnerabilidades								
4: Registrar y mantener riesgos								
5: Registrar y mantener planes de tratamiento								
6: Registrar acciones ejecutadas								
7: Verificar trazas de riesgos								
8: Verificar evolución de riesgos								

Una vez tratadas estas consideraciones funcionales, será necesario explicar cómo se llega al modelamiento y desarrollo de estos módulos; se verá al detalle en las siguientes secciones.

4.5 Modelos físicos en la base de datos

Para la representación del modelo físico de lo planteado en los módulos funcionales, se usará la siguiente simbología:

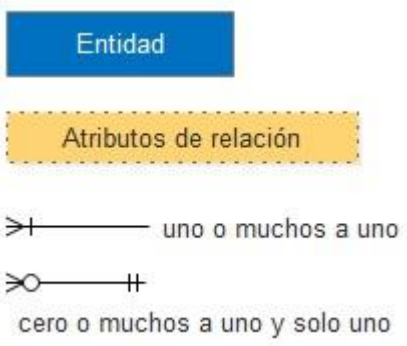


Figura 4.11 Simbología usada en el modelo físico.

A continuación para cada uno de los módulos funcionales se tiene el modelo físico de los datos así como el diccionario de datos correspondientes.

4.5.1 Gestión de los controles de la norma

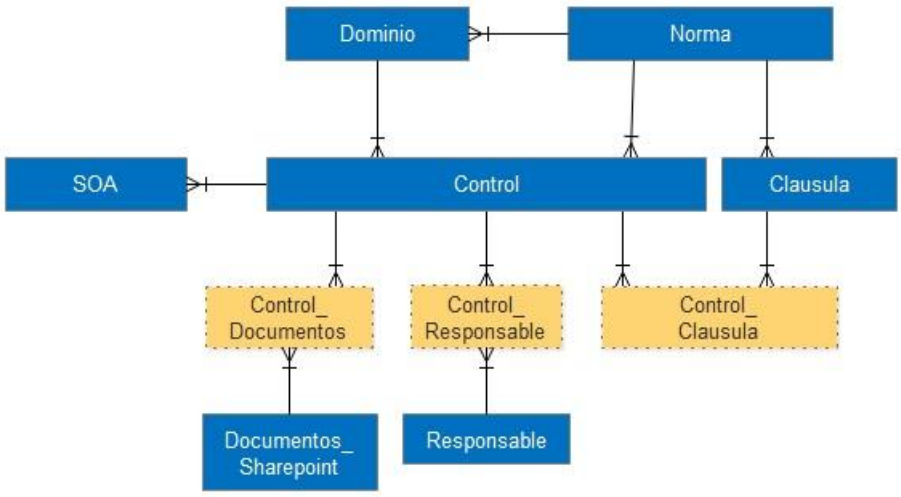


Figura 4.12 Modelo para Gestión de los controles de la norma

Tabla 24 Diccionario de datos: Gestión de los controles de la norma, Dominio.

Nombre Campo	Tipo	Descripción	PK	FK
autoid	int	Secuenciador incremental de los dominios de la norma	X	
codigo	string	Código que la norma tiene definido para cada dominio		
nombre	string	Denominación del dominio de la norma		
objetivo	string	Objetivo especificado en la norma		
norma	int	Referencia a la norma y su versión correspondiente		X
eliminado	bool	Indicador de si el dominio está habilitado para una versión de la norma en cuestión		

Tabla 25 Diccionario de datos: Gestión de los controles de la norma, Norma.

Nombre Campo	Tipo	Descripción	PK	FK
autoid	int	Secuenciador incremental de la norma	X	
norma	string	Nombre de la norma registrada		
version	string	Versión de la norma		
Anio	int	Año en que la versión de la norma se hace oficial		
descripción	string	Descripción de la norma norm. Ejemplo: ISO 27001:2013 v 1.0		

Tabla 26 Diccionario de datos: Gestión de los controles de la norma, Documento aplicabilidad.

Nombre Campo	Tipo	Descripción	PK	FK
Autoid	long	Secuenciador incremental de los controles considerados en el SoA	X	
Idcontrol	int	Referencia a los controles de la norma		X
Control	string	Campo desnormalizado que concatena el código y el titulo del control del cual se indica si aplica o no.		
Aplica	bool	Indicador de si aplica o no el control		

justificacion	*string*	*Explicación, motivo por el cual un control será considerado o no en el SoA.*		
Fecha_cre	*datetime*	*Fecha de registro inicial del control en el SoA*		
Usu_cre	*string*	*Usuario que realiza el registro inicial.*		
Fecha_mod	*datetime*	*Fecha de modificación del estado (Aplica/No Aplica) o justificación dentro del SoA.*		
Usu_mod	*string*	*Usuario que registra la mofificación.*		
Eliminado	*bool*	*Indicador de habilitación/deshabilitación de un registro.*		

Tabla 27 Diccionario de datos: Gestión de los controles de la norma, Control.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Autoid	*int*	*Secuenciador incremental de los controles especificados en el Anexo A de la norma*	*X*	
Código	*string*	*Código del control*		
Nombre	*string*	*Título del control especificado en el Anexo A de la norma*		
Descripción	*string*	*Descripción del control*		
Norma	*int*	*Referencia a la norma*		*X*

Tabla 28 Diccionario de datos: Gestión de los controles de la norma, Claúsula.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
autoid	*int*	*Secuenciador incremental de las claúsulas*	*X*	
codigo	*string*	*Código de la claúsula*		
titulo	*string*	*Título de la claúsula, o sea, el tópica de cada sección en el anexo SL*		
descripcion	*string*	*Descripción de la claúsula*		
norma	*int*	*Referencia a la norma*		*X*

Tabla 29 Diccionario de datos: Gestión de los controles de la norma, Responsable.

Nombre Campo	Tipo	Descripción	PK	FK
codigo	long	Id de cada empleado de ASTINAVE EP. Este código está asociado a la tabla maestra de empleado del ERP	X	
Nombres_ completos	string	Nombres y apellidos del empleado		
cargo	string	Cargo del empleado		

Tabla 30 Diccionario de datos: Gestión de los controles de la norma, Control Documento.

Nombre Campo	Tipo	Descripción	PK	FK
Autoid	long	Secuenciador incremental de los documentos que se asocian a un control de la norma	X	
Id_control	int	Referencia al control de la norma		X
Código_control	string	Código del control de la norma asociado		
Guid_documento	string	Guid del documento asociado. Este identificado único lo genera el gestor documental		X
nombre_ documento	string	Nombre del documento asociado		
Ruta_documento	string	Ruta del documento asociado		
Fecha_cre	datetime	Fecha en que realiza la asociación		
Usu_cre	string	Usuario que realiza la asociación		
Fecha_mod	datetime	Fecha en que se realiza la modificación		
Usu_mod	string	Usuario que realiza la modificación		
Eliminado	bool	Indicador del estado de habilitación de la asociación del control con algún documento		

4.5.2 Gestión de los activos de información

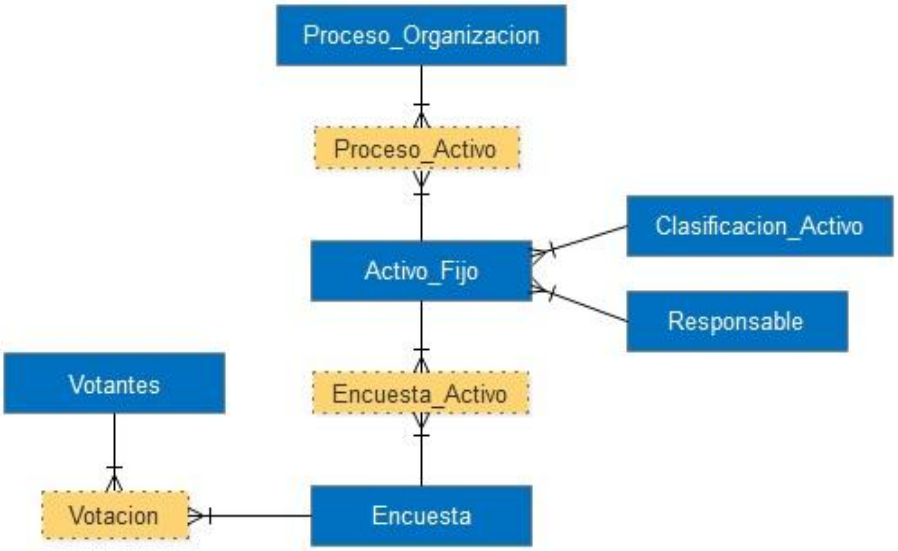


Figura 4.13 Modelo de Gestión de los activos de información.

Tabla 31 Diccionario de datos: Gestión de los activos de información, Tipo Proceso.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
autoid	*int*	*Secuenciador incremental de los tipo de proceso*	*X*	
codigo	*string*	*Código del tipo de proceso*		
nombre	*string*	*Denominación del tipo de proceso (Gobernante, de apoyo, etc.)*		

Tabla 32 Diccionario de datos: Gestión de los activos de información, Proceso.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Pro_id	*int*	*Secuenciador incremental de los procesos organizacionales*	*X*	
Pro_tipo	*int*	*Referencia del tipo de proceso*		*X*
Pro_codigo	*string*	*Código del proceso*		
Pro_nombre	*string*	*Nombre del proceso organizacional*		
Pro_parentid	*int*	*Referencia jerárquica del proceso para conformar el esquema macroproceso-proceso-subproceso.*		
Fecha_cre	*datetime*	*Fecha de registro del proceso.*		
Usu_cre	*string*	*Usuario que registra el proceso*		
Fecha_mod	*datetime*	*Fecha en que se realiza la modificación*		
Usu_mod	*string*	*Usuario que modifica el proceso*		
eliminado	*bool*	*Indicador de habilitación/deshabilitación del proceso*		

Tabla 33 Diccionario de datos: Gestión de los activos de información, Activo Información.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Ain_autoid	*Long*	*Secuenciador incremental de los activos de información*	*X*	
Ain_codigo_ clasificacion	*string*	*Código referenciado desde el nivel de la clasificación general de activos seleccionada*		*X*
Ain_codigo_nativo	*string*	*Código arrastrados desde otros sistemas como en los casos de activos fijos, personas y documentos*		
Ain_codigo_ heredado	*string*	*Es el código generado en función de la clasificación general seleccionada*		
Ain_tipo_activo	*string*	*Denominación del tipo de activo (bien, documento, persona, otro)*		
Ain_descripcion	*int*	*Descripción del activo de información*		
Ain_observaciones	*string*	*Observaciones/comentarios relevantes respecto al activo registrado*		
Ain_cod_ responsable	*long*	*Referencia al código único del custodio/responsable del activo de información*		*X*
Ain_responsable	*string*	*Campo desnormalizado para guardar los nombres completos del responsable del activo*		
Ain_fecha	*datetime*	*Fecha en la que se levantó el activo de información. Se asume que desde esa fecha el activo forma parte del catálogo único de activos de información de la organización*		
Ain_fecha_cre	*datetime*	*Fecha de registro del activo. Para auditoría.*		
Ain_usu_cre	*string*	*Usuario que registró el activo de información*		
Ain_fecha_mod	*datetime*	*Fecha de modificación del activo de Información.*		
Ain_usu_mod	*string*	*Usuario que modifica el activo de información*		
Ain_eliminado	*Bool*	*Indicador de habilitación/deshabilitación del activo.*		

Tabla 34 Diccionario de datos: Gestión de los activos de información, Proceso Activo.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Pac_autoid	*long*	*Secuenciador incremental de la relación*	*X*	
Pac_proceso	*int*	*Referencia a un proceso organizacional*		*X*
Pac_activo	*long*	*Referencia a un activo de información*		*X*
Pac_c	*decimal*	*Valor para la tasación del activo de información desde el enfoque de la confidencialidad*		
Pac_d	*decimal*	*Valor para la tasación del activo de información desde el enfoque de la disponibilidad*		
Pac_i	*decimal*	*Valor para la tasación del activo de información desde el enfoque de la integridad*		
Pac_t	*decimal*	*Valor para la tasación total (promediada) del activo de información*		
Pac_fecha_cre	*datetime*	*Fecha de registro inicial de la asociación.*		
Pac_usu_cre	*string*	*Usuario que realiza el registro inicial.*		
Pac_fecha_ mod	*datetime*	*Fecha de modificación del estado del registro.*		
Pac_usu_mod	*string*	*Usuario que registra la modificación.*		
eliminado	*Bool*	*Indicador de habilitación/deshabilitación de un registro.*		

Tabla 35 Diccionario de datos: Gestión de los activos de información, Clasificación activo.

Nombre Campo	Tipo	Descripción	PK	FK
Cac_id	int	Secuenciador incremental de la clasificación para activos de información	X	
Cac_parentid	int	Referencia para la jerarquización de la clasificación de activos de información.		
Cac_codigo	string	Código de la clasificación		
Cac_nombre	string	Nombre de la clasificación para activos de la información		
Cac_descripcion	string	Descripción de la clasificación para activos de información		
Cac_fecha_cre	datetime	Fecha de registro de la clasificación		
Cac_usu_cre	string	Usuario que realizó el registro		
Cac_fecha_mod	datetime	Fecha de modificación de la clasificación		
Cac_usu_mod	string	Usuario que realiza la modificación		
Cac_eliminado	bool	Indicador de habilitación/deshabilitación de un registro.		

Tabla 36 Diccionario de datos: Gestión de los activos de información, Encuesta.

Nombre Campo	Tipo	Descripción	PK	FK
Enc_autoid	long	Secuenciador incremental	X	
Enc_procesoid	int	Referencia al proceso organizacional		X
Enc_descripcion	string	Descripción para la encuesta		
Enc_estado	string	Estado de la encuestas (pendiente, cerrada)		
Enc_fecha_ini	datetime	Fecha a partir de la cual se puede empezar a responder la encuesta.		
Enc_hora_ini	datetime	Hora a partir de la cual se puede empezar a responder la encuesta.		
Enc_fecha_fin	datetime	Fecha hasta la cual se puede responder la encuesta.		
Enc_hora_fin	datetime	Hora hasta la cual se puede responder la encuesta.		
Enc_fecha_cre	datetime	Fecha del registro de la encuesta		
Enc_usu_cre	string	Usuario que registra la encuesta		
Enc_fecha_mod	datetime	Fecha de modificación		
End_usu_mod	string	Usuario que modifica la encuesta		
End_eliminado	bool	Indicador de habilitación/ deshabilitación de un registro.		

Tabla 37 Diccionario de datos: Gestión de los activos de información, Encuesta Activo.

Nombre Campo	Tipo	Descripción	PK	FK
Eac_autoid	long	Secuenciador incremental	X	
Eac_encuesta	long	Referencia a la encuesta		X
Eac_activo	Long	Referencia al activo de información		X
Eac_fecha_cre	datetime	Fecha de registro de la relación		
Eac_usu_cre	string	Usuario que registra la relación		
Eac_fecha_mod	datetime	Fecha de modificación		
Eac_usu_mod	string	Usuario que modifica la relación		
Eac_eliminado	Bool	Indicador de habilitación/ deshabilitación de un registro.		

Tabla 38 Diccionario de datos: Gestión de los activos de información, Votación.

Nombre Campo	Tipo	Descripción	PK	FK
Vot_autoid	long	Secuenciador incremental	X	
Vot_encuesta	long	Referencia a la encuesta		X
Vot_proceso	int	Referencia al proceso organizacional		X
Vot_activo	long	Referencia al activo de información		X
Vot_cod_erp	long	Referencia al código único del votante		X
Vot_votante	string	Campo desnormalizado para conservar directamente nombre y apellidos del votante		
Vot_observación	string	Observaciones del votante		
Vot_c	decimal	Valor de impacto puesto por el votante para el enfoque de la confidencialidad		
Vot_d	decimal	Valor de impacto puesto por el votante para el enfoque de la disponibilidad		
Vot_i	decimal	Valor de impacto puesto por el votante para el enfoque de la integridad		
Vot_fecha_cre	datetime	Fecha de registro de la votación		
Vot_usu_cre	string	Usuario que registra la votación		
Vot_fecha_mod	datetime	Fecha de modificación de la votación		
Vot_usu_mod	string	Usuario que modifica la votación		
Vot_eliminado	bool	Indicador de habilitación/deshabilitación .		

4.5.3 Gestión de Riesgos

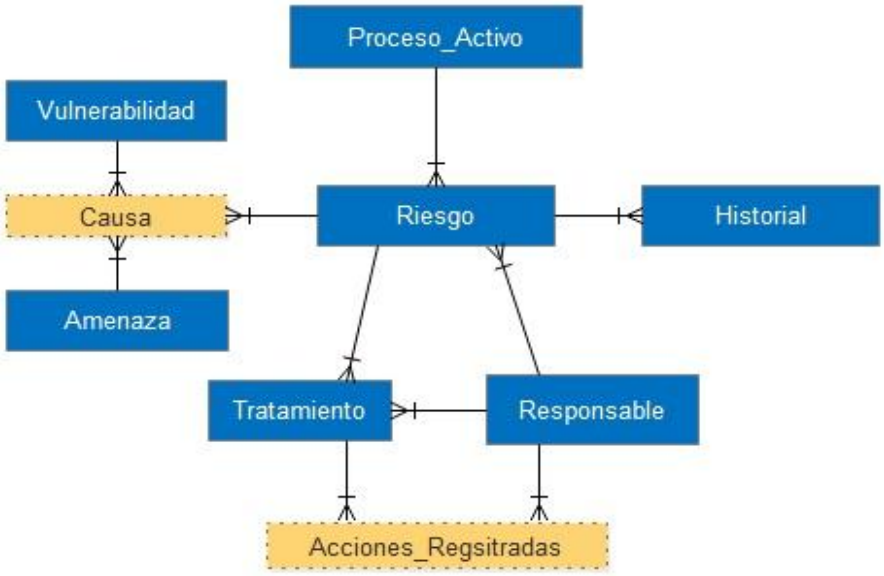


Figura 4.14 Modelo para Gestión de Riesgos

Tabla 39 Diccionario de datos: Gestión de Riesgos, Amenaza.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Ame_id	*int*	*Secuenciador incremental de las amenazas*	*X*	
Ame_parentid	*int*	*Autoreferencia para definir un árbol jerárquico de las amenazas*		
Ame_codigo	*string*	*Código de la amenaza*		
Ame_nombre	*string*	*Denominación de la amenaza*		
Ame_fecha_cre	*datetime*	*Fecha de registro de la amenaza*		
Ame_usu_cre	*string*	*Usuario que registró la amenaza*		
Ame_fecha_mod	*datetime*	*Fecha de modificación de la amenaza*		
Ame_usu_mod	*string*	*Usuario que modifica la amenaza*		
Ame_eliminado	*bool*	*Indicador de habilitación/ deshabilitación de un registro.*		

Tabla 40 Diccionario de datos: Gestión de Riesgos, Vulnerabilidad.

Nombre Campo	Tipo	Descripción	PK	FK
vul_id	int	Secuenciador incremental de las vulnerabilidades	X	
vul _parentid	int	Autoreferencia para definir un árbol jerárquico de las vulnerabilidades		
vul _codigo	string	Código de la vulnerabilidad		
vul _nombre	string	Denominación de la vulnerabilidad		
vul _fecha_cre	datetime	Fecha de registro de la vulnerabilidad		
vul _usu_cre	string	Usuario que registró la vulnerabilidad		
vul _fecha_mod	datetime	Fecha de modificación de la vulnerabilidad		
vul _usu_mod	string	Usuario que modifica la vulnerabilidad		
vul _eliminado	bool	Indicador de habilitación/deshabilitación de un registro.		

Tabla 41 Diccionario de datos: Gestión de Riesgos, Amenaza vulnerabilidad.

Nombre Campo	Tipo	Descripción	PK	FK
Vam_autoid	long	Secuenciador incremental del par amenaza-vulnerabilidad	X	
Vam_amenaza	int	Referencia a la amenaza		X
Vam_ vulnerabilidad	int	Referencia a la vulnerabilidad		X
Vam_fecha_cre	datetime	Fecha de registro del par amenaza-vulnerabilidad		
Vam_usu_cre	string	Usuario que registra el par amenaza-vulnerabilidad		
Vam_fecha_mod	datetime	Fecha de modificación del par amenaza-vulnerabilidad		
Vam_usu_mod	string	Usuario que modifica el par amenaza-vulnerabilidad		
Vam_eliminado	bool	Indicador de habilitación/deshabilitación del par amenaza-vulnerabilidad		

Tabla 42 Diccionario de datos: Gestión de Riesgos, Causa.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Pav_autoid	*long*	*Secuenciador incremental de la causa (conjunto de pares amenazas-vulnerabilidades con probabilidad de ocurrencia definida)*	*X*	
Pav_proceso	*int*	*Referencia al proceso organizacional*		*X*
Pav_activo	*long*	*Referencia al activo de información*		*X*
Pav_amenaza	*int*	*Referencia a la amenaza*		*X*
Pav_ vulnerabilidad	*int*	*Referencia a la vulnerabilidad*		*X*
Pav_riesgo	*long*	*Referencia al riesgo*		*X*
Pav_probabilidad	*decimal*	*Valor de la probabilidad de ocurrencia del par amenaza-vulnerabilidad*		
Pav_consecuencia	*string*	*Descripción de la consecuencia en el activo por esta causa*		
Pav_fecha_cre	*datetime*	*Fecha de creación de la causa*		
Pav_usu_cre	*string*	*Usuario que registra la causa*		
Pav_fecha_mod	*datetime*	*Fecha de modificación de la causa*		
Pav_usu_mod	*string*	*Usuario que modifica la causa*		
Pav_eliminado	*bool*	*Indicador de habilitación/deshabilitación de la causa*		

Tabla 43 Diccionario de datos: Gestión de Riesgos, Riesgos.

Nombre Campo	Tipo	Descripción	PK	FK
Ari_autoid	long	Secuenciador incremental para cada riesgo	X	
Ari_descripcion	string	Descripción del riesgo		
Ari_proceso_activo	long	Referencia a la relación proceso-activo		X
Ari_prob_causa	decimal	Valor promediado de la probabilidad de ocurrencia de todos los pares amenaza-vulnerabilidad que componen la causa		
Ari_impacto_ tasacion	decimal	Valor del impacto que para ese activo de información en ese proceso de la organización se definió en el proceso de tasación directo o por votación de los involucrados		
Ari_riesgo	decimal	Valor del riesgo (IxP)		
Ari_consecuencia	string	Descripción de la consecuencia del riesgo sobre el activo de información		
Ari_cod_ responsable	long	Código único del responsable del riesgo		
Ari_responsable	string	Campo desnormalizado que guarda nombres y apellidos del responsable del riesgo.		
Ari_fecha	datetime	Fecha con la cual se indica que el riesgo empezó a ser gestionado		
Ari_fecha_cre	datetime	Fecha de registro del riesgo		
Ari_usu_cre	string	Usuario que registra el riesgo		
Ari_fecha_mod	datetime	Fecha de modificación del riesgo		
Ari_usu_mod	string	Usuario que modifica el riesgo		
Ari_eliminado	bool	Indicador de habilitación/deshabilitación del riesgo		

Tabla 44 Diccionario de datos: Gestión de Riesgos, Plan tramitamiento.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Ria_autoid	*long*	*Secuenciador incremental del plan de tratamiento del riesgo*	*X*	
Ria_riesgo	*long*	*Referencia al riesgo*		*X*
Ria_accion	*string*	*Descripción de la acción propuesta para el correspondiente tratamiento del riesgo*		
Ria_idhistorial	*long*	*Referencia al registro del riesgo en el historial correspondiente*		*X*
Ria_cod_ responsable	*long*	*Código único del responsable de la acción propuesta*		*X*
Ria_responsable	*string*	*Campo desnormalizado que guarda nombres y apellidos del responsable de la acción propuesta*		
Ria_respuesta	*string*	*Respuesta al riesgo (mitigar, aceptar, evitar, transferir)*		
Ria_observaciones	*string*	*Observaciones sobre la acción propuesta*		
Ria_fecha	*datetime*	*Fecha de cumplimiento de la acción propuesta*		
Ria_causa	*long*	*Referencia a la causa asociado al riesgo al que se está dando tratamiento*		*X*
Ria_fecha_cre	*datetime*	*Fecha de registro de la acción propuesta*		
Ria_usu_cre	*string*	*Usuario que registra la acción propuesta*		
Ria_fecha_mod	*datetime*	*Fecha de modificación de la acción propuesta*		
Ria_usu_mod	*string*	*Usuario que modifica la acción propuesta*		
Ria_eliminado	*bool*	*Indicador de habilitación/deshabilitación de la acción propuesta*		

Tabla 45 Diccionario de datos: Gestión de Riesgos, Plan control

Nombre Campo	Tipo	Descripción	PK	FK
Pco_autoid	long	Secuenciador incremental de la relación entre el plan (acción propuesta) y algún control de la norma (Anexo A)	X	
Pco_plan	long	Referencia al plan de acciones para el tratamiento al riesgo		X
Pco_control	int	Referencia al control de la norma		X
Pco_fecha_cre	datetime	Fecha de registro de la relación		
Pco_usu_cre	string	Usuario que registra la relación		
Pco_fecha_mod	datetime	Fecha de modificación de la relación		
Pco_usu_mod	string	Usuario que modifica la relación		
Pco_eliminado	bool	Indicador de habilitación/deshabilitación de la relación		

Tabla 46 Diccionario de datos: Gestión de Riesgos, Acción.

Nombre Campo	Tipo	Descripción	PK	FK
Rpa_autoid	long	Secuenciador incremental de la acción realizada	X	
Rpa_plan	long	Referencia del plan (acción propuesta)		X
Rpa_fecha	datetime	Fecha de ejecución de la acción realizada		
Rpa_accion	string	Descripción de lo realizado		
Rpa_cod_ ejecutor	long	Código único del ejecutor de la acción		X
Rpa_ejecutor	string	Campo desnormalizado que guarda nombres y apellidos del ejecutor de la acción realizada		
Rpa_estado	string	Estado de la acción realizada		
Rpa_fecha_cre	datetime	Fecha de registro de la acción ejecutada		
Rpa_usu_cre	string	Usuario que registra la acción ejecutada		
Rpa_fecha_mod	datetime	Fecha de modificación de la acción ejecutada		
Rpa_usu_mod	string	Usuario que modifica la acción ejecutada		
Rpa_eliminado	bool	Indicador de habilitación/ deshabilitación de la acción realizada		

Tabla 47 Diccionario de datos: Gestión de Riesgos, Historial riesgo.

Nombre Campo	*Tipo*	*Descripción*	*PK*	*FK*
Hri_autoid	*long*	*Secuenciador incremental para registro del historial*	*X*	
Hri_riesgo	*long*	*Referencia al riesgo*		*X*
Hri_p	*decimal*	*Valor de la probabilidad de ocurrencia*		
Hri_i	*decimal*	*Valor del impacto*		
Hri_r	*decimal*	*Valor del riesgo*		
Hri_quien	*string*	*Quién realiza el cambio que provoca un registro en el historial*		
Hri_timestamp	*datetime*	*Fecha de registro en el historial*		
Hri_eliminado	*bool*	*Indicador de habilitación/deshabilitación del registro del historial*		

4.6 Casos de Uso

A continuación la definición de actores y casos de uso en los módulos funcionales explicados previamente:

Tabla 48 Definición de Actores.

	Actor	Descripción
Miembros grupo metodológico del SGSI	Oficial de Seguridad de la Información	Es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones del SGSI
	Responsable de Seguridad de la Información	Es el responsable de supervisar y articular la ejecución de las medidas que se delinean en el SGSI.
	Gestor de Riesgos	Es el responsable de gestionar los riegos de los activos de información de la organización.
	Revisor de Gestión	Rol delegado por el gestor de riego que permite que un miembro del equipo de metodológico colabora con la supervisión de los riesgos.
Otros	Dueño de Proceso	Responsable de un proceso dentro de la organización.
	Responsable de activo de la información	Custodio asignado al activo de la información.
	Responsable de Riesgo	Responsable del riesgo del activo. En la práctica puede coincidir con el responsable del activo.
	Ejecutor de actividad de planes de acción	Responsable asignado para dar cumplimientos a una actividad dentro de un plan para el tratamiento de riesgos.
	Administrador del sistema	Responsable de los cambios en configuración, comportamiento y permisos del aplicativo para el SGSI

4.6.1 Casos de Uso para la Gestión de los controles de la norma

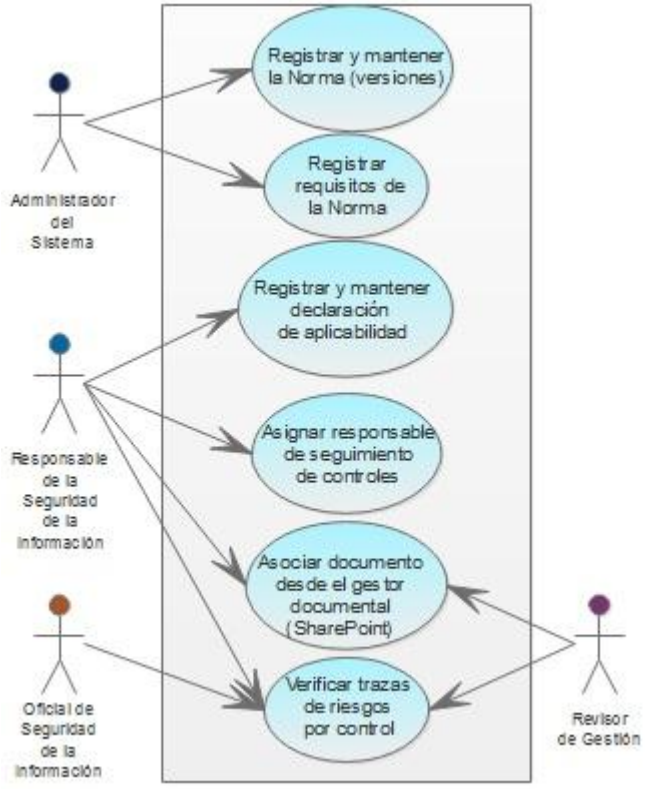


Figura 4.15 Casos de Uso: Gestión de los controles de la norma.

Tabla 49 Caso de uso: registro y mantenimiento de la norma.

Caso de Uso	Registro y mantenimiento de la norma
Actores	Administrador del sistema
Descripción	
Registro y mantenimiento de las versiones de la norma ISO 27001	
Condiciones/ Restricciones/Asunciones	
1. Como no existe una UI, esta operación se realizará directamente en base. 2. No se registrará una nueva norma a menos que la versión y el año de la misma no existan en los registros de la tabla correspondiente	
Curso Normal	**Alternativa**
1.- El administrador ingresa un nuevo registro en la base definiendo la versión y el año correspondientes	
2.- El administrador modifica algún dato sobre la norma	
3.- El administrador elimina un registro de la norma	3.1.- Si el registro de la norma afecta la integración referencial establecida con las cláusulas y controles de la misma, la base no permitirá que dicha operación se realice

Tabla 50 Caso de Uso: Registrar y mantener requisitos de la norma.

Caso de Uso	Registrar y mantener requisitos de la norma
Actores	Administrador del sistema
Descripción	
Ingreso en la base de requisitos de la norma: cláusulas (Anexo SL) y controles (Anexo A)	
Condiciones/ Restricciones/Asunciones	
Como no existe una UI, esta operación se realizará directamente en base.	
Curso Normal	**Alternativa**
1.-El administrador ingresa un nuevo registro con los requerimientos de la norma.	
2.- El administrador modifica los requisitos de la norma	
El administrador elimina un registro de requisito de la norma en el Anexo SL	Si el registro afecta la integración referencial establecida, la base no permitirá que dicha operación se realice
El administrador elimina un registro de requisito de la norma en el Anexo A	Si el registro afecta la integración referencial establecida, la base no permitirá que dicha operación se realice

Tabla 51 Caso de Uso: Registrar y mantener la declaración de aplicabilidad.

Caso de Uso	Registrar y mantener la declaración de aplicabilidad
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable gestiona el SoA.	
Condiciones/ Restricciones/Asunciones	
1. Se hace uso de la UI web implementada para ello. 2. Se puede cambiar n-veces si un control del anexo A aplica o no al igual que su justificación correspondiente.	
Curso Normal	**Alternativa**
1.-El responsable busca los controles por dominio y procede a indicar con un check si aplica en el SGSI y cuál es la justificación respectiva. Se guarda.	1.1-El responsable busca los controles por dominio y procede a desaplicarlos del SGSI y a escribir cual es la justificación respectiva. Se guarda.

Tabla 52 Caso de Uso: Asignar responsable a seguimiento de controles.

Caso de Uso	Asignar responsable a seguimiento de controles
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable deberá individualmente o grupalmente seleccionar controles del anexo A y asignarles un responsable de seguimiento.	
Condiciones/ Restricciones/Asunciones	
1. El responsable asignado deberá tener el rol de revisor de gestión 2. La búsqueda de responsables está integrada a la base e nómina y del ERP	
Curso Normal	**Alternativa**
1.-El responsable busca los controles por dominio y procede a chequearlos, luego busca los responsables y los asigna.	1.1-El responsable busca los controles por dominio y procede a chequearlos, luego busca los responsables y los desasigna.

Tabla 53 Caso de Uso: Asociar documentos.

Caso de Uso	Asociar documentos
Actores	Responsable de Seguridad de la Información Revisor de gestión
Descripción	
El responsable o revisor deberá individualmente o grupalmente seleccionar controles del anexo A y asociarlos a uno o varios documentos controlados desde el gestor documental (Sharepoint)	
Condiciones/ Restricciones/Asunciones	
Los documentos habilitados en la búsqueda serán aquello que estén en la librería del Sistema Integrado de Gestión en Sharepoint	
Curso Normal	**Alternativa**
1.-El responsable o revisor busca los controles por dominio y procede a chequearlos/seleccionarlos, luego busca los documentos y los asocia.	1.1-El responsable o revisor busca los controles por dominio y procede a chequearlos/seleccionarlos, luego busca los documentos y los desasocia.

Tabla 54 Caso de Uso: Verificar trazas de riesgos por control.

Caso de Uso	Verificar trazas de riesgos por control
Actores	Oficial de Seguridad de la Información Responsable de Seguridad de la Información Revisor de gestión
Descripción	
El oficial, responsable o revisor deberá seleccionar un control del anexo A y verificar los riesgos en cuyos planes de acción este control ha sido considerado para mitigación.	
Condiciones/ Restricciones/Asunciones	
En el línea de tiempo que se aprecia para cada riesgo toma mucha relevancia el registro del historial del riesgo que fue considerado a la hora de definir un plan de acción para ese riesgo	
Curso Normal	**Alternativa**
1.-El oficial, responsable o revisor busca los controles por dominio y procede a chequear/seleccionar alguno de ellos, luego busca los riesgos asociados a fin de verificar por cada riesgo una línea de tiempo en donde se pueden apreciar las acciones propuestas y las realizadas para dar tratamiento a ese riesgo.	

4.6.2 Casos de Uso para la Gestión de los activos de información

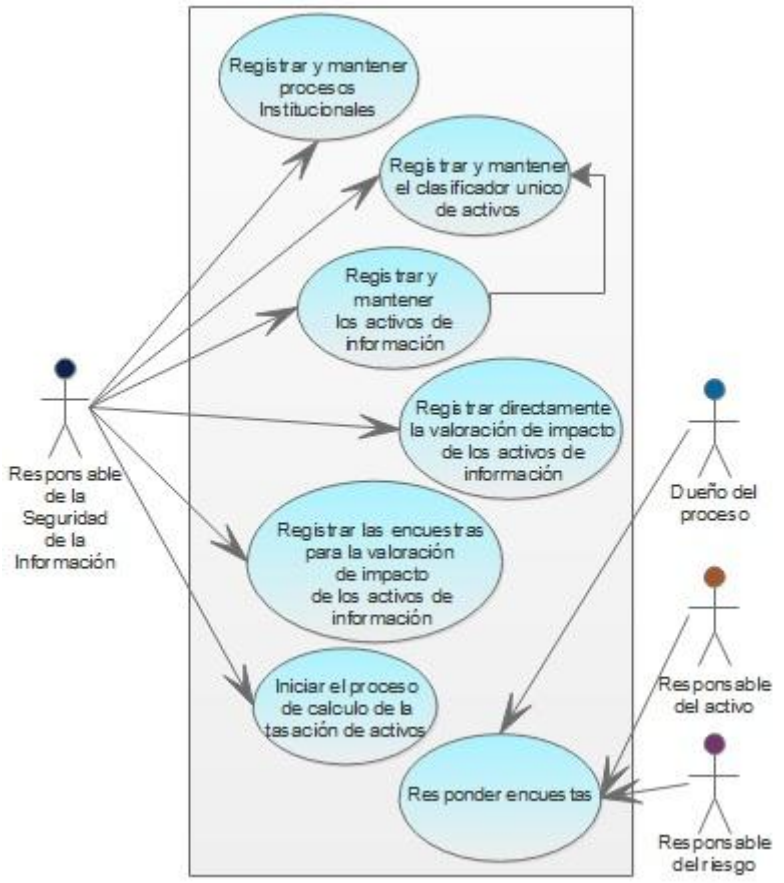


Figura 4.16 Casos de Uso: Gestión de los activos de información.

Tabla 55 Caso de Uso: Registrar y mantener procesos institucionales.

Caso de Uso	Registrar y mantener procesos institucionales
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable deberá registra y mantener el árbol de macroprocesos/procesos/subprocesos de la organización	
Condiciones/ Restricciones/Asunciones	
Los cambios en el árbol de procesos deberán previamente ser aprobados por el gerente general. La codificación jerárquica de los procesos es automática.	
Curso Normal	**Alternativa**
1.-El responsable elige algún nivel del árbol para crear un nuevo nodo, para modificar o eliminar el nodo seleccionado.	

Tabla 56 Caso de Uso: Registrar y mantener el clasificador único de activos.

Caso de Uso	Registrar y mantener el clasificador único de activos
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable deberá registrar y mantener el árbol de la clasificación única para los activos de información	
Condiciones/ Restricciones/Asunciones	
Los cambios en el clasificador deberán ser previamente aprobados por el Comité de Seguridad de la Información de la organización.	
Curso Normal	**Alternativa**
1.- El responsable elige algún nivel del árbol del clasificador para crear uno nuevo, para modificar o eliminar el nodo seleccionado.	

Tabla 57 Caso de Uso: Registrar y mantener los activos de información.

Caso de Uso	Registrar y mantener los activos de información
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable deberá registrar y mantener el catálogo único de activos de información haciendo uso del clasificador ya establecido	
Condiciones/ Restricciones/Asunciones	
1. Para el registro y gestión de cada activo de información, éste deberá vincularse a un proceso de la organización y a un subtipo de activo como 'bien', 'documento', 'persona', 'otro'. 2. Para el caso de que el activo de información sea subtipado como un bien la fecha y el responsable serán la fecha de compra y el custodio del bien, respectivamente. La integración a nivel de los sistemas es con la base de activos fijos del ERP. 3. Para el caso de que el activo de información sea 'documento' la integración será con el gestor documental de la organización (Sharepoint). 4. Para el caso de que el activo de información sea 'persona' la integración será con la base de empleados activos de la organización. 5. Para el caso de que el activo de información sea 'otro' se hará referencia escrita del mismo tan exhaustiva como se quiera. 6. La codificación de los activos es automática y va en función del código del clasificador seleccionado. Así se consigue que exista un Catálogo Único de Activos de Información.	
Curso Normal	**Alternativa**
1.-El responsable elige algún nivel del árbol del clasificador para indicar que es en esta clasificación en donde registrará un nuevo activo. Tanto si se crea o modifica un activo, el responsable deberá elegir una fecha de control y un responsable.	
2.- El responsable elige algún nivel del árbol del clasificador para indicar que es en esta clasificación en donde quiere revisar los activos registrados. Podrá modificar o eliminar activos.	

Tabla 58 Caso de Uso: Registrar encuestas para valoración de activos.

Caso de Uso	Registrar encuestas para valoración de activos
Actores	Responsable de Seguridad de la Información
Descripción	
El responsable deberá registrar encuestas para que los involucrados en los procesos organizacionales asociados a los activos de información pueda votar por el impacto de los mismos.	
Condiciones/ Restricciones/Asunciones	
1. Las encuestas requerirán una reunión formal posterior para que los involucrados procedan a la votación correspondiente.	
Curso Normal	**Alternativa**
1.-Para el registro de la encuesta el responsable deberá elegir un proceso organizacional, del conjunto de activos de información asociados a este proceso podrá elegir sobre cuales se realizará la tasación. Asimismo deberá definir el lapso de vigencia de la encuesta y quiénes responderán.	
2.-El responsable podrá eliminar una encuesta previamente registrada.	

Tabla 59 Caso de Uso: Responder a encuestas.

Caso de Uso	Responder a encuestas
Actores	Dueño del proceso Responsable de activo Responsable de riesgo
Descripción	
Los votantes podrán realizar una valoración del impacto para cada activo de información puesto en la encuesta en función de la confidencialidad, disponibilidad e integridad.	
Condiciones/ Restricciones/Asunciones	
1. Los votantes ya conocen la metodología de valoración de impacto (tasación) para los activos de información. Existe una escala de impacto con enfoque para la afectación de la organización en la imagen, lo operativo, lo financiero y lo legal. 2. Sólo se podrán responder encuestas si está vigente 3. En todo momento los involucrados y los miembros del grupo metodológico podrán verificar cómo avanzan las votaciones.	
Curso Normal	**Alternativa**
1.-Los votantes ingresan a la encuesta y para cada activo dan un valor de 1 a 5 para los criterios de confidencialidad, disponibilidad e integridad. El promedio de estos valores es la tasación del activo.	
2.- Mientras la encuesta esté vigente los votantes podrán modificar los valores de la tasación para cualquiera de los activos considerados en la encuesta.	

Tabla 60 Caso de Uso: Procesar automáticamente la tasación de activos.

Caso de Uso	Procesar automáticamente la tasación de activos
Actores	Responsable de seguridad de la información
Descripción	
El responsable deberá por cada proceso organizacional, dar un click (operación bajo demanda) para iniciar el proceso que tomará todas las votaciones de los activos de información asociados a ese proceso y obtener para cada activo el valor de impacto que será considerado en la gestión de riesgo correspondiente.	
Condiciones/ Restricciones/Asunciones	
1. Por cada ejecución del proceso automático el sistema le permite al responsable generar un registro en el historial de los riesgos.	
Curso Normal	**Alternativa**
1.-el responsable selecciona un proceso de la organización y ejecuta el proceso que automáticamente calculará la tasación para todos los activos involucrados en ese proceso, y, que obviamente, hayan sido considerados en las votaciones. El responsable tiene la opción de afectar el historial de riesgos de ese activo.	1.1.-el responsable selecciona un proceso de la organización y ejecuta el proceso que automáticamente calculará la tasación para todos los activos involucrados en ese proceso, y, que obviamente, hayan sido considerados en las votaciones. El responsable tiene la opción de no afectar el historial de riesgos de ese activo.

Tabla 61 Caso de Uso: Realizar tasación directa de los activos.

Caso de Uso	Realizar tasación directa de los activos
Actores	Responsable de seguridad de la información
Descripción	
El responsable podrá omitir la generación de encuestas y las votaciones correspondientes para proceder a un registro directo de la tasación de cada activo.	
Condiciones/ Restricciones/Asunciones	
1. Se asume que el responsable se respaldará en un juicio de experto para la tasación directa.	
Curso Normal	**Alternativa**
1.-el responsable seleccionará uno o más activos de información y registrará la valoración para la confidencialidad, disponibilidad e integridad, el sistema calculará automáticamente la tasación como el promedio de los 3 valores ingresados.	

4.6.3 Casos de Uso para la Gestión de Riesgos

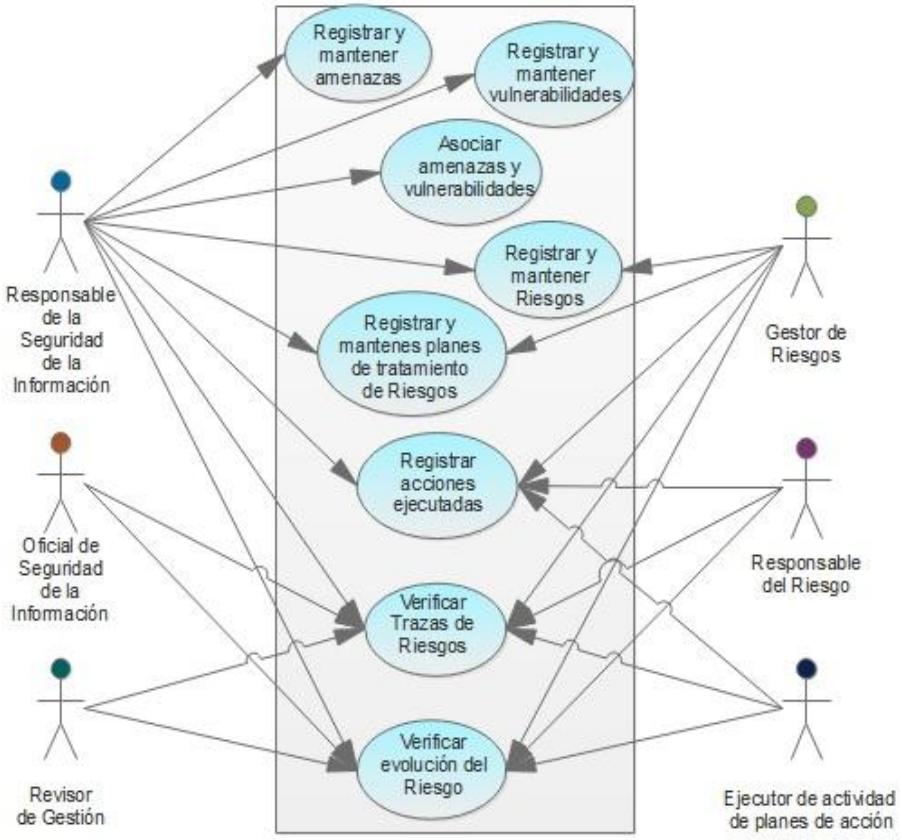


Figura 4.17 Casos de Uso: Gestión de Riesgos.

Tabla 62 Caso de Uso: Registro y mantenimiento de amenazas.

<table>
<tr><td>Caso de Uso</td><td colspan="2">Registro y mantenimiento de amenazas</td></tr>
<tr><td>Actores</td><td colspan="2">Responsable de seguridad de la información</td></tr>
<tr><td colspan="3">Descripción</td></tr>
<tr><td colspan="3">El responsable de seguridad de la información deberá registrar y dar mantenimiento al árbol jerárquico de amenazas a los activos de información.</td></tr>
<tr><td colspan="3">Condiciones/ Restricciones/Asunciones</td></tr>
<tr><td colspan="3">1. Para la metodología de riesgos implementada en el sistema, amenazas son las situaciones que potencialmente podrían desencadenar un incidente en la seguridad de la información.
2. Las amenazas inicialmente cargadas en el sistema son las especificadas como comunes en el Anexo C de la 27005.
3. La codificación de las amenazas es automática.</td></tr>
<tr><td>Curso Normal</td><td colspan="2">Alternativa</td></tr>
<tr><td>1.- El responsable de seguridad de la información se ubica en algún nivel del árbol de amenazas y elige la opción para generar una nueva amenaza. El sistema notifica que la operación se realizó con éxito.</td><td colspan="2"></td></tr>
<tr><td>2.- El responsable de seguridad de la información se ubica en algún nivel del árbol de amenazas y elige la opción para modificar la amenaza. El sistema notifica que la operación se realizó con éxito.</td><td colspan="2"></td></tr>
<tr><td>3.- El responsable de seguridad de la información se ubica en algún nivel del árbol de amenazas y elige la opción para eliminar la amenaza. El sistema notifica que la operación se realizó con éxito.</td><td colspan="2">3.1- El responsable de seguridad de la información se ubica en algún nivel del árbol de amenazas y elige la opción para eliminar la amenaza. El sistema notifica que la operación no se puede completar porque la amenaza a ser eliminada está asociada a vulnerabilidades.</td></tr>
</table>

Tabla 63 Caso de Uso: Registro y mantenimiento de vulnerabilidades.

Caso de Uso	Registro y mantenimiento de vulnerabilidades
Actores	Responsable de seguridad de la información
Descripción	
El responsable de seguridad de la información deberá registrar y dar mantenimiento al árbol jerárquico de vulnerabilidades. Las vulnerabilidades se definen como debilidades de los activos de información que pudieran ser explotadas por una amenaza	
Condiciones/ Restricciones/Asunciones	
1. Para la metodología de riesgos implementada en el sistema, una vulnerabilidad es la debilidad de un activo de información que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo. 2. Las vulnerabilidades inicialmente cargadas en el sistema son las especificadas como comunes en el Anexo D de la 27005. 3. La codificación de las vulnerabilidades es automática.	
Curso Normal	**Alternativa**
1.- El responsable de seguridad de la información se ubica en algún nivel del árbol de vulnerabilidades y elige la opción para generar una nueva vulnerabilidad. El sistema notifica que la operación se realizó con éxito.	
2.- El responsable de seguridad de la información se ubica en algún nivel del árbol de vulnerabilidades y elige la opción para modificar la vulnerabilidad. El sistema notifica que la operación se realizó con éxito.	
3.- El responsable de seguridad de la información se ubica en algún nivel del árbol de vulnerabilidades y elige la opción para eliminar la vulnerabilidad. El sistema notifica que la operación se realizó con éxito.	3.1- El responsable de seguridad de la información se ubica en algún nivel del árbol de vulnerabilidades y elige la opción para eliminar la vulnerabilidad. El sistema notifica que la operación no se puede completar porque la vulnerabilidad a ser eliminada está asociada a una causa de riesgo que se está controlando.

Tabla 64 Caso de Uso: Asociar amenazas y vulnerabilidades.

Caso de Uso	Asociar amenazas y vulnerabilidades
Actores	Responsable de seguridad de la información
Descripción	
El responsable deberá asociar amenazas vs vulnerabilidades a fin de definir causas de riesgos en los activos de información.	
Condiciones/ Restricciones/Asunciones	
1. La relación entre amenazas y vulnerabilidades se define de muchos a muchos. 2. Cada registro de esta relación se definirá como par amenaza-vulnerabilidad 3. Durante la operación de registro de pares amenaza-vulnerabilidad el sistema validará y evitará la duplicidad de estas relaciones.	
Curso Normal	**Alternativa**
1.-el responsable seleccionará uno o más amenazas y buscará una o más vulnerabilidades para asociarlas. El sistema notificará el éxito de la operación e indicará cuántos pares amenaza-vulnerabilidad registró.	
2.-el responsable seleccionará uno o más amenazas y podrá eliminar una o más vulnerabilidades asociadas. El sistema notificará el éxito de la operación.	2.1.-el responsable seleccionará uno o más amenazas y podrá eliminar una o más vulnerabilidades asociadas. El sistema notificará que la operación no procede porque el par amenaza-vulnerabilidad está asociado a una causa de riesgo que está siendo controlado.

Tabla 65 Caso de Uso: Registrar y mantener riesgos.

Caso de Uso	Registrar y mantener riesgos
Actores	Responsable de seguridad de la información Gestor de riesgos
Descripción	
El responsable o el gestor deberán registrar y controlar los riesgos por cada activo de información. Esta operación constituye la fase de identificación, análisis y evaluación del riesgo.	
Condiciones/ Restricciones/Asunciones	
1. Se define como riesgo a la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. 2. La valoración de un riesgo se define como Impacto x Probabilidad. El impacto será la tasación de cada activo y la probabilidad será el promedio de las probabilidades de ocurrencia de todos los pares amenaza-vulnerabilidad que se constituyen en la causa del riesgo. 3. Cada cambio en el impacto o en la probabilidad provocará un registro automático en el historial del riesgo. 4. El primer registro de riesgo por defecto será el riesgo inherente; los cambios de valoración sucesivos en el tiempo en presencia de planes de acción pasarán a ser el riesgo residual.	
Curso Normal	**Alternativa**
1.-el responsable o el gestor seleccionarán uno o más activos y buscará conformar un conjunto específico de pares amenaza-vulnerabilidad con probabilidad de ocurrencia para cada uno de ellos. Una vez que guarda la causa de riesgo definida el valor del riesgo (IxP) se calculará de manera automática. A continuación debe definirse un nombre de riesgo, una fecha de control y un responsable.	
2.-el responsable o el gestor seleccionarán uno o más riesgos y procederá a eliminarlos. El sistema notificará el éxito de la operación.	2.1-el responsable o el gestor seleccionarán uno o más riesgos y procederá a eliminarlos. El sistema notificará que la operación no se puede realizar porque el riesgo ha generado planes de acción para su tratamiento.

Tabla 66 Caso de Uso: Registrar y mantener planes de acción para tratamiento de riesgos.

Caso de Uso	Registrar y mantener planes de acción para tratamiento de riesgos
Actores	Responsable de seguridad de la información Gestor de riesgos
Descripción	
El responsable o el gestor deberán registrar y mantener los planes de acción para el tratamiento respectivo a cada riesgo identificado y evaluado.	
Condiciones/ Restricciones/Asunciones	
1. Para cada acción propuesta se podrá vincular un proyecto que coadyuve al tratamiento del riesgo.	
Curso Normal	**Alternativa**
1.-el responsable o el gestor seleccionará un riesgo y definirá una acción a realizarse, para ello deberá indicar el registro del historial del riesgo a considerar, los pares amenaza-vulnerabilidad involucrados, la respuesta al riesgo, fecha de acción propuesta, un responsable de la ejecución, la periodicidad de la acción, los controles de la norma en el anexo a cuya implementación será un control operacional que ayudará a controlar el riesgo.	
2.-el responsable o el gestor eliminarán una acción registrada para ser realizada como parte del tratamiento de un riesgo. El sistema notificará el éxito de la operación.	2.1-el responsable o el gestor eliminarán una acción registrada para ser realizada como parte del tratamiento de un riesgo. El sistema notificará que la operación no procede dado la acción propuesta ya cuenta con registros de ejecución asociados.

Tabla 67 Caso de Uso: Registrar acciones ejecutadas.

Caso de Uso	Registrar acciones ejecutadas
Actores	Responsable de seguridad de la información Gestor de riesgos Responsable del riesgo Ejecutor de actividad de planes de acción
Descripción	
El responsable de seguridad de la información, el gestor, el responsable del riesgo o el ejecutor de la acción deberá registrar y mantener las acciones ya ejecutadas para el cumplimiento de los planes propuestos.	
Condiciones/ Restricciones/Asunciones	
1. Los 3 primeros actores procederán al registro de acciones sólo si se verifica que los ejecutores no han realizado el registro correspondiente. 2. En muchos de los casos el ejecutor de la actividad coincidirá con el responsable del riesgo 3. El registro de acciones ejecutadas con fechas no concordantes respecto a las fechas del riesgo y los planes de acción para su tratamiento no serán descartadas, pero en la verificación de las líneas de tiempo los actores en cuestión verificarán la inconsistencia.	
Curso Normal	**Alternativa**
1.- El responsable de seguridad de la información, el gestor, el responsable del riesgo o el ejecutor de la acción deberá registrar la acción ejecutada para el cumplimiento de los planes propuestos, describiendo lo realizado, el responsable, el estado (‘pendiente’, ‘cumplido’, ‘atendiéndose’, etc.) y la fecha de ejecución.	
2.- El responsable de seguridad de la información, el gestor, el responsable del riesgo o el ejecutor de la acción eliminará un registro de una acción ejecutada.	

Tabla 68 Caso de Uso: Verificar trazas de riesgos.

Caso de Uso	Verificar trazas de riesgos
Actores	Oficial de seguridad de la información Responsable de seguridad de la información Revisor de gestión Gestor de riesgos Responsable del riesgo Ejecutor de actividad de planes de acción
Descripción	
El oficial, el responsable de seguridad, el revisor, el gestor, el responsable del riesgo y el ejecutor de la actividad podrán verificar la trazabilidad de acciones por cada riesgo, para ello contarán con herramientas como la matriz de riesgos, reporte de acciones y primordialmente la visualización de líneas de tiempo.	
Condiciones/ Restricciones/Asunciones	
1. El registro de acciones ejecutadas con fechas no concordantes respecto a las fechas del riesgo y los planes de acción para su tratamiento verificarán dicha inconsistencia en la vista de la línea de tiempo	
Curso Normal	**Alternativa**
1.- El oficial, el responsable de seguridad, el revisor, el gestor, el responsable del riesgo y el ejecutor de la actividad podrán verificar la trazabilidad de acciones por cada riesgo, para ello seleccionarán un riesgo y buscarán la visualización de la línea de tiempo. Para revisión grupal harán uso de la opción de ver la matriz de riesgos o ver el reporte de acciones.	

Tabla 69 Caso de Uso: Verificar evolución del riesgo.

Caso de Uso	Verificar evolución del riesgo
Actores	Oficial de seguridad de la información Responsable de seguridad de la información Revisor de gestión Gestor de riesgos Responsable del riesgo
Descripción	
El oficial, el responsable de seguridad, el revisor, el gestor y el responsable del riesgo podrán verificar la evolución de los riesgos, para ello contarán con herramientas como el mapa de calor riesgos, la verificación directa por cada riesgo y la misma visualización de líneas de tiempo.	
Condiciones/ Restricciones/Asunciones	
1. Si se verifican inconsistencias en la vista de la línea de tiempo por causa de fechas mal establecidas en el esquema riesgo→plan→acción, la evolución del riesgo no estará clara 2. Implícitamente el sistema estará verificando los registros del historial de riesgos.	
Curso Normal	**Alternativa**
1.- El oficial, el responsable de seguridad, el revisor, el gestor y el responsable del riesgo podrán verificar la evolución del riesgo, para ello seleccionarán un riesgo y buscarán la opción para ver la evolución del riesgo qué les presentará el riesgo inherente y el residual directamente. También podrán hacer uso de la opción de ver la línea de tiempo.	

CAPÍTULO 5

IMPLEMENTACIÓN Y PRUEBAS

En este capítulo se revisarán detalles de la puesta en producción de la solución propuesta, desde la publicación hasta las pruebas de uso y aplicación para cada uno de los módulos funcionales. En la Figura 5.1 se aprecia el inicio de la aplicación para el SGSI desarrollada e implementada.

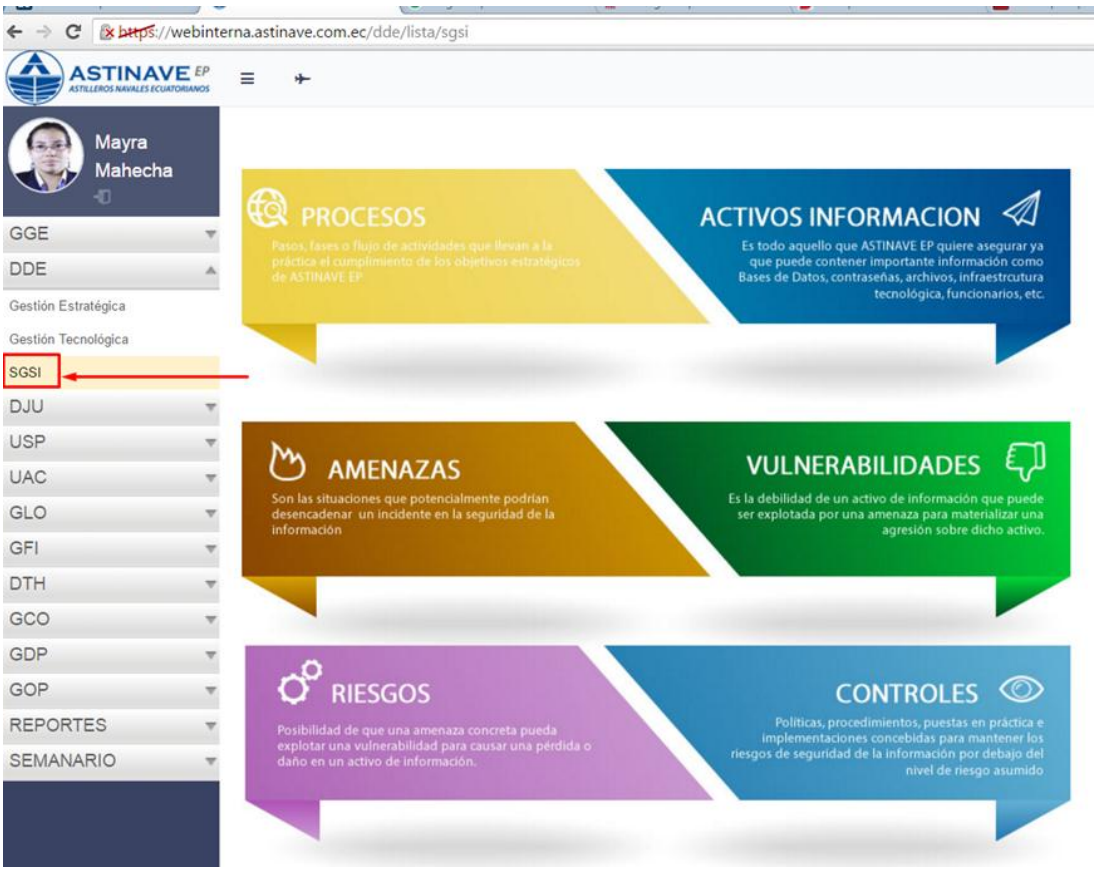


Figura 5.1 Vista principal del Aplicativo SGSI.

5.1 Entorno de producción

Considerando que la solución fue desarrollada usando el Framework .Net y, pese a que desde el 2015 éste fue liberado y se han dado pasos agigantados para su integración en plataformas LINUX, en esta implementación se usaron servidores virtuales con Windows Server 2012 R2.

En la Figura 5.2 se pueden apreciar los servidores involucrados en la implementación.

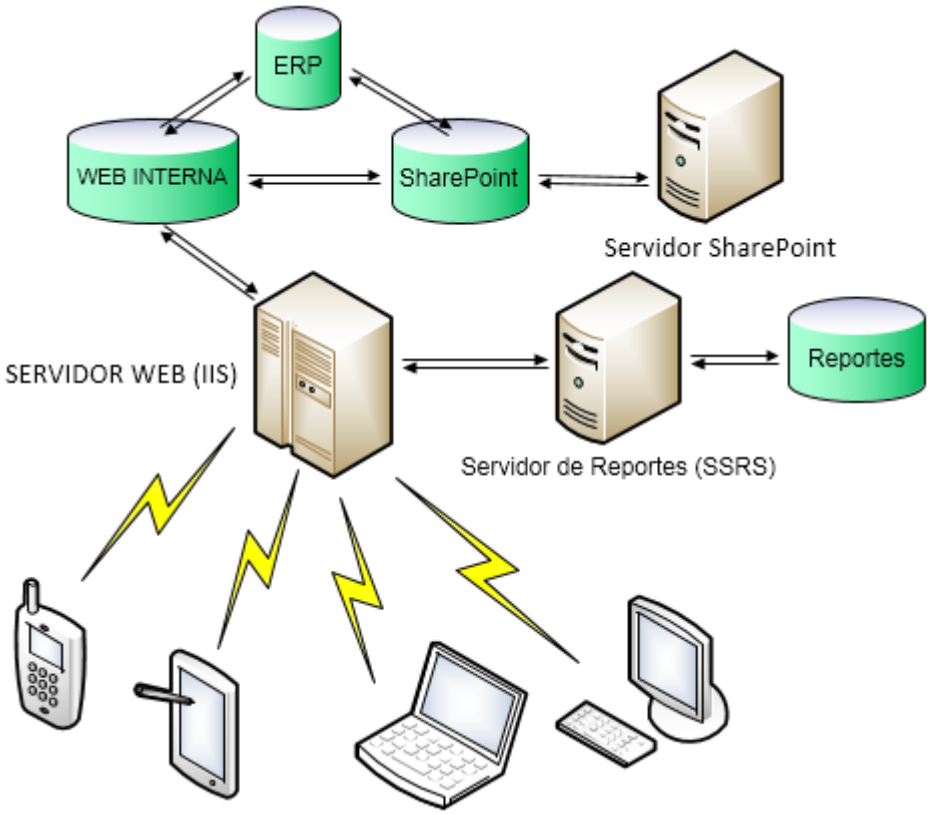


Figura 5.2 Arquitectura física de producción para la solución propuesta.

5.1.1 Servidor Web

El servidor web es el programa que permitirá almacenar y publicar páginas web, en este caso Active Server Pages, a las que el usuario accederá usando un browser.

Para Windows el servidor web establecido como un rol nativo es el Internet Information Services (IIS), el cual facilita tener las páginas web de los aplicativos de la intranet de la organización en un servidor. Además el IIS 8, la versión empleada para esta implementación, proporciona una plataforma segura, sencilla de

administrar y modular para hospedar sitios web HTML, ASP.NET, PHP, servicios FTP y servicios web ASMX y WCF. Ver Figura 5.3.

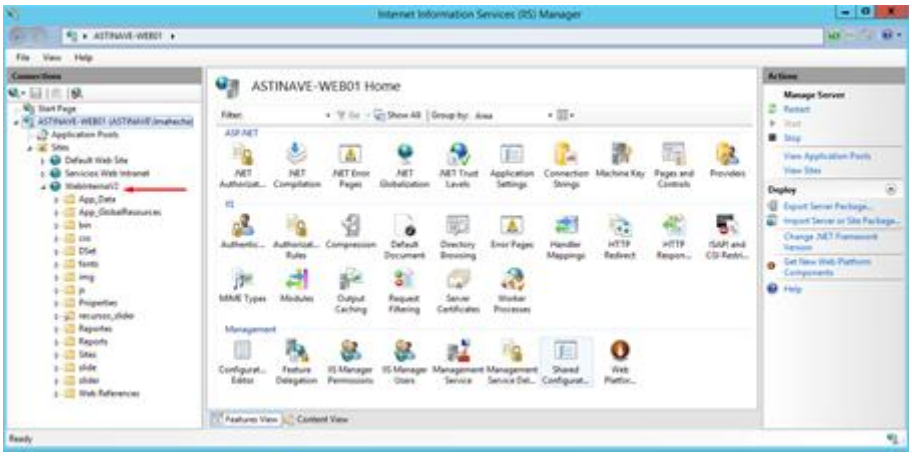


Figura 5.3 UI del Internet Information Services Manager.

A continuación se indican algunas de las ventajas más destacadas de IIS 8:

Aislamiento automático de aplicaciones.

1. Procesos de trabajo con identidad única y configuración en espacio aislado, lo que reduce aún más los riesgos de seguridad.

2. Componentes IIS integrados e incluso reemplazables fácilmente por módulos personalizados.

3. Almacenamiento en caché dinámico integrado y compresión mejorada para mejor performance del sitio web.

Para este servidor se establecieron las siguientes características en capacidad de disco y procesamiento como se muestra en la siguiente figura:

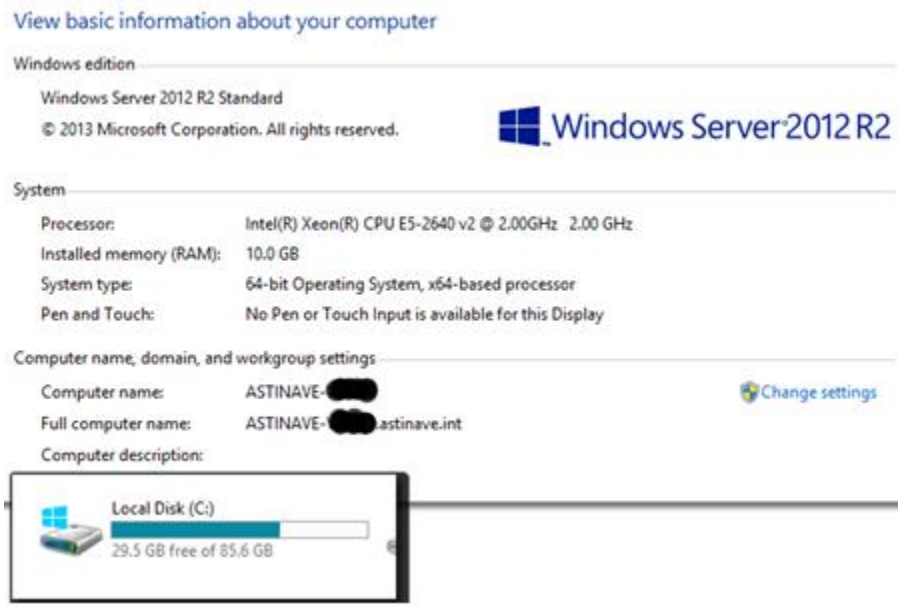


Figura 5.4 Características del Servidor Web.

Publicación del sitio

Tomando la solución desde el IDE utilizado para el desarrollo, el Visual Studio 2012, se publicará la aplicación web usando el método de despliegue Web Deploy, de esta forma se obtendrá como resultado un precompilado que se desplegará en el servidor IIS especificado una vez se sincronice con la versión local desde la cual se inicia la publicación. Para conseguir esta sincronización entre el servidor de desarrollo, por lo general el equipo del desarrollador, y el servidor web, este último debe

tener la misma versión de Web Deploy instalada que el equipo de desarrollo; para éste, esta característica quedó establecida cuando se instaló el Visual Studio. La secuencia del despliegue de la solución se aprecia desde la Figura 5.5 hasta Figura 5.9.

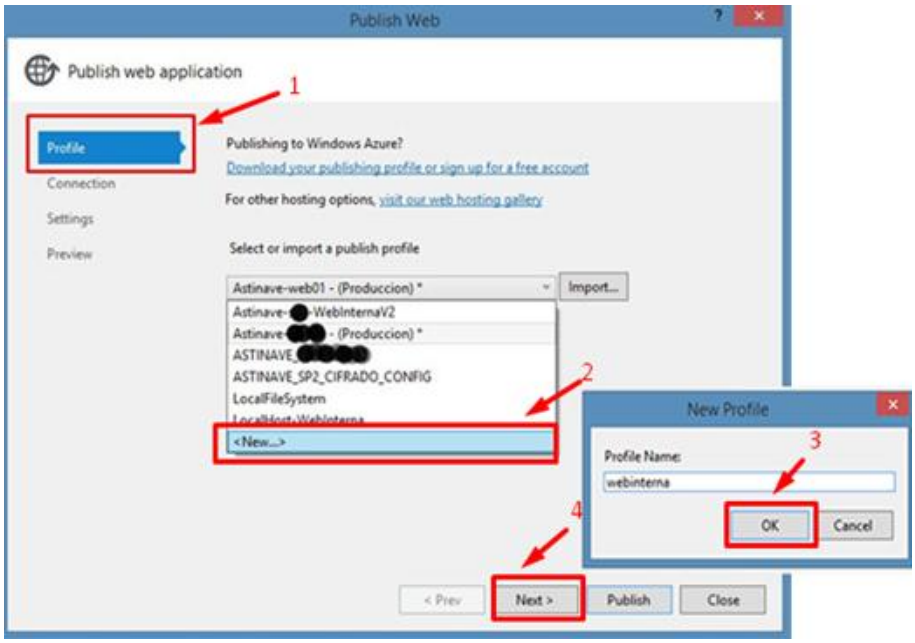


Figura 5.5 Publicación del Sitio: creación de un perfil para el despliegue.

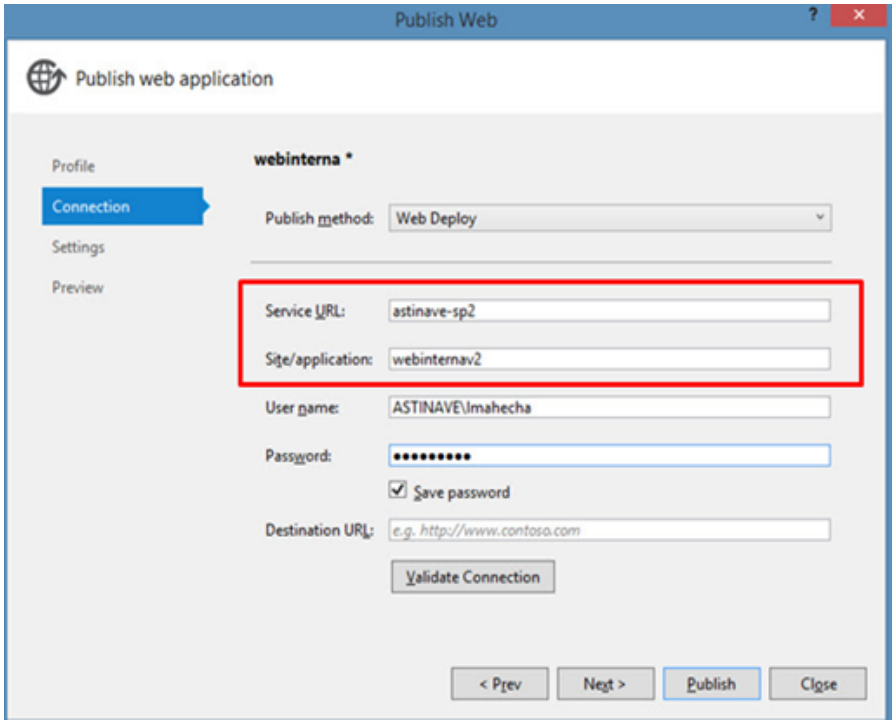


Figura 5.6 Publicación del Sitio: Definición de la ruta del despliegue.

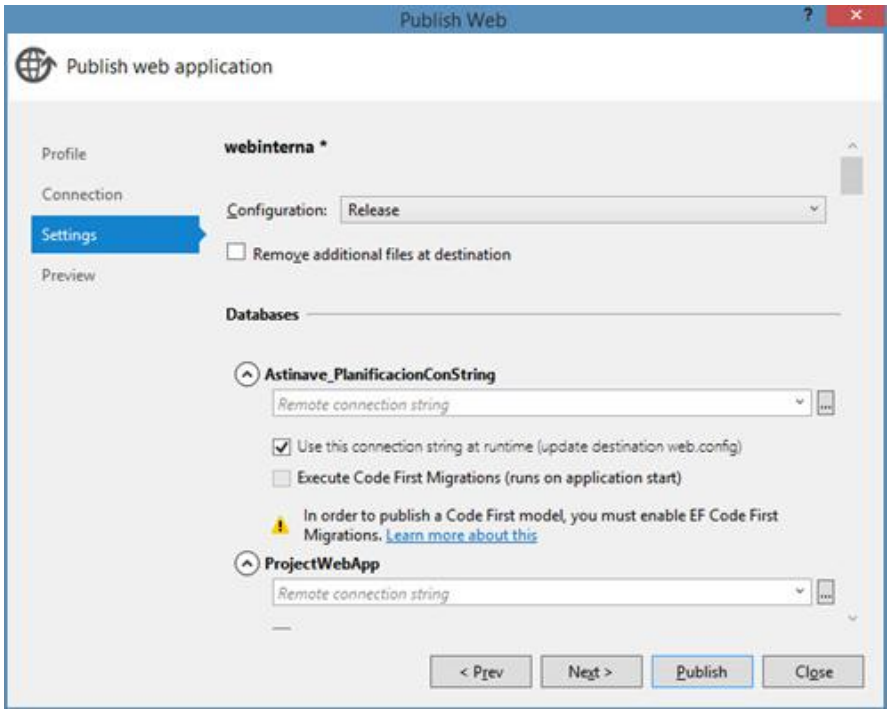


Figura 5.7 Publicación del Sitio: configuraciones.

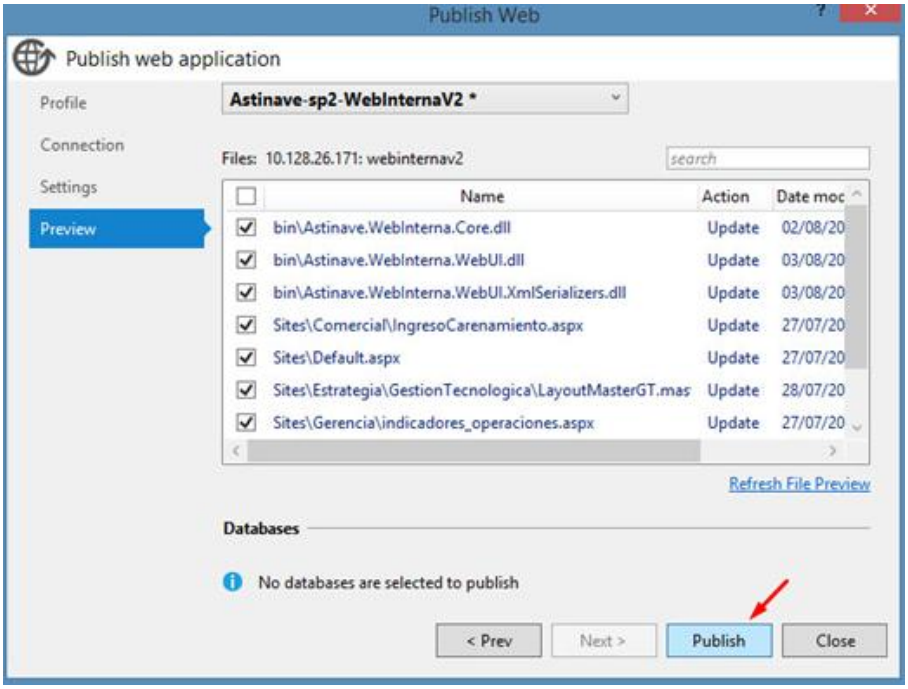


Figura 5.8 Publicación del Sitio: vista previa antes del despliegue.

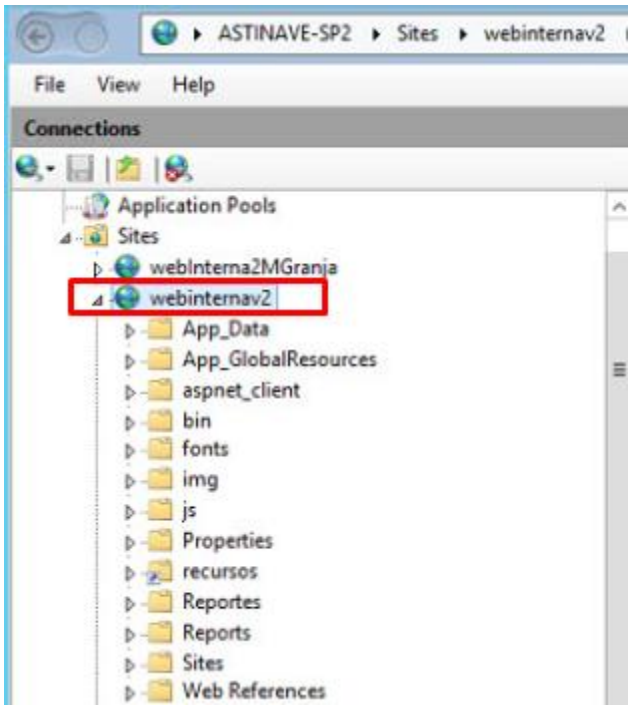


Figura 5.9 Publicación del Sitio: resultado de la publicación en el IIS.

5.1.2 Servidores de bases de datos

Para el servidor que aloja la base de datos de los módulos funcionales de toda la intranet, incluyendo los de la solución propuesta se manejaron los siguientes requerimientos de procesamiento y almacenamiento:

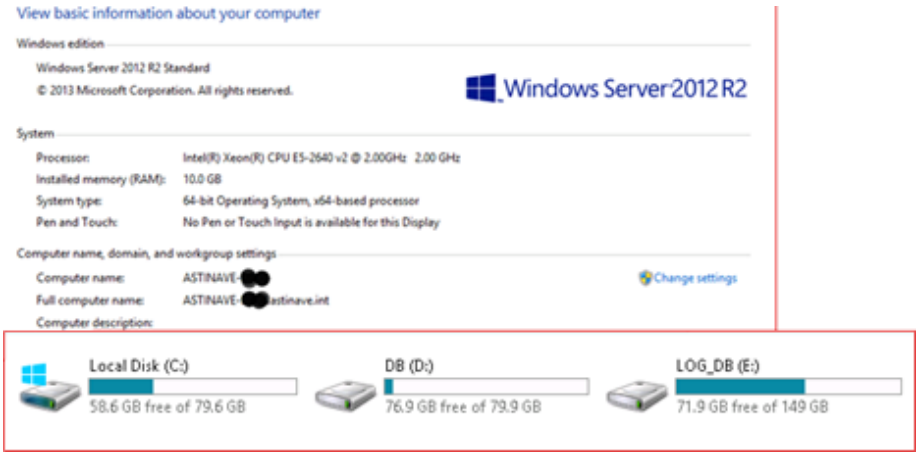


Figura 5.10 Propiedades del servidor de la base de datos.

En ASTINAVE EP se manejan algunas bases de datos, como se puede observar en la Figura 5.2, de las integraciones Involucradas con la aplicación se tiene la base de datos del ERP Dynamics GP 10.0 (SQL SERVER 2008 R2) y la base de datos de Sharepoint 2013 (SQL SERVER 2014); la base de la web interna de la cual forma parte la solución propuesta también es una SQL SERVER 2014. Así que como consideración importante en la puesta en producción se tuvo a la comunicación de estas bases de datos remotas para lo cual

fue necesario crear servidores vinculados haciendo uso de la característica de Linked Servers que proporciona el motor tal como se muestra en la Figura 5.11.

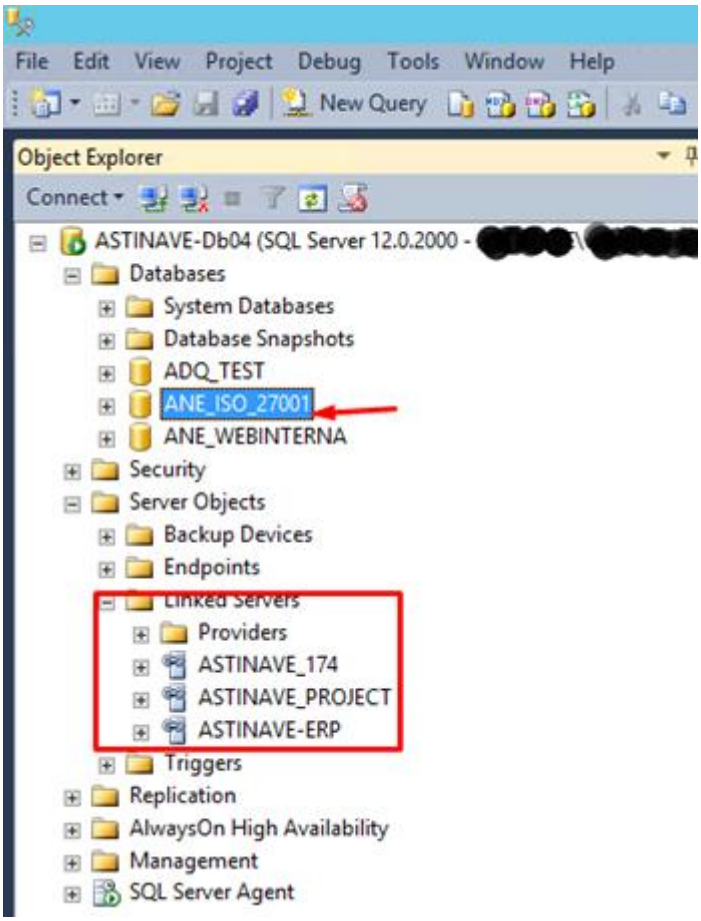


Figura 5.11 Servidores de bases de datos vinculados.

La parte inicial del código T-Sql que permite la vinculación de los servidores es:

```
EXEC master.dbo.sp_addlinkedserver @server = N'ASTINAVE-ERP',
@srvproduct=N'ERP', @provider=N'SQLNCLI', @datasrc=N'astinave-
erp'
```

```
EXEC master.dbo.sp_addlinkedsrvlogin @rmtsrvname=N'ASTINAVE-
ERP',@useself=N'False',@locallogin=NULL,@rmtuser=N'sa',@rmtpasswo
rd='########'
```

Una vez que 2 bases de datos remotas interactúan como servidores vinculados no se pueden gestionar transacciones (commit, rollback…), bloqueos o niveles de aislamiento de allí que fue muy importante en fase de desarrollo programar una buena gestión de excepciones desde la capa de datos en función de la integridad referencial entre las entidades del modelo.

Aparte de las tablas expuestas en el modelo de datos físico del capítulo 4, en la base también se implementaron:

1. 3 vistas
2. 39 Stored Procedures
3. 8 funciones escalares

5.1.3 Servidor de Reportes

SQL Server Reporting Services 2008 (SSRS) es una característica incluída en el motor desde la versión del 2008 que se utiliza para diseñar, desarrollar, probar e implementar informes. Para la creación y despliegue de los reportes se

apoya en la funcionalidad de SQL Server Data Tools (SSDT), la herramienta, que justo en la versión del 2014, se descarga por aparte y que permite continuar con los proyectos de Business Intelligence ejecutándose sobre Visual Studio 2010 Shell. Ver Figura 5.12.

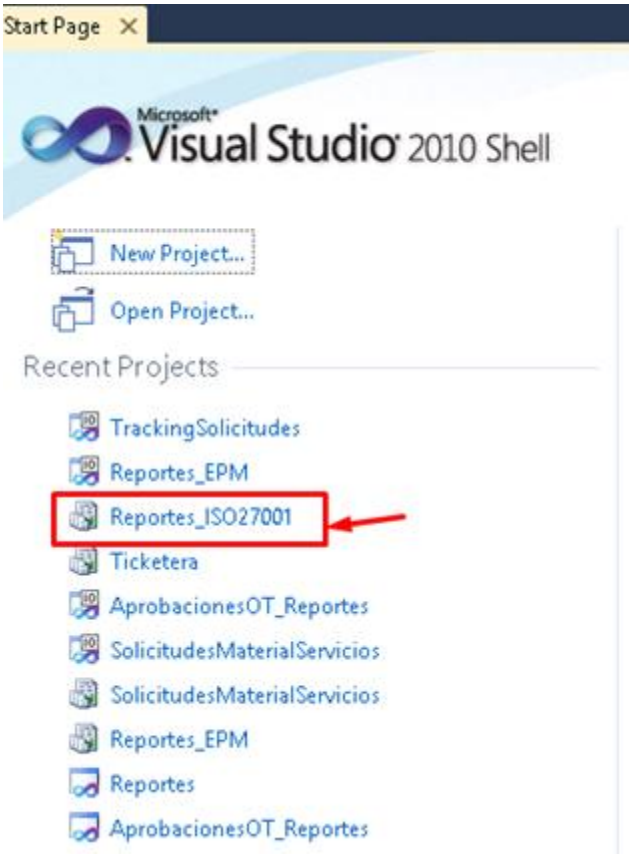


Figura 5.12 Vista Inicial de Visual Studio 2010 Shell para cargar el proyecto de SSDT.

Para esta puesta en producción se generó una solución en donde se definieron los datasources, datasets e informes (archivos .rdl). Ver Figura 5.13.

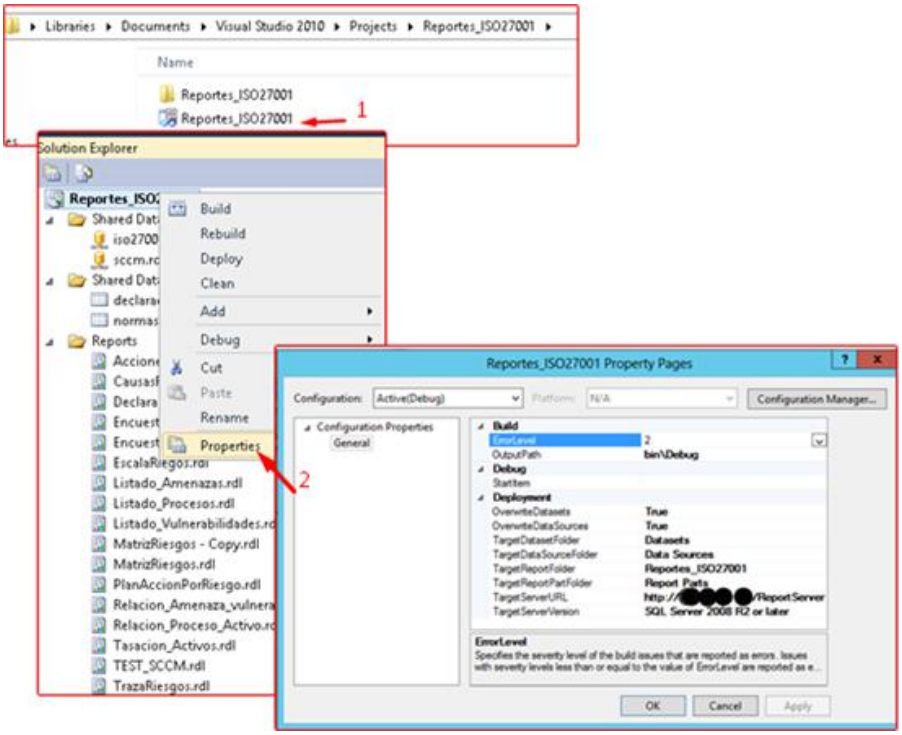


Figura 5.13 Solución en SSDT con los reportes del SGSI.

Para la configuración de la instancia del servidor de reportes en modo nativo, sea como local o remota, fue necesario hacer uso de Reporting Services Configuration Manager (RSCM). Algunas de las tareas que se realizan con esta herramienta son:

1. Configurar la cuenta de servicio del servidor Informe.

2. Crear y configurar las direcciones URL. El servidor de informes y el Administrador de informes son las aplicaciones ASP.NET que se accede a través de las direcciones URL.

3. Crear y configurar la base de datos del servidor de informes.

4. Administrar copias de seguridad, restaurar o reemplazar la clave simétrica que se utiliza para cifrar las cadenas de conexión y credenciales almacenadas.

5. Configurar la cuenta de ejecución desatendida. Esta cuenta se utiliza para las conexiones remotas durante las operaciones programadas o cuando las credenciales de usuario no están disponibles

6. Configurar servidor de informes por correo electrónico. SSRS utiliza un protocolo simple de transferencia de correo (SMTP) para entregar informes a buzones de emails.

En la Figura 5.14 se aprecia la vista del RSCM.

Figura 5.14 Opciones del Reporting Services Configuration Manager.

Una vez se configuran los parámetros deseados en el servidor de reportes, el IIS correspondiente despliega el sitio ‘Reports’ en donde se publicarán los reportes creados previamente con SSDT. Estos mismos reportes luego serán consumidos desde la aplicación web que se ejecuta en el servidor web cuyo despliegue se explicó en la sección 5.1. Ver Figura 5.15.

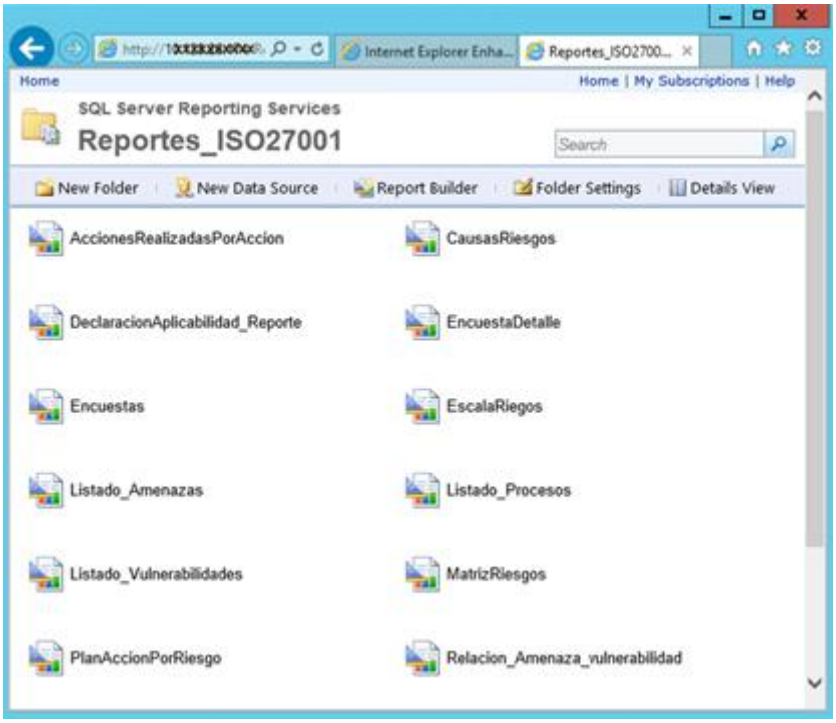


Figura 5.15 Vista de los reportes publicados en el sitio ‘Reports’ del SSRS.

5.2 Pruebas de Aplicación y Uso de la Herramienta: Gestión de Controles de la Norma.

A continuación las pruebas correspondientes al módulo funcional de Gestión de Controles de la Norma de la solución propuesta. Todas las funcionalidades descritas a continuación se encuentran en la opción 'Controles' de la página inicial del aplicativo.

Figura 5.16 Opción 'Controles'.

5.2.1 Declaración de Aplicabilidad

El mantenimiento de los controles permite marcarlos para indicar que serán considerados en la declaración de aplicabilidad, indicando la justificación de los mismos, los controles pueden ser buscados por dominios y subdominios. En la siguiente secuencia figuras se aprecia esta funcionalidad.

Figura 5.17 Búsqueda de controles.

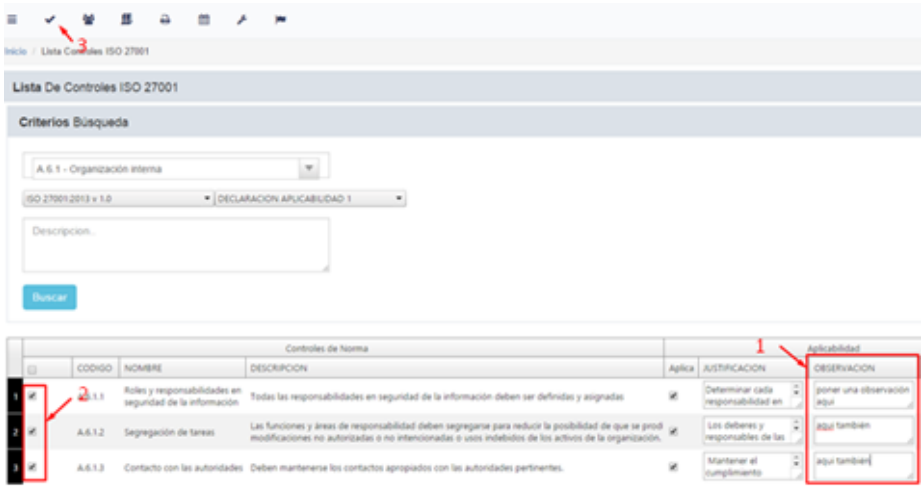


Figura 5.18 Lista de controles de las norma ISO 27001:2013.

5.2.2 Consulta de Responsables asignados

En esta opción los controles pueden ser puestos bajo el control de uno o más revisores de control, éstos son buscados en la base de colaboradores activos de la organización. La Figura 5.19 da evidencia de cómo se procede a la búsqueda, se asigna o desasigna un responsable.

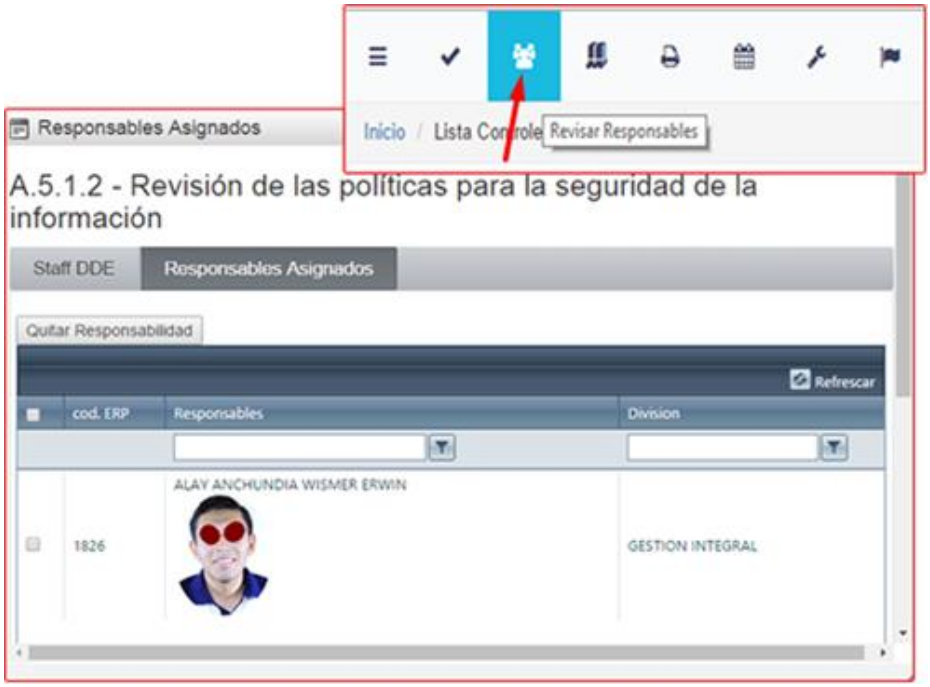


Figura 5.19 Vista de búsqueda y asignación de responsables para seguimiento de controles.

5.2.3 Consulta de documentos asignados

La opción consiste en seleccionar uno o más controles y asociarlos con uno o más documentos de aquellos que son

gestionados en la biblioteca del Sistema Integrado de Gestión del Sharepoint. Ver Figura 5.20.

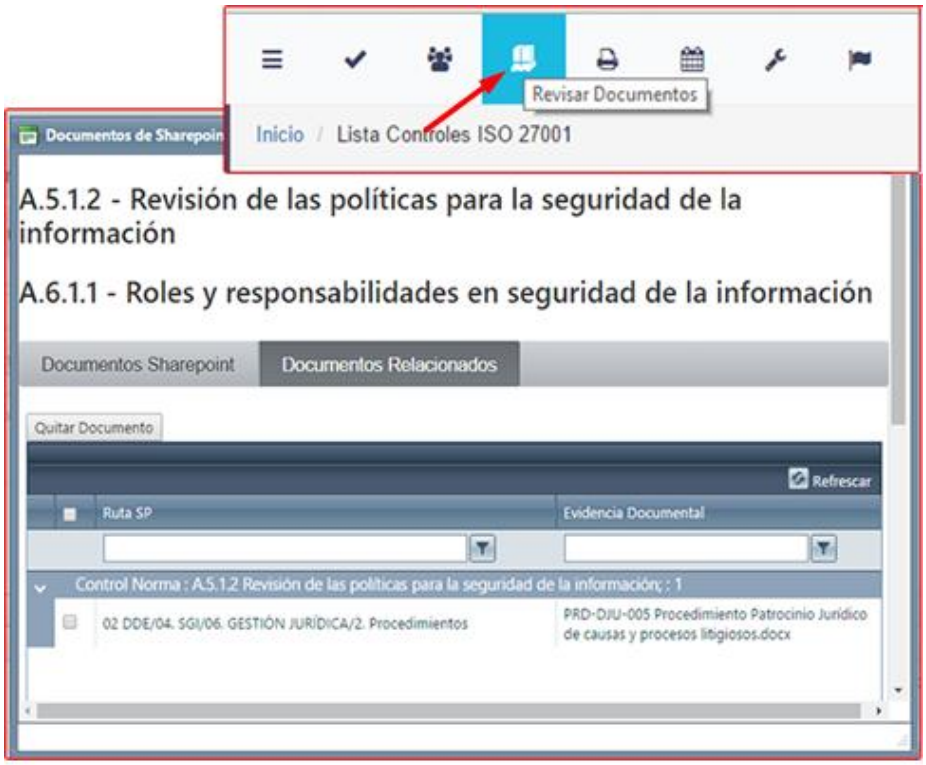


Figura 5.20 Vista de búsqueda y asignación de documentos.

5.2.4 Consulta de seguimiento por control

Si de controlar se trata, la opción de seguimiento permite ver el conjunto de riesgos registrados, los cuales haciendo drill down muestran los planes de acciones y sus respectivas acciones realizadas y registradas por los ejecutores asignados. Ver Figura 5.21.

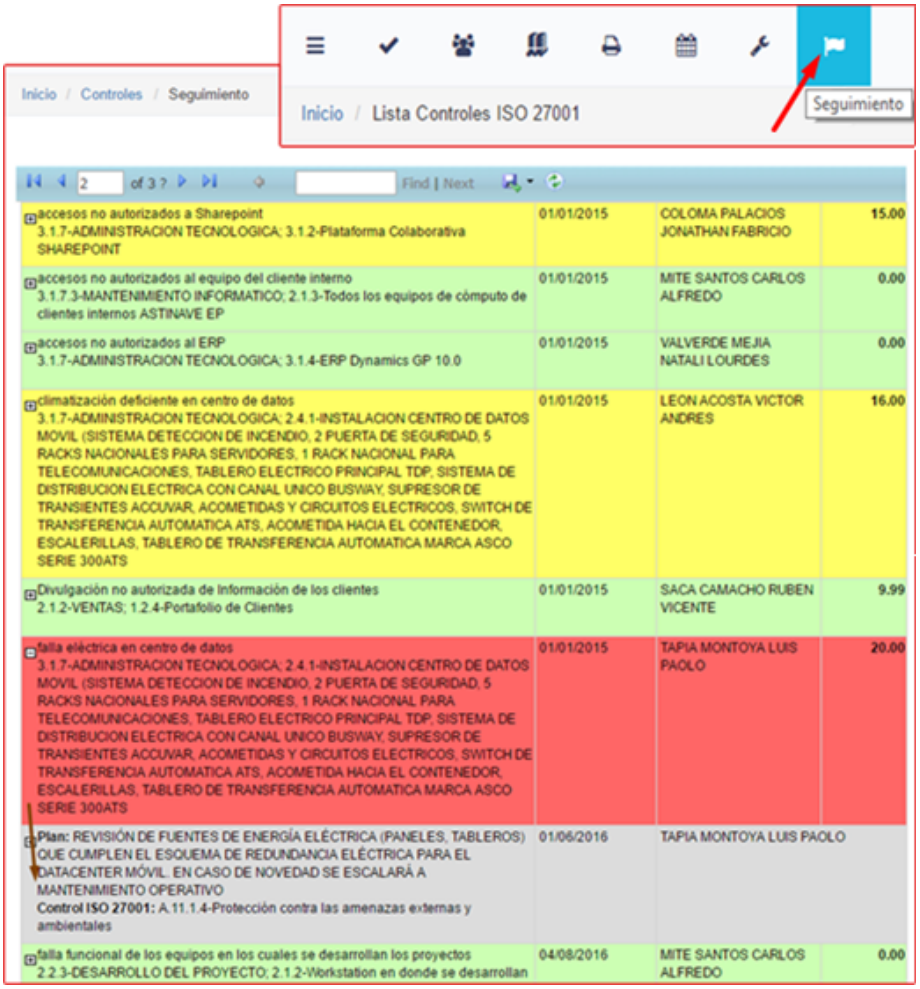


Figura 5.21 Reporte de seguimiento riesgo-plan-acción.

5.2.5 Consulta de Línea de Tiempo por Control

Se selecciona un control del Anexo A y en la opción de ver línea de tiempo se pueden verificar los riesgos asociados, por cada riesgo se puede ver la línea de tiempo respectiva, en esta línea de tiempo se muestran cuándo se registró el riego, a quién se asignó, las acciones propuestas para el tratamiento y las acciones realizadas. Ver la Figura 5.22.

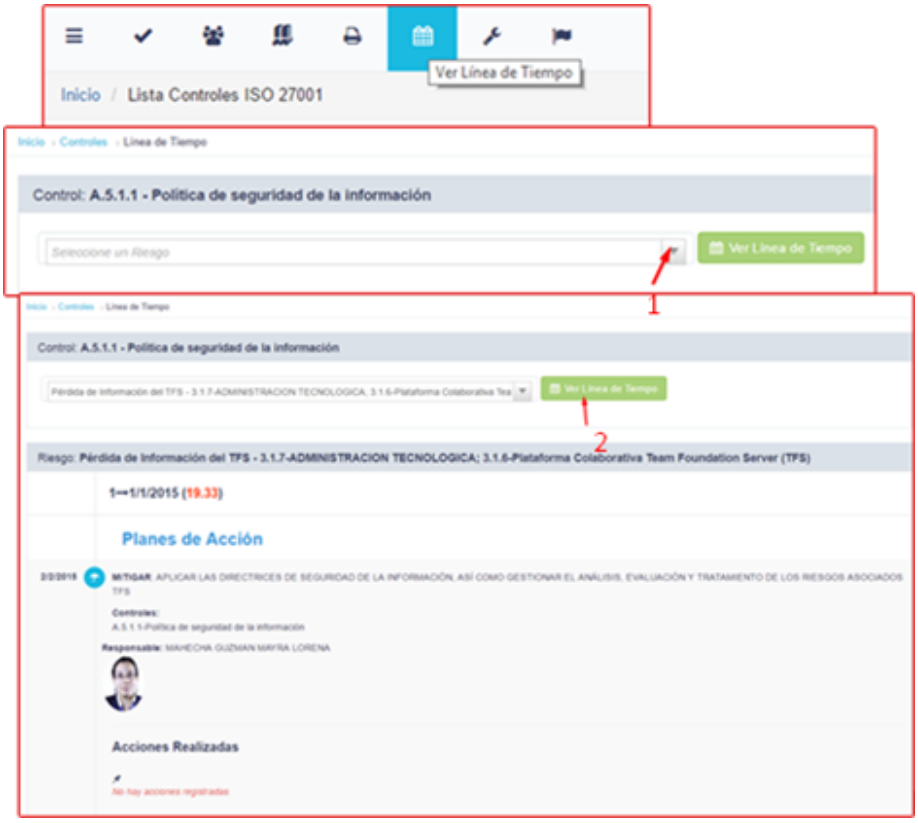


Figura 5.22 Consulta de línea de tiempo por control.

5.2.6 Registro de acciones realizadas dentro de los planes de tratamiento

Para aquellos que fueron asignados como ejecutores de las acciones planeadas para el tratamiento de los riesgos, esta opción les permite registrar lo realizado, poniendo fecha y estado. Ver Figura 5.23.

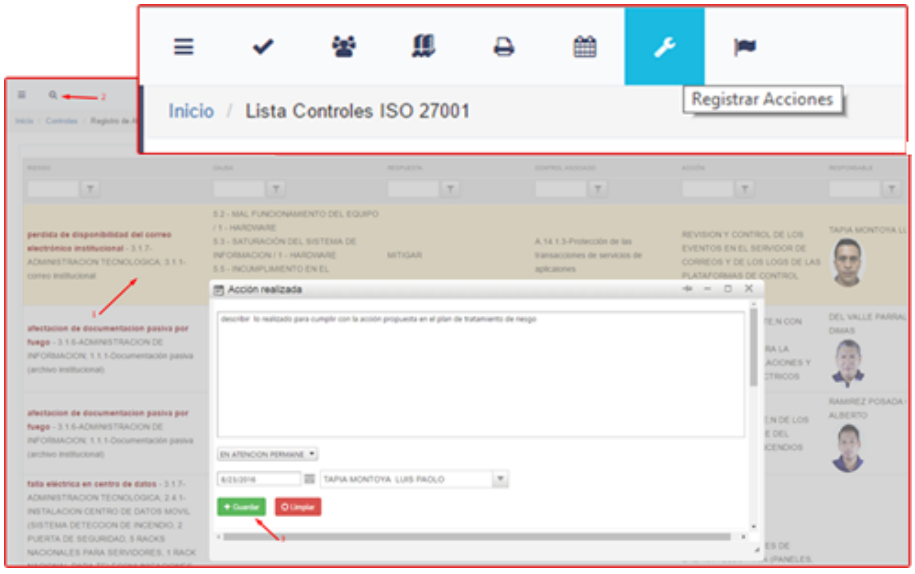


Figura 5.23 Registro de acciones realizadas según el plan de acciones propuesto.

5.3 Gestión de Activos de Información

A continuación las pruebas correspondientes al módulo funcional de Gestión de Activos de Información de la solución propuesta. Todas las funcionalidades descritas a continuación se encuentran distribuídas en la opción ‘Activos Información’ y la opción ‘Procesos’ de la página inicial del aplicativo.

Figura 5.24 opciones ‘Activos Información’ y ‘Procesos’.

5.3.1 Registro y Mantenimiento de Procesos Empresariales

En esta opción se permite el registro y mantenimiento de macro procesos – procesos - subprocesos en un árbol de jerarquías para los procesos empresariales.

Los procesos se muestran en un árbol desde el cual podrán insertarse nuevos procesos y editar los ya existentes, además de consultar el reporte de los procesos, ver Figura 5.25, Figura 5.26 y Figura 5.27 respectivamente.

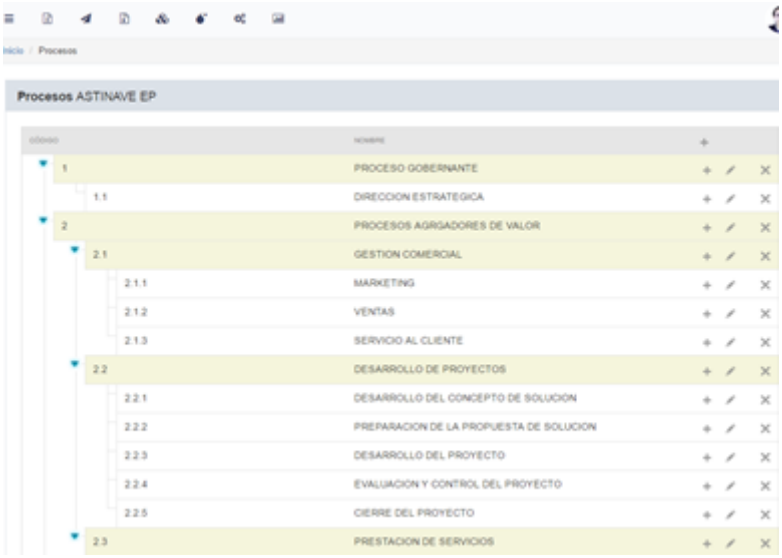


Figura 5.25 Árbol de procesos de la organización.

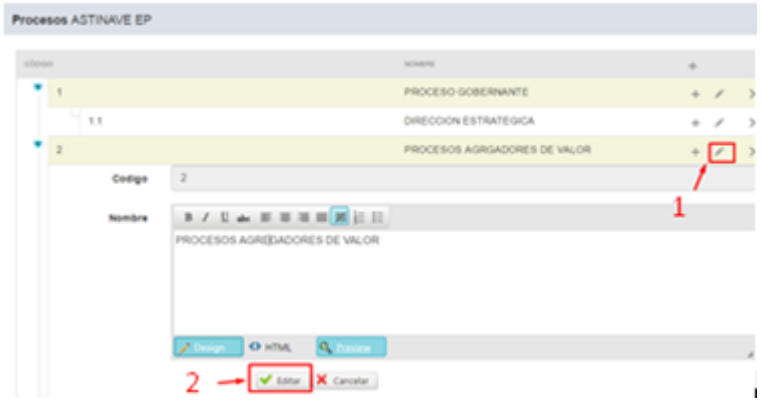


Figura 5.26 Edición de procesos.

Código	Nombre
1	PROCESO GOBERNANTE
1.1	DIRECCION ESTRATEGICA
2	PROCESOS AGREGADORES DE VALOR
2.1	GESTION COMERCIAL
2.1.1	MARKETING
2.1.2	VENTAS
2.1.3	SERVICIO AL CLIENTE
2.2	DESARROLLO DE PROYECTOS
2.2.1	DESARROLLO DEL CONCEPTO DE SOLUCION
2.2.2	PREPARACION DE LA PROPUESTA DE SOLUCION
2.2.3	DESARROLLO DEL PROYECTO
2.2.4	EVALUACION Y CONTROL DEL PROYECTO
2.2.5	CIERRE DEL PROYECTO
2.3	PRESTACION DE SERVICIOS
2.3.1	INICIO-PLANIFICACION
2.3.2	EJECUCION CARANAMIENTO
2.3.3	EJECUCION MANTENIMIENTO INDUSTRIAL
2.3.4	MONITOREO-CONTROL Y CIERRE

Figura 5.27 Reporte de Procesos.

5.3.2 Registro y Mantenimiento de Activos

La aplicación brinda un clasificador general de activos, lo que permitirá que los activos de información que se vayan registrando se clasifiquen de acuerdo a una lógica unificada. En la Figura 5.28 se muestra el árbol del clasificador y la Figura 5.29 se aprecia el desglose correspondiente.

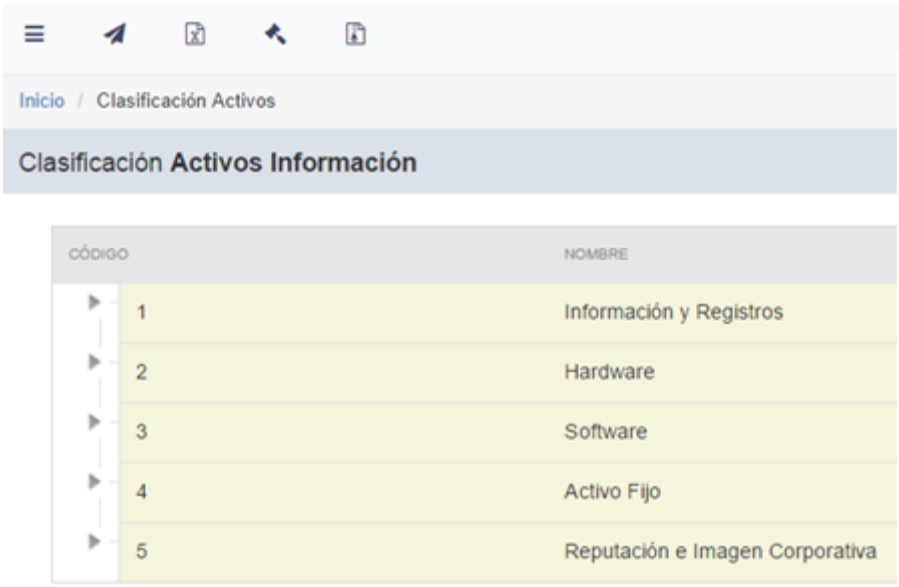


Figura 5.28 Vista del clasificador general de los activos de información.

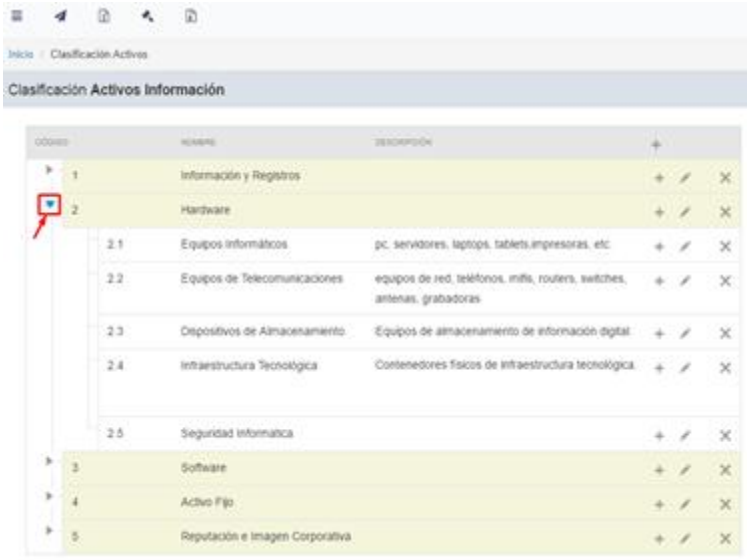


Figura 5.29 Vista del despliegue de un tipo de activo en el clasificador general de los activos de información.

Cuando se va a proceder al registro de un activo se selecciona la categoría deseada en el clasificador y se da click en la opción ‘Revisar Activos Info’ tal como se aprecia en la Figura 5.30.

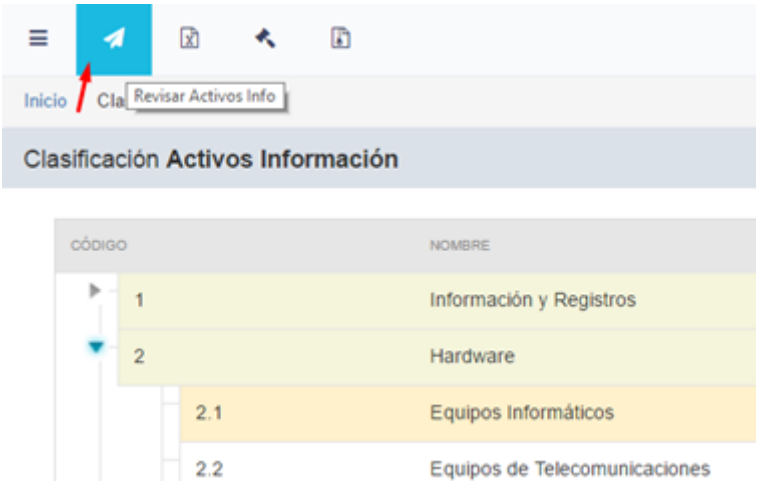


Figura 5.30 Opción para el registro y mantenimiento de los activos.

Lo siguiente que se ve son los activos que ya se han registrado para esa categoría, ver Figura 5.31, de igual forma se pueden ver los botones para referenciar bienes controlados por activo fijo y para escribir directamente el activo de información. Asimismo está el combo box que permite seleccionar uno o más procesos.

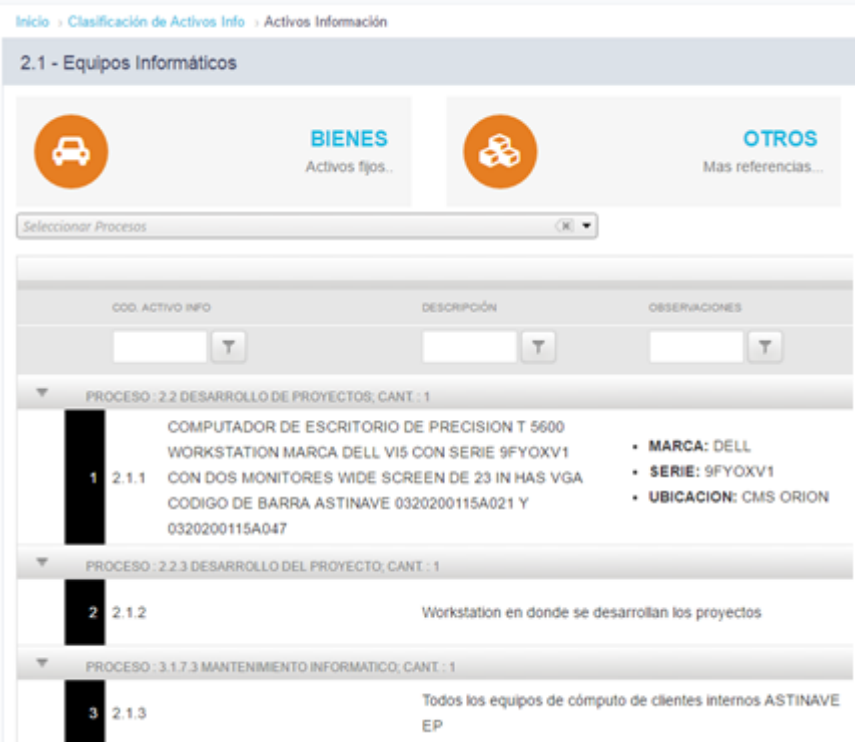


Figura 5.31 Vista del clasificador general de los activos de información.

Una vez que se despliega el combo box se muestra la jerarquía de los procesos permitiendo chequear más de uno para indicar que los activos a guardarse estarán asociados a dichos procesos. Así se lo aprecia en la siguiente figura.

Figura 5.32 Selección del proceso empresarial durante el registro de un bien.

Como el ejemplo se trata de registrar un activo de información categorizado dentro de ‘Equipos Informáticos’, el sistema ya tiene predeterminado que el usuario o lo escribirá directamente o lo buscará en la base de activos fijos. En la Figura 5.33 se muestra una búsqueda de bienes administrados. Una vez que se seleccionen uno o varios activos y se dé click en ‘agregar’ ya estarán registrados en el catálogo unificado de activos. Se podrá cambiar el propietario y asignar la fecha de control.

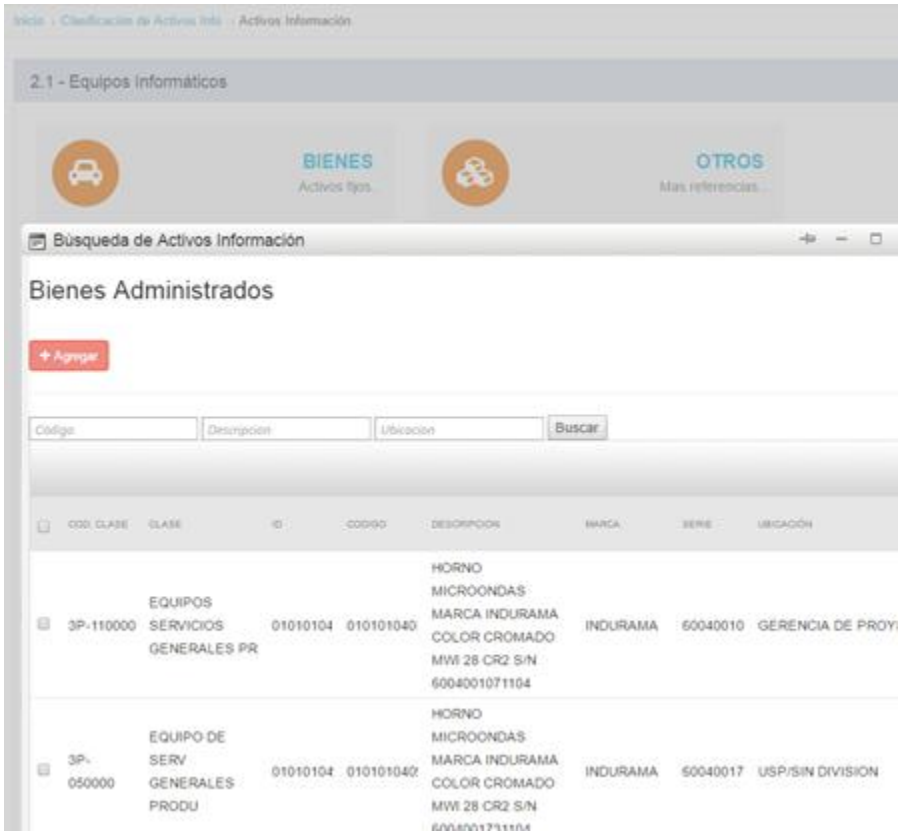


Figura 5.33 Búsqueda de activos fijos y otros bienes administrados.

En todo momento se puede descargar el catálogo de activos, el reporte que se puede ver en la Figura 5.34, siempre mostrará los activos asociados a los procesos correspondientes que se hayan elegido al momento del registro.

Figura 5.34 Reporte del catálogo de activos.

5.3.3 Asociación de Activos de Información

Desde el árbol de procesos también pueden registrarse los activos, por ejemplo en la Figura 5.35 se muestra como se selecciona un proceso.

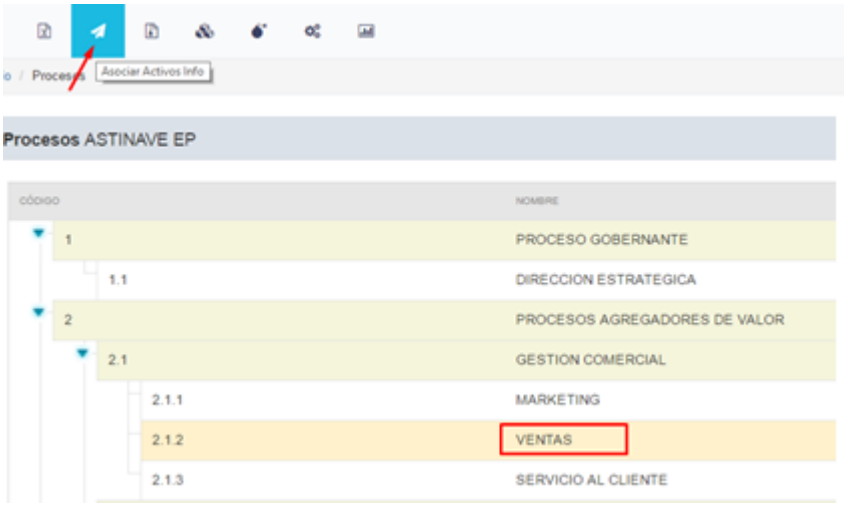


Figura 5.35 Selección de un proceso para la asociación de activos.

Una vez que se da click en la opción 'Asociar Activos Info' se verá el listado de activos de información previamente asociados, ver Figura 5.36.

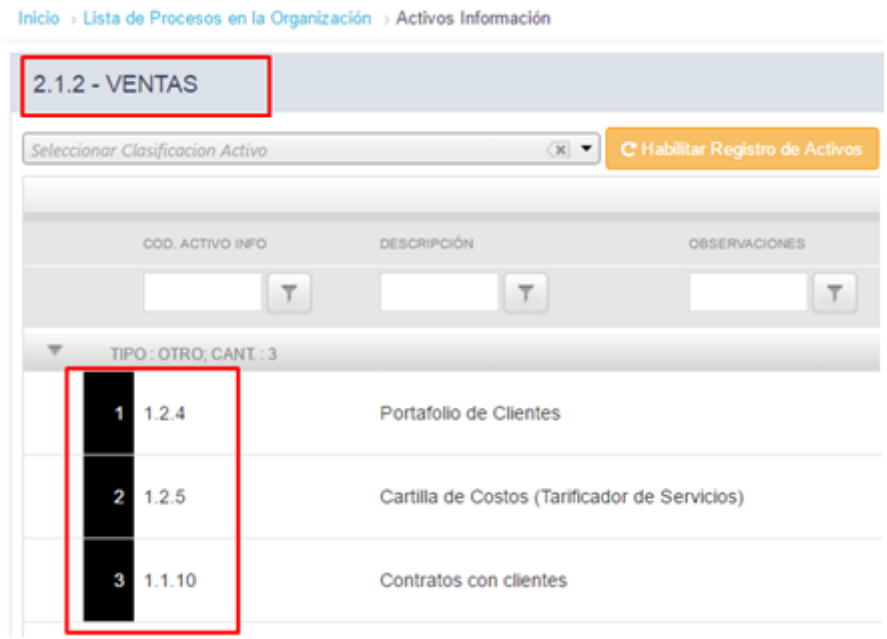


Figura 5.36 Vista de activos asociados a un proceso.

En la lista desplegable, que se puede apreciar en la Figura 5.37, se muestra el árbol de la clasificación de los activos, se puede seleccionar más de uno, dando click en ‘Registrar registros de activos’ se activarán las opciones de registros disponibles.

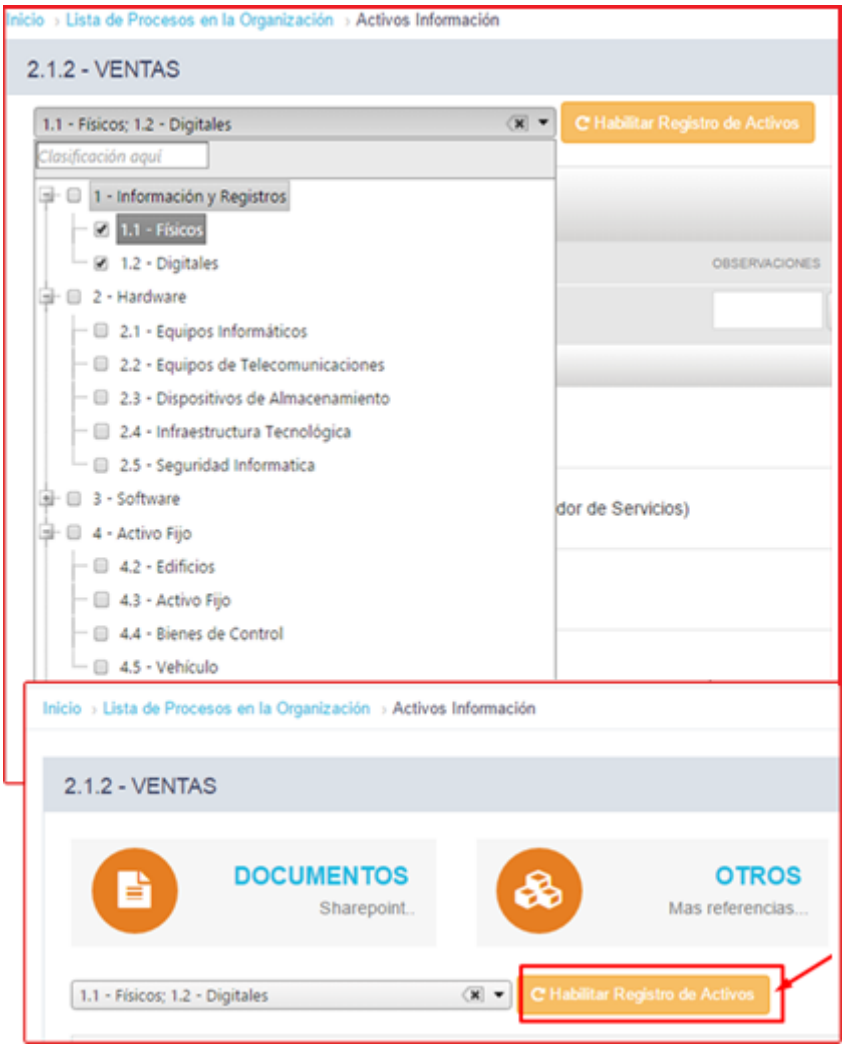


Figura 5.37 Selección del tipo de activos para poder asociar activos a un proceso.

Para el caso del ejemplo, con la opción ‘otros’ se escribe de manera sencilla el activo que se quiere asociar, mientras que

con la opción ‘documentos’ se traen referencias de documentos registrados previamente en Sharepoint. Ver la Figura 5.38 y la Figura 5.39 respectivamente.

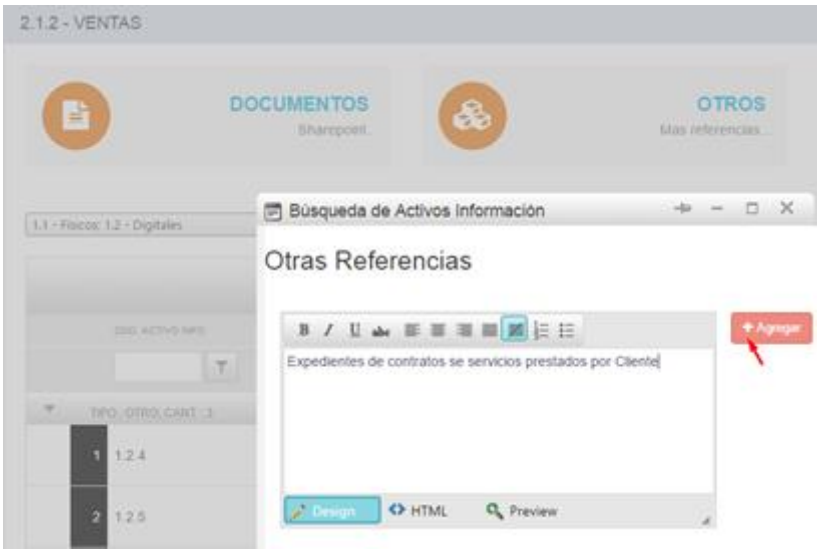


Figura 5.38 Registro de un activo de forma general .

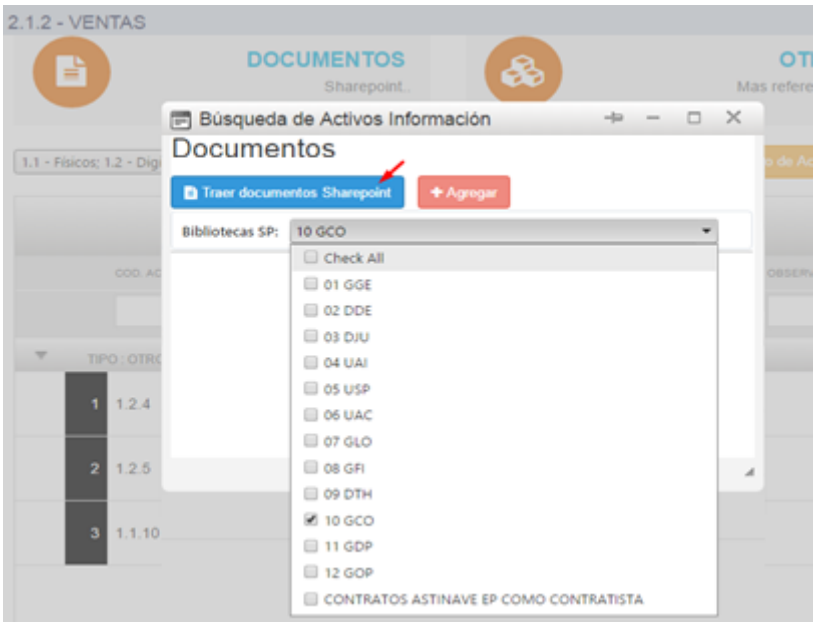


Figura 5.39 Registro de un activo de información documental .

El sistema también permitirá que la asociación de activos ocurra de manera masiva, es decir se pueden seleccionar varios procesos y asociarles varios activos del catálogo a la vez como se muestra en la siguiente figura.

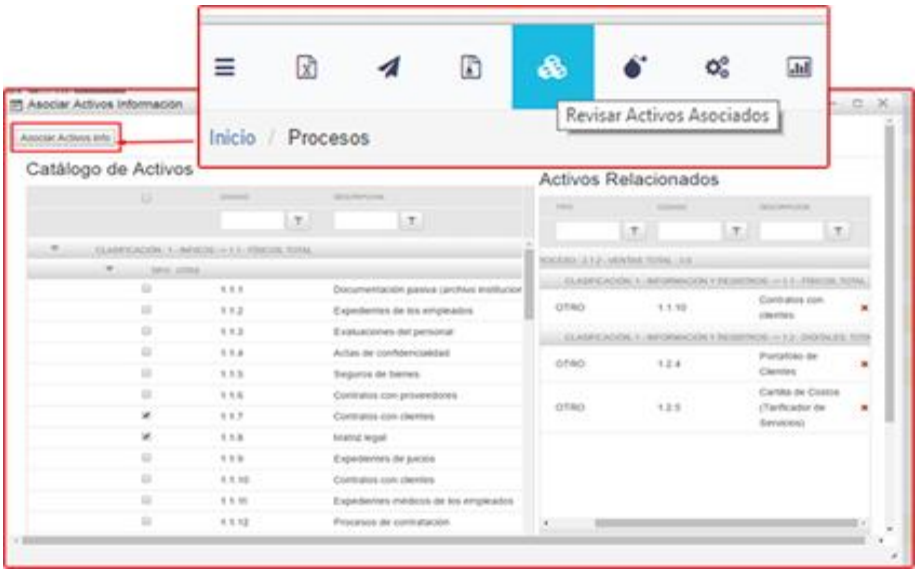


Figura 5.40 Vista de los activos asociados a un proceso.

Desde la opción de procesos también estará disponible la descarga del catálogo de activos en donde se aprecian los activos por procesos como se ve en la siguiente figura.

2.1.2 - VENTAS	
1.1 - FÍSICOS	
1.1.10 - Contratos con clientes	490 - SACA CAMACHO RUBEN VICENTE
1.2 - DIGITALES	
1.2.4 - Portafolio de Clientes	490 - SACA CAMACHO RUBEN VICENTE
1.2.5 - Cartilla de Costos (Tarificador de Servicios)	263 - JAMA AVEIGA HUGO JOSÉ
2.2 - DESARROLLO DE PROYECTOS	
2.1 - EQUIPOS INFORMÁTICOS	
2.1.1 - COMPUTADOR DE ESCRITORIO DE PRECISION T 5600 WORKSTATION MARCAI	340 - MITE VARGAS LEOPOLDO EFREN
2.2.1 - DESARROLLO DEL CONCEPTO DE SOLUCION	
1.2 - DIGITALES	
1.2.20 - Información de Proyectos	
2.2.2 - PREPARACION DE LA PROPUESTA DE SOLUCION	
1.2 - DIGITALES	
1.2.19 - Información de Propuestas	
2.2.3 - DESARROLLO DEL PROYECTO	
1.2 - DIGITALES	
1.2.20 - Información de Proyectos	
2.1 - EQUIPOS INFORMÁTICOS	
2.1.2 - Workstation en donde se desarrollan los proyectos	
3.1 - PROPIETARIO	
3.1.7 - Plataforma Colaborativa Team Foundation Server (TFS)	
3.1.8 - Plataforma Colaborativa Rational	
3.1.9 - Plataforma Colaborativa PLM	

Figura 5.41 Reporte de activos de información asociados a los procesos.

5.3.4 Generación de encuestas y votación para la valoración de los activos.

Una opción que se consideró importante y novedosa incluir, es la de registrar encuestas por proceso para que los dueños de tales procesos y los propietarios de los activos asociados a ese proceso puedan indicar la valoración del impacto de los activos en función de la confidencialidad, disponibilidad e integridad. En la Figura 5.42. se aprecia que en la encuesta ya viene incluído el listado de activos registrados en ese proceso, permitiendo

incluso al usuario que registra la encuesta que descarte algunos, se debe escribir una breve descripción de la encuesta, definiendo el lapso en que estará disponible la encuesta y, obviamente, a quienes les estará permitido responder a la encuesta. Ver Figura 5.42 y Figura 5.43.

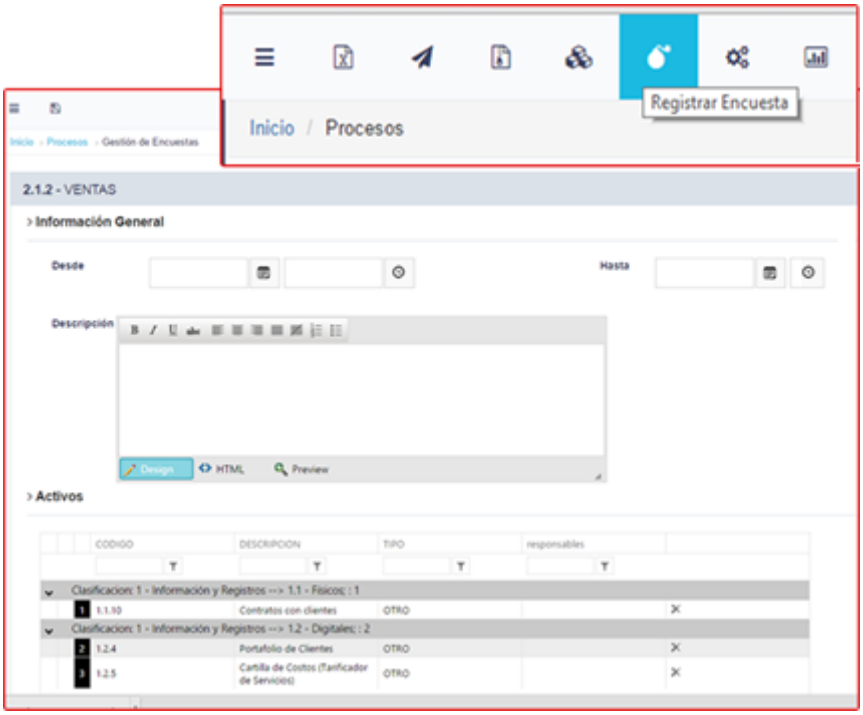


Figura 5.42 Registro de la encuesta .

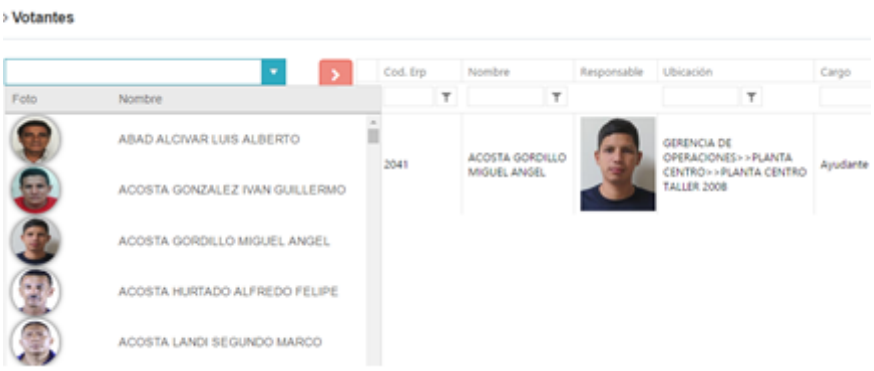


Figura 5.43 Registro de los encuestados/votantes.

Una vez que los encuestados ingresen verán las encuestas que tienen asignadas, ver Figura 5.44, y si no está cerrada podrá ingresar a responderlas.

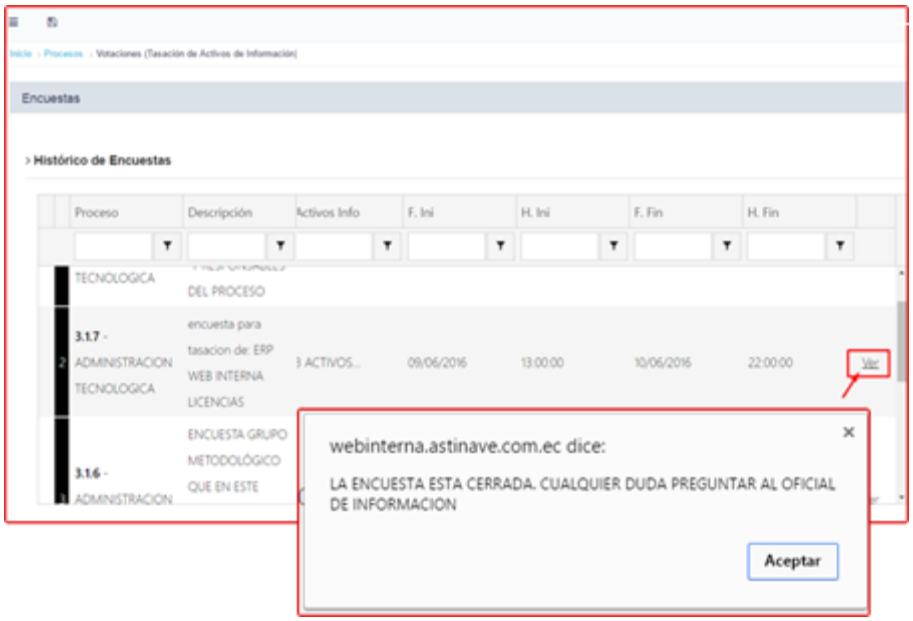


Figura 5.44 Vista de las encuestas por los votantes.

Mientras realiza la votación el encuestado tendrá visible la escala de impactos preestablecida en el sistema; abajo estará el listado de activos a los cuales les dará una valoración en

función de la escala indicada para los criterios de Confidencialidad (C), Disponibilidad (D), Integridad(I). Estas particularidades se aprecian en la siguiente figura.

Figura 5.45 Vista de la votación de una encuesta.

Una vez que las encuestas de todos los procesos hayan sido respondidas, el responsable de seguridad de la información, podrá hacer uso de la opción ‘procesar encuestas’ que consolidará todas las encuestas para cada uno de los activos permitiendo de manera optativa que los cambios en el Impacto afecten el historial de riesgos. Ver Figura 5.46.

Figura 5.46 Procesamiento de las encuestas.

En todo momento se podrá transparentar lo que los encuestados valoraron en la encuestas, será suficiente dar click en la opción 'Ver Reportes de Votaciones' para tener un reporte con desglose hasta llegar a lo cada encuestado respondió. Ver Figura 5.47.

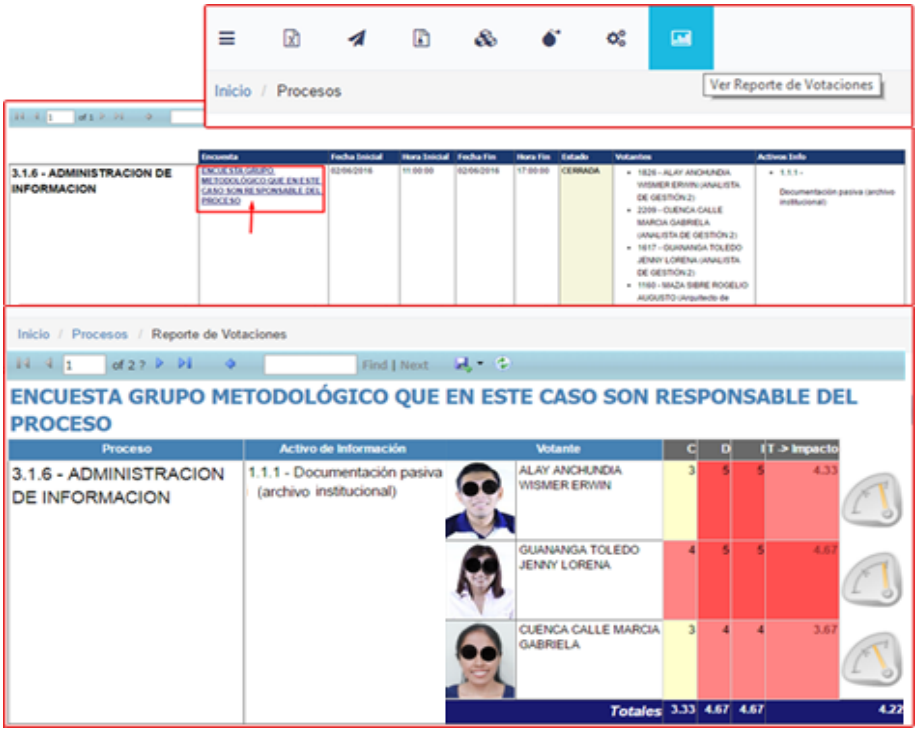


Figura 5.47 Reporte de encuestas y sus respectivas votaciones.

5.3.5 Tasación de activos

Aunque el mecanismo de las encuestas y su procesamiento son la primera alternativa de obtener la tasación de los activos, el sistema también da una segunda alternativa en la cual el criterio del responsable de seguridad de la información es el preponderante así que le permite que de valoraciones de impacto directamente. En la opción ‘Activos de Información’ - ‘Tasación’ tendrá una ventana en donde aparecerán todos los activos del catálogo. Ver la Figura 5.48 y la Figura 5.49.

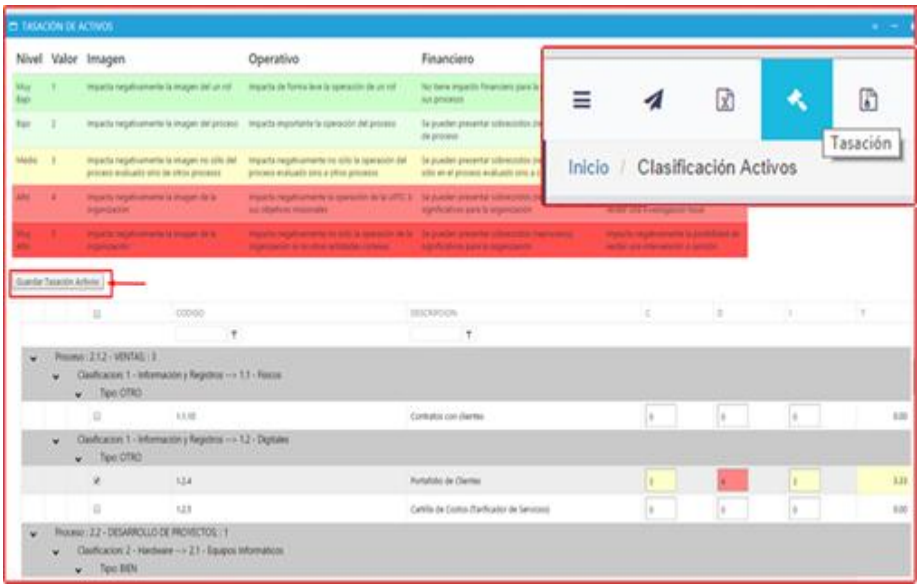


Figura 5.48 Vista de la tasación directa para los activos.

Figura 5.49 Vista de la escala de impacto para los activos.

Por cualquiera de las 2 alternativas se conseguirá tener siempre disponible el reporte de tasación de activos tal como se muestra en la siguiente figura.

Impacto	Valor
Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5

Código	Descripción	C	D	I	T
2.1.2 - VENTAS		1,00	1,33	1,00	1,11
1 - Información y Registros --> 1.1 - Físicos		0,00	0,00	0,00	0,00
OTRO		0,00	0,00	0,00	0,00
1.1.10	Contratos con clientes	0,00	0,00	0,00	0,00
1 - Información y Registros --> 1.2 - Digitales		1,50	2,00	1,50	1,67
OTRO		1,50	2,00	1,50	1,67
1.2.4	Portafolio de Clientes	3,00	4,00	3,00	3,33
1.2.5	Cartilla de Costos (Tarificador de Servicios)	0,00	0,00	0,00	0,00
2.2 - DESARROLLO DE PROYECTOS		0,00	0,00	0,00	0,00
2 - Hardware --> 2.1 - Equipos Informáticos		0,00	0,00	0,00	0,00
BIEN		0,00	0,00	0,00	0,00
2.1.1	COMPUTADOR DE ESCRITORIO DE PRECISION	0,00	0,00	0,00	0,00
2.2.1 - DESARROLLO DEL CONCEPTO DE SOLUCION		0,00	0,00	0,00	0,00
1 - Información y Registros --> 1.2 - Digitales		0,00	0,00	0,00	0,00
OTRO		0,00	0,00	0,00	0,00
1.2.20	Información de Proyectos	0,00	0,00	0,00	0,00
2.2.2 - PREPARACION DE LA PROPUESTA DE SOLUCION		0,00	0,00	0,00	0,00
1 - Información y Registros --> 1.2 - Digitales		0,00	0,00	0,00	0,00
OTRO		0,00	0,00	0,00	0,00
1.2.19	Información de Propuestas	0,00	0,00	0,00	0,00
2.2.3 - DESARROLLO DEL PROYECTO		0,00	0,00	0,00	0,00
1 - Información y Registros --> 1.2 - Digitales		0,00	0,00	0,00	0,00
OTRO		0,00	0,00	0,00	0,00
1.2.20	Información de Proyectos	0,00	0,00	0,00	0,00

Figura 5.50 Reporte de la tasación de activos de Información.

5.4 Gestión de Riesgos

A continuación las pruebas correspondientes al módulo funcional de Gestión de Riesgos la solución propuesta. Todas las funcionalidades descritas a continuación se encuentran distribuídas en las opciones de ‘Amenazas’, ‘Vulnerabilidades’ y ‘Riesgos’ de la página inicial del aplicativo, como se muestra en la siguiente figura.

Figura 5.51 Opciones de 'Amenazas', 'Vulnerabilidades' y 'Riesgos'.

5.4.1 Registro y mantenimiento de vulnerabilidades

El sistema implementa la metodología de la ISO 27005 para la gestión de riesgos, así que la clasificación de vulnerabilidades se toma del Anexo D de esta norma siguiendo el formato de tener un árbol en donde se pueden registrar nuevas vulnerabilidades o editar las existentes. Ver la Figura 5.52 y la Figura 5.53.

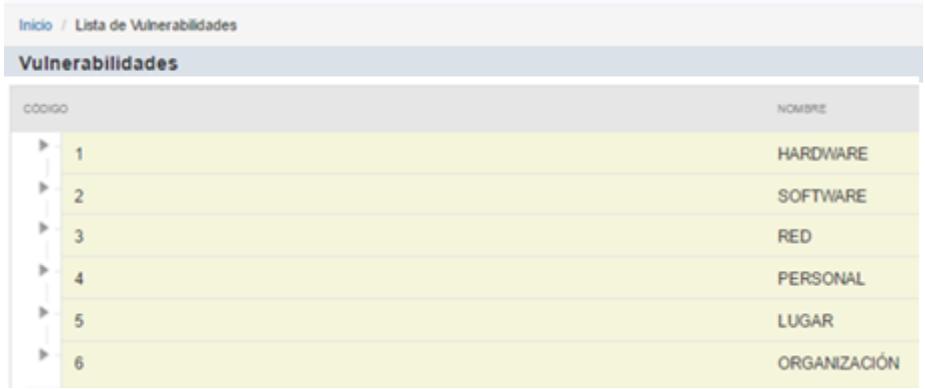
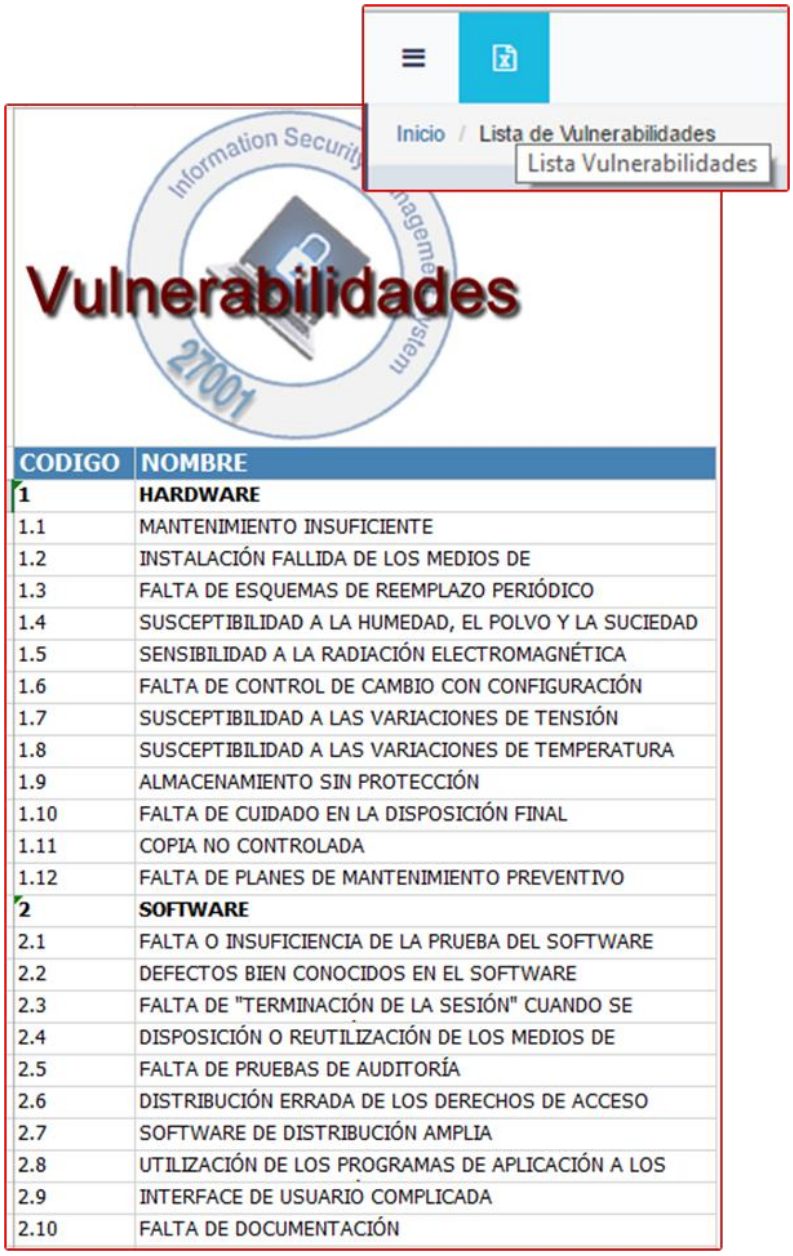


Figura 5.52 Vista del catálogo de vulnerabilidades.

1		HARDWARE
2		SOFTWARE
3		RED
	3.1	FALTA DE PRUEBA DEL ENVÍO O LA RECEPCIÓN DE MENSAJES
	3.2	LÍNEAS DE COMUNICACIÓN SIN PROTECCIÓN
	3.3	TRÁFICO SENSIBLE SIN PROTECCIÓN
	3.4	CONEXIÓN DEFICIENTE DE LOS CABLES
	3.5	PUNTO ÚNICO DE FALLA
	3.6	FALTA DE IDENTIFICACIÓN Y AUTENTIFICACIÓN DE EMISOR Y RECEPTOR
	3.7	ARQUITECTURA INSEGURA DE LA RED
	3.8	TRANSFERENCIA DE CONTRASEÑAS AUTORIZADAS
	3.9	GESTIÓN INADECUADA DE LA RED (CAPACIDAD DE RECUPERACIÓN DEL ENRUTAMIENTO)
	3.10	CONEXIONES DE RED PÚBLICA SIN PROTECCIÓN
	3.11	TRÁFICO NO SEGMENTO
4		PERSONAL
5		LUGAR
6		ORGANIZACIÓN

Figura 5.53 Desglose del árbol de vulnerabilidades.

En la opción ‘Lista de vulnerabilidades’ se puede generar el reporte con el catálogo de vulnerabilidades, ver la Figura 5.54.



CODIGO	NOMBRE
1	**HARDWARE**
1.1	MANTENIMIENTO INSUFICIENTE
1.2	INSTALACIÓN FALLIDA DE LOS MEDIOS DE
1.3	FALTA DE ESQUEMAS DE REEMPLAZO PERIÓDICO
1.4	SUSCEPTIBILIDAD A LA HUMEDAD, EL POLVO Y LA SUCIEDAD
1.5	SENSIBILIDAD A LA RADIACIÓN ELECTROMAGNÉTICA
1.6	FALTA DE CONTROL DE CAMBIO CON CONFIGURACIÓN
1.7	SUSCEPTIBILIDAD A LAS VARIACIONES DE TENSIÓN
1.8	SUSCEPTIBILIDAD A LAS VARIACIONES DE TEMPERATURA
1.9	ALMACENAMIENTO SIN PROTECCIÓN
1.10	FALTA DE CUIDADO EN LA DISPOSICIÓN FINAL
1.11	COPIA NO CONTROLADA
1.12	FALTA DE PLANES DE MANTENIMIENTO PREVENTIVO
2	**SOFTWARE**
2.1	FALTA O INSUFICIENCIA DE LA PRUEBA DEL SOFTWARE
2.2	DEFECTOS BIEN CONOCIDOS EN EL SOFTWARE
2.3	FALTA DE "TERMINACIÓN DE LA SESIÓN" CUANDO SE
2.4	DISPOSICIÓN O REUTILIZACIÓN DE LOS MEDIOS DE
2.5	FALTA DE PRUEBAS DE AUDITORÍA
2.6	DISTRIBUCIÓN ERRADA DE LOS DERECHOS DE ACCESO
2.7	SOFTWARE DE DISTRIBUCIÓN AMPLIA
2.8	UTILIZACIÓN DE LOS PROGRAMAS DE APLICACIÓN A LOS
2.9	INTERFACE DE USUARIO COMPLICADA
2.10	FALTA DE DOCUMENTACIÓN

Figura 5.54 Reporte de vulnerabilidades.

5.4.2 Registro y mantenimiento de amenazas

Asimismo para el catálogo de amenazas se tomó el Anexo C de la norma 27005, al igual que con las vulnerabilidades se define un árbol desde el cual el responsable de seguridad de la

información podrá registrar nuevas amenazas o editar las ya existentes y obtener un reporte sencillo del catálogo de amenazas. Ver la Figura 5.55, la Figura 5.56 y la Figura 5.57.

Figura 5.55 Vista del catálogo de amenazas.

Figura 5.56 Desglose del árbol de amenazas.

Listado Amenazas

Tipo	Cód.	Amenaza
1 - DAÑO FÍSICO	1.1	FUEGO
	1.2	DAÑO POR AGUA
	1.3	CONTAMINACIÓN
	1.4	ACCIDENTE IMPORTANTE
	1.5	DESTRUCCI&OACUTE;N DEL EQUIPO O LOS MEDIOS
	1.6	POLVO, CORROSIÓN, CONGELAMIENTO
	1.7	EVENTOS NATURALES - FENÓMENOS CLIMÁTICOS
	1.8	FENÓMENOS SÍSMICOS
	1.9	FENÓMENOS VOLCÁNICOS
	1.10	FENÓMENOS METEOROLÓGICOS
	1.11	INUNDACIÓN
2 - PÉRDIDA DE LOS SERVICIOS ESENCIALES	2.1	FALLA EN EL SISTEMA DE SUMINISTRO DE AGUA
	2.2	PÉRDIDA DE SUMINISTRO DE ENERGÍA
	2.3	FALLA EN EL EQUIPO DE TELECOMUNICACIONES
	2.4	FALLA EN EL SISTEMA DE SUMINISTRO DE AIRE ACONDICIONADO
3 - PERTURBACIÓN DEBIDA A LA RADIACIÓN	3.1	RADIACIÓN ELECTROMAGNÉTICA
	3.2	RADIACIÓN TÉRMICA
	3.3	IMPULSOS ELECTROMAGNÉTICOS
4 - COMPROMISO DE LA INFORMACIÓN	4.1	INTERCEPTACIÓN DE SEÑALES DE INTERFERENCIA
	4.2	ESPIONAJE REMOTO
	4.3	ESCUCHA SUBREPTICIA
	4.4	HURTO DE MEDIOS O DOCUMENTOS
	4.5	HURTO DE EQUIPO
	4.6	RECUPERACIÓN DE MEDIOS RECICLADOS O DESECHADOS
	4.7	DIVULGACION
	4.8	DATOS PROVENIENTES DE FUENTES NO CONFIABLES
	4.9	MANIPULACIÓN CON HARDWARE
	4.10	MANIPULACIÓN CON SOFTWARE
	4.11	DETECCIÓN DE LA POSICION
	4.12	HACKING INFORMATICO
	4.13	ATAQUES DE INGENIERIA SOCIAL
	4.14	CAMBIOS NO AUTORIZADOS
5 - FALLAS TÉCNICAS	5.1	FALLA DEL EQUIPO
	5.2	MAL FUNCIONAMIENTO DEL EQUIPO
	5.3	SATURACIÓN DEL SISTEMA DE INFORMACION
	5.4	MAL FUNCIONAMIENTO DEL SOFTWARE
	5.5	INCUMPLIMIENTO EN EL MANTENIMIENTO DEL SISTEMA DE
6 - ACCIONES NO AUTORIZADAS	6.1	USO NO AUTORIZADO DEL EQUIPO
	6.2	COPIA FRAUDULENTA DEL SOFTWARE
	6.3	USO DE SOFTWARE FALSO O COPIADO

Figura 5.57 Reporte de Amenazas.

La asociación de las vulnerabilidades con amenazas es lo realmente valioso que tendrá que hacer el responsable de seguridad de la información, ya que al armar este par amenaza-vulnerabilidad estará dejando listas las posibles causas que definirán luego las causas de los riegos que se gestionarán en el SGSI. Para ello se tiene la opción ‘Asociar vulnerabilidades’

con la cual se pueden relacionar muchas amenazas con muchas vulnerabilidades. Ver la Figura 5.58.

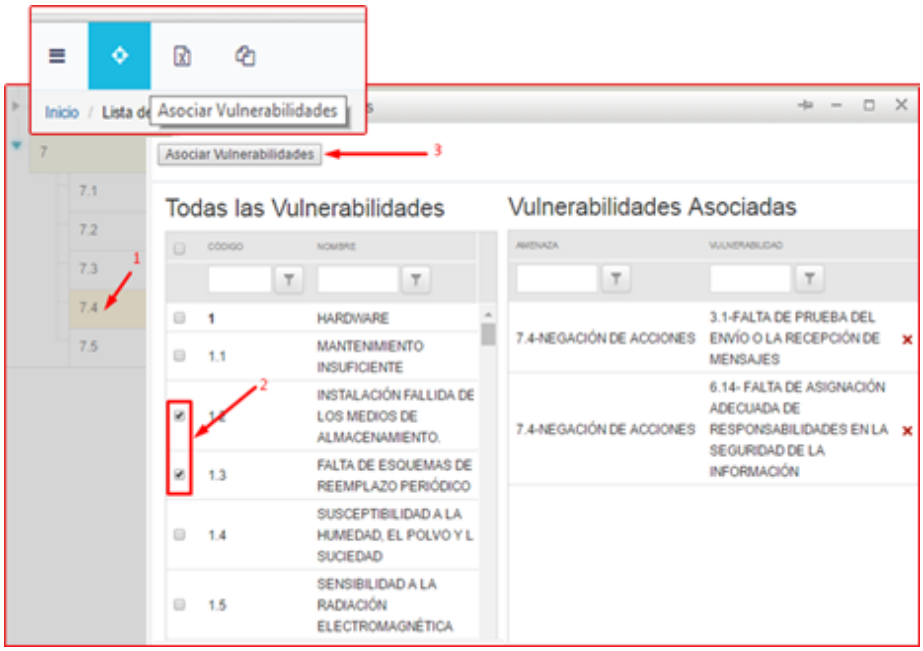
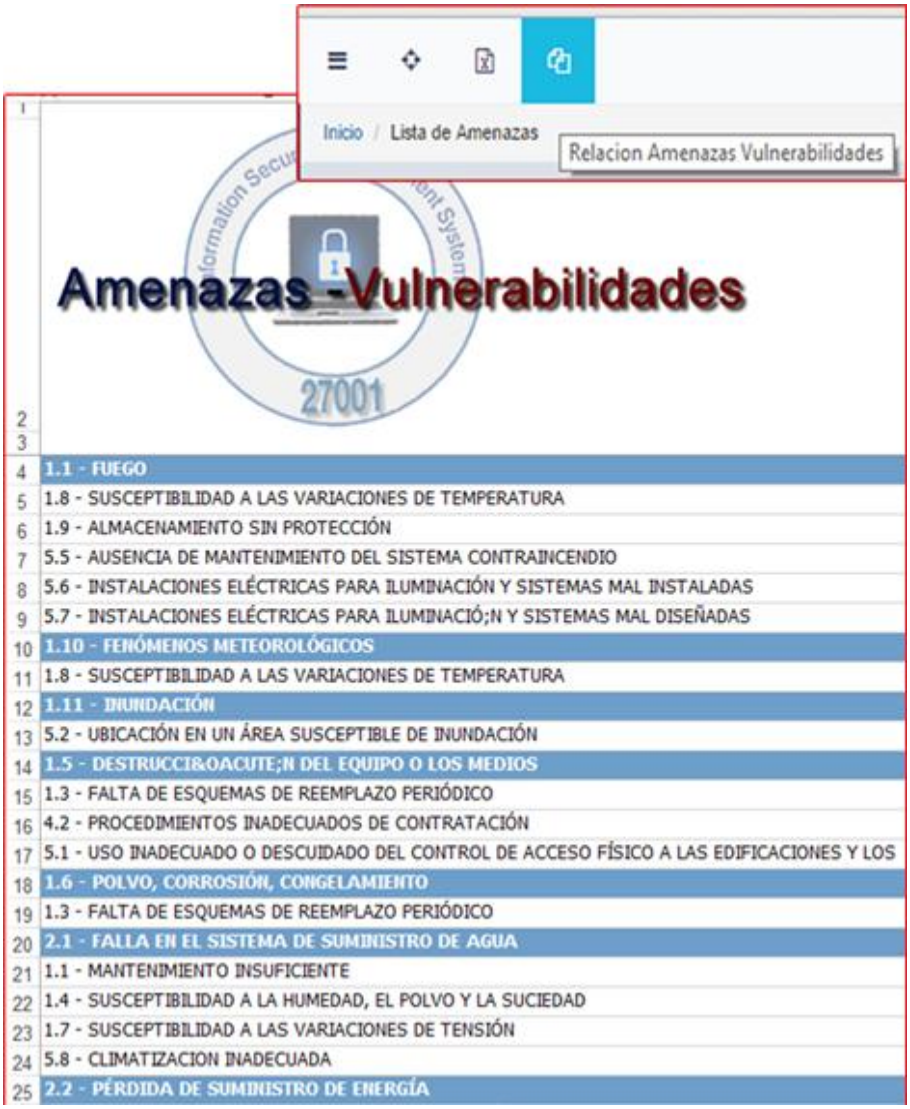


Figura 5.58 Opción para asociar las amenazas y las vulnerabilidades.

De igual forma se tendrá disponible un reporte con la asociación de vulnerabilidades y amenazas realizadas tal como se muestra en la siguiente figura.



4	1.1 - FUEGO
5	1.8 - SUSCEPTIBILIDAD A LAS VARIACIONES DE TEMPERATURA
6	1.9 - ALMACENAMIENTO SIN PROTECCIÓN
7	5.5 - AUSENCIA DE MANTENIMIENTO DEL SISTEMA CONTRAINCENDIO
8	5.6 - INSTALACIONES ELÉCTRICAS PARA ILUMINACIÓN Y SISTEMAS MAL INSTALADAS
9	5.7 - INSTALACIONES ELÉCTRICAS PARA ILUMINACIÓ;N Y SISTEMAS MAL DISEÑADAS
10	1.10 - FENÓMENOS METEOROLÓGICOS
11	1.8 - SUSCEPTIBILIDAD A LAS VARIACIONES DE TEMPERATURA
12	1.11 - INUNDACIÓN
13	5.2 - UBICACIÓN EN UN ÁREA SUSCEPTIBLE DE INUNDACIÓN
14	1.5 - DESTRUCCI&OACUTE;N DEL EQUIPO O LOS MEDIOS
15	1.3 - FALTA DE ESQUEMAS DE REEMPLAZO PERIÓDICO
16	4.2 - PROCEDIMIENTOS INADECUADOS DE CONTRATACIÓN
17	5.1 - USO INADECUADO O DESCUIDADO DEL CONTROL DE ACCESO FÍSICO A LAS EDIFICACIONES Y LOS
18	1.6 - POLVO, CORROSIÓN, CONGELAMIENTO
19	1.3 - FALTA DE ESQUEMAS DE REEMPLAZO PERIÓDICO
20	2.1 - FALLA EN EL SISTEMA DE SUMINISTRO DE AGUA
21	1.1 - MANTENIMIENTO INSUFICIENTE
22	1.4 - SUSCEPTIBILIDAD A LA HUMEDAD, EL POLVO Y LA SUCIEDAD
23	1.7 - SUSCEPTIBILIDAD A LAS VARIACIONES DE TENSIÓN
24	5.8 - CLIMATIZACION INADECUADA
25	2.2 - PÉRDIDA DE SUMINISTRO DE ENERGÍA

Figura 5.59 Reporte de asociación de amenazas y vulnerabilidades.

5.4.3 Registro y mantenimiento de riesgos

La primera ventana que aparece cuando se da click en la opción ‘Riesgos’ es la que se muestra en la Figura 5.60; primero se ve la pestaña en donde están todos los activos registrados

con o sin tasación. En la segunda pestaña estará el registro del riesgo en sí.

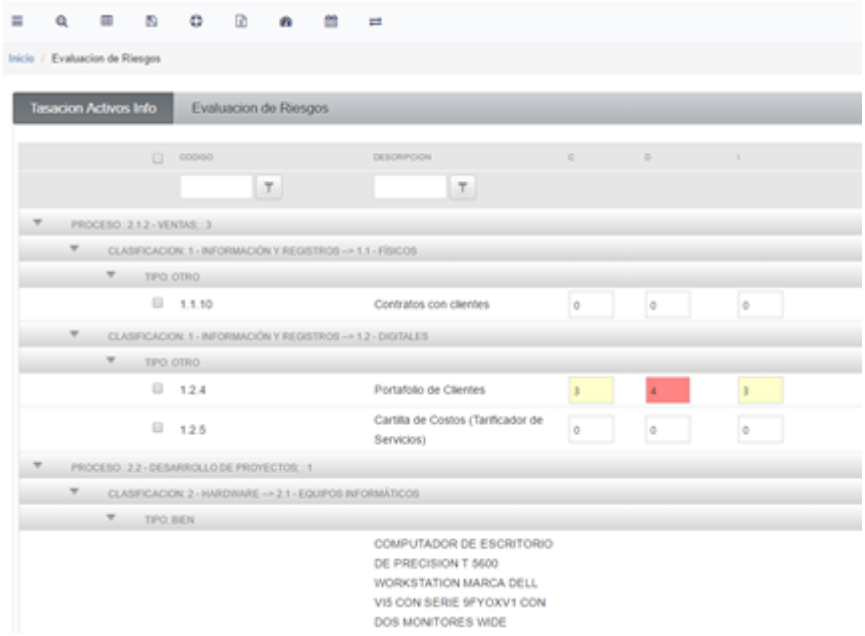


Figura 5.60 Pestaña de ‘activos’ en el registro de riesgos.

Es decir, que cuando se seleccionan uno o más riesgos en la primera pestaña y se da click en la opción ‘Ver riesgos’ (ver Figura 5.61), los riesgos de los activos seleccionados aparecerán en la segunda pestaña. En la parte superior de la pestaña ‘Evaluación de riesgos’ aparecen las escalas de impacto x probabilidad indicando las zonas de riesgo que se preestablecieron (ver Figura 5.62).

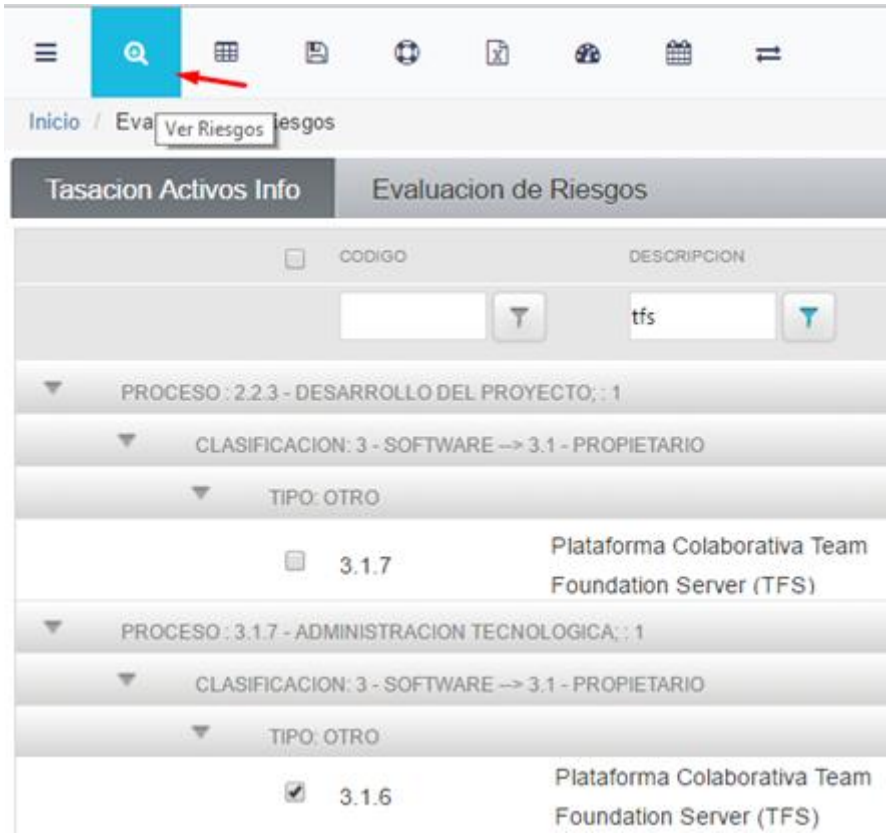


Figura 5.61 Búsqueda de riesgos por activo.

Figura 5.62 Vista de las zonas de riesgos en la pestaña 'Evaluación de riesgos'.

Si se quiere registrar un nuevo riesgo o cambiar las causas de riesgos y su respectiva probabilidad en un riesgo ya registrado se debe dar click en la opción 'Buscar Amenazas Vulnerabilidades' con lo cual se despliega una ventana modal en donde se recuerda la escala de probabilidades definida y un combo box con el árbol de amenazas de modo tal que se puedan seleccionas una o varias amenazas y dar click en

‘Buscar’ a fin de traer las vulnerabilidades asociadas a ellas. Ver Figura 5.63.

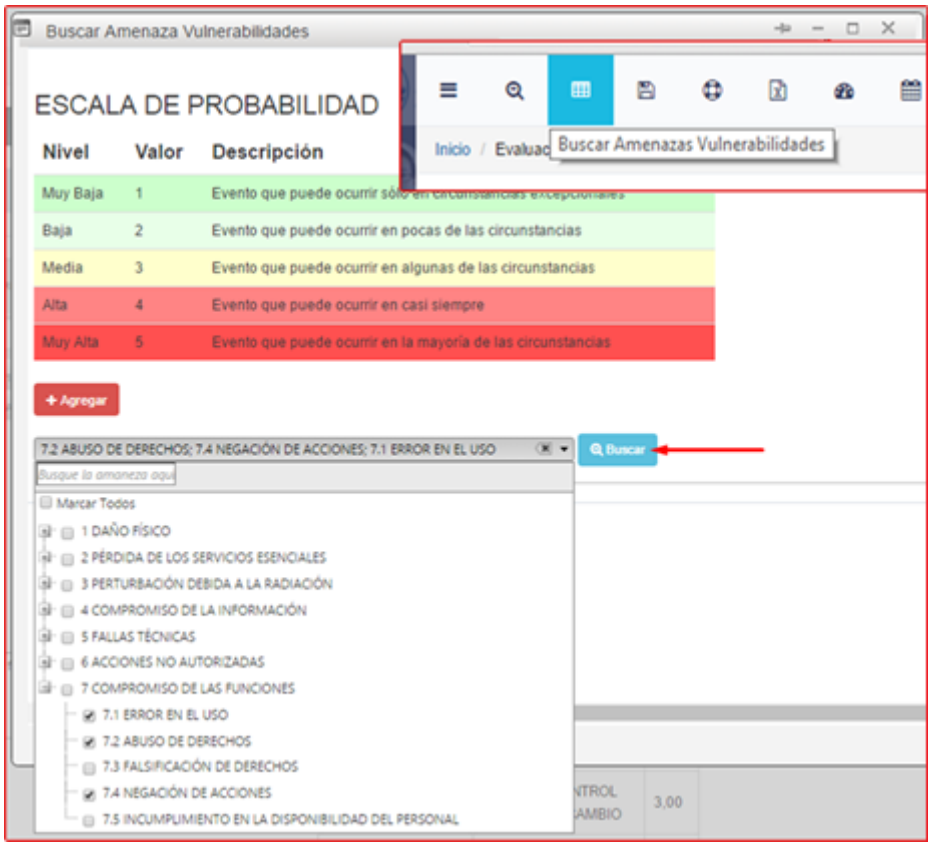


Figura 5.63 Búsqueda de pares amenaza-vulnerabilidad para establecer las causas de un riesgo.

Con el resultado de la búsqueda se tienen todos los pares amenaza-vulnerabilidad que pueden ser causa del riesgo que se quiere registrar. Por cada par el responsable de seguridad de la información o el gestor de riesgos deberá indicar una probabilidad de ocurrencia y al final dar click en ‘agregar’ tal como se muestra en la siguiente figura.

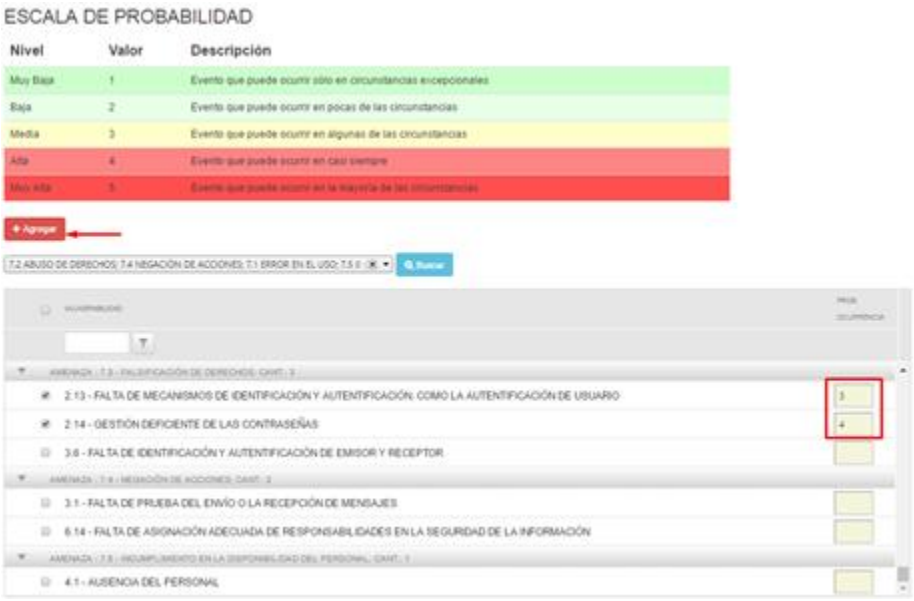


Figura 5.64 Definición de probabilidades de ocurrencia en las causas del riesgo.

Una vez que se definieron las causas con su probabilidad correspondiente, el sistema obtiene una probabilidad de ocurrencia promedio que se multiplicará con el valor de la tasación (Impacto) para así obtener el valor del riesgo. Se debe completar la información del riesgo con la respectiva descripción, asignación de responsable y fecha de registro. Ver Figura 5.65.

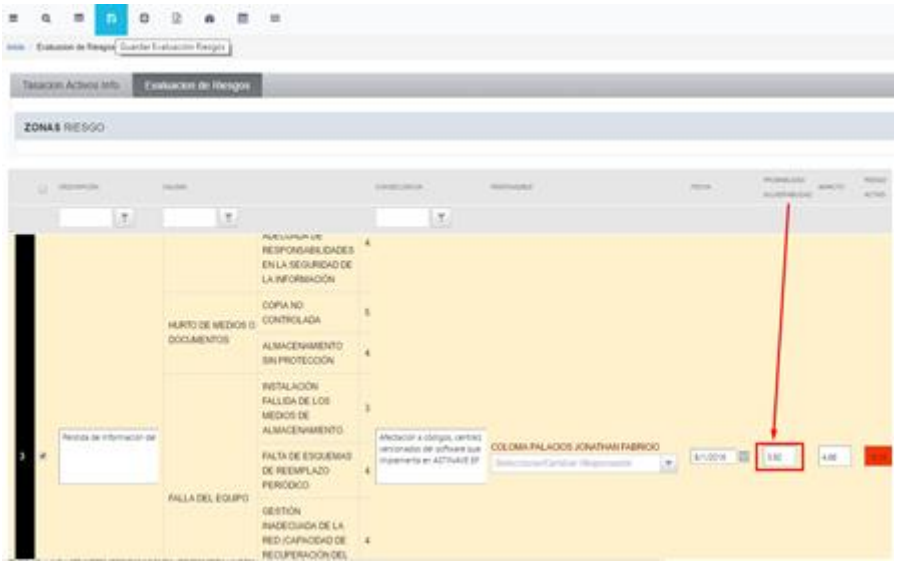


Figura 5.65 Registro de riesgo completo.

En todo momento un riesgo puede ser controlado verificando cómo evoluciona, es decir, el historial que lleva el sistema va a permitir que siempre se tenga visibilidad del riesgo inherente y del residual si es que luego de la aplicación de controles operacionales hay cambios en el valor del riesgo. Ver Figura 5.66.

Figura 5.66 Consulta de la evolución del riesgo.

5.4.4 Registro de planes de acción para el tratamiento de riesgos.

Una vez que se registra un riesgo también debería registrarse el tratamiento correspondiente, éste será una serie de acciones propuestas a fin de mitigar, aceptar, transferir o evitar el riesgo. Para ello se selecciona un riesgo y se da click en la opción ‘Registrar Planes Acción’.

En la ventana de ‘Plan de Acción’ se indica a qué riesgo se le registra el plan, se muestra el historial de cambios que ha tenido

el riesgo seleccionando de manera predeterminada el último registro tal como se aprecia en la Figura 5.67.

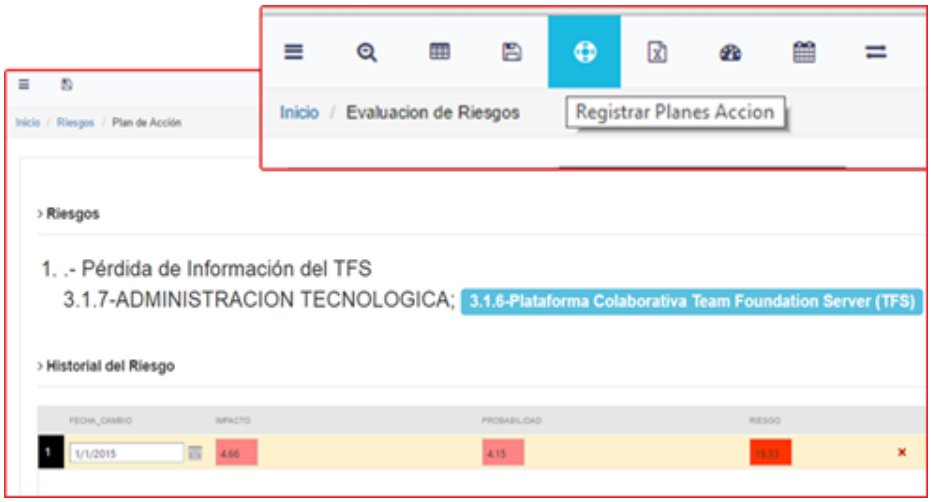


Figura 5.67 Vista de la ventana para el registro de planes de acción.

De igual forma el usuario podrá seleccionar los pares amenaza-vulnerabilidad que conforman la causa del riesgo. Ver Figura 5.68.

Figura 5.68 Elección de las causas definidas en el riesgo para el registro de una acción de tratamiento.

Deberá, como es obvio, describir en qué consiste la acción propuesta, qué tipo de respuesta al riesgo será, quien será el responsable de ejecutarla, la fecha recomendad de ejecución y uno o muchos controles recomendado del anexo a tal como se aprecia en la Figura 5.69.

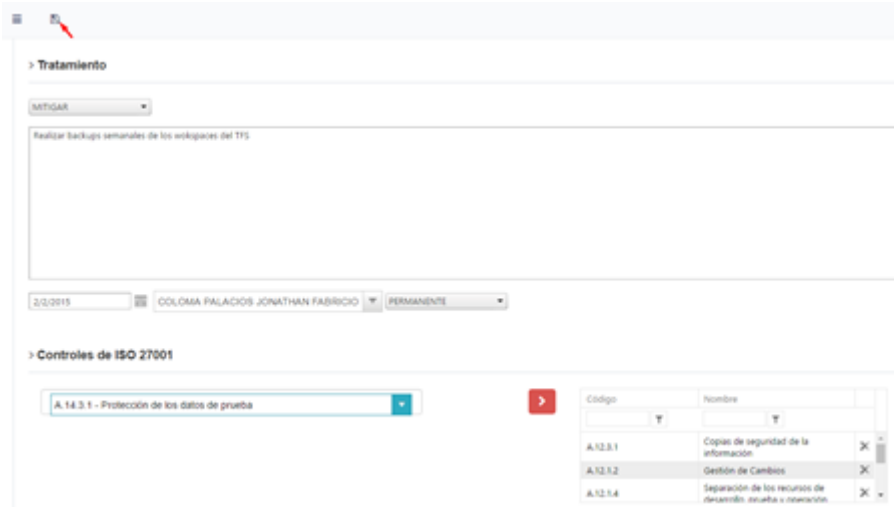


Figura 5.69 Descripción de la acción planeada, definición de tratamiento, fecha, responsable y controles de la norma asociados.

El responsable de seguridad de la información o el gestor de riesgos siempre tendrá acceso al histórico de acciones planificadas y de ser necesario podrá eliminarlas. Ver Figura 5.70.

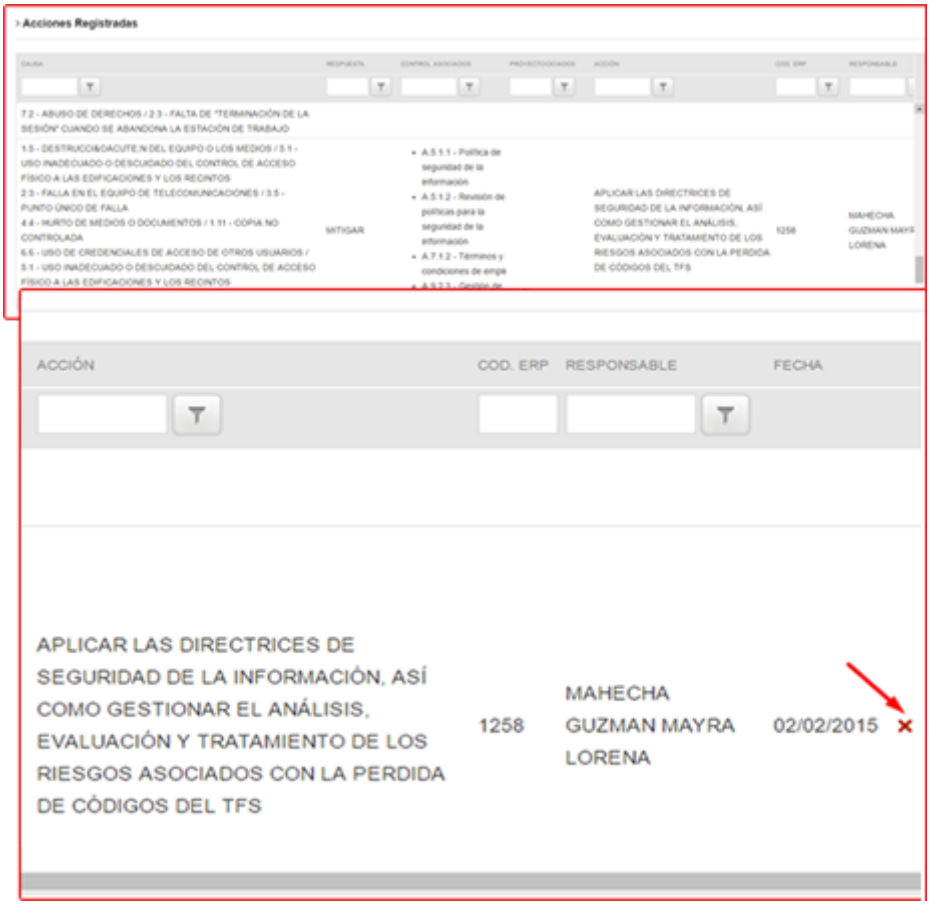
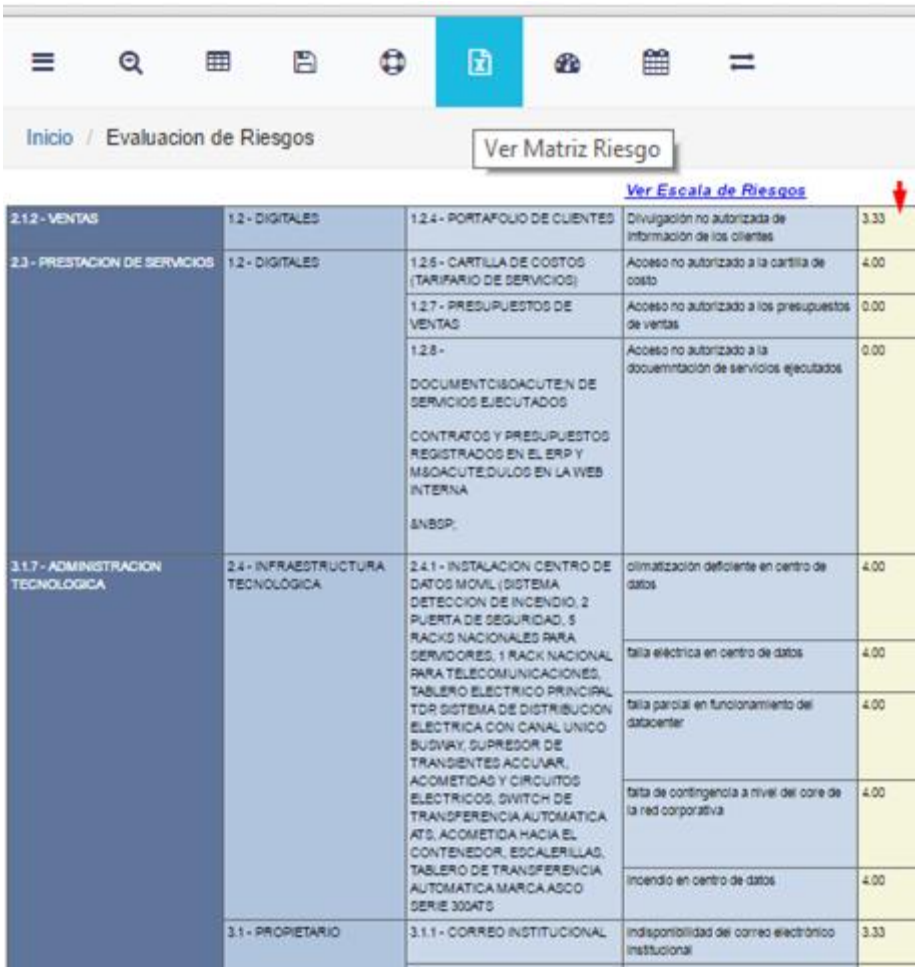


Figura 5.70 Opción y Consulta de acciones planeadas para el tratamiento de riesgos.

5.4.5 Seguimiento de riesgos

Para dar seguimiento a los riesgos y a las acciones propuestas para tratarlos, el sistema proporciona una matriz de riesgos en la cual las filas son los activos con el correspondiente proceso y, obvio, la descripción del riesgo y el valor del impacto. Las columnas son las causas del riesgo y la probabilidad promediada. Con ambas, filas y columnas, se logra tener el valor del riesgo en su fórmula primaria Impacto x Probabilidad.

En la secuencia gráfica de la Figura 5.71, Figura 5.72 y Figura 5.73 se pueden apreciar los fragmentos de la matriz de riesgo la cual, dicho sea de paso, se hará más extensa a medida que el número de riesgos aumente.



2.1.2 - VENTAS	1.2 - DIGITALES	1.2.4 - PORTAFOLIO DE CLIENTES	Divulgación no autorizada de información de los clientes	3.33
2.3 - PRESTACION DE SERVICIOS	1.2 - DIGITALES	1.2.6 - CARTILLA DE COSTOS (TARIFARIO DE SERVICIOS)	Acceso no autorizado a la cartilla de costo	4.00
		1.2.7 - PRESUPUESTOS DE VENTAS	Acceso no autorizado a los presupuestos de ventas	0.00
		1.2.8 - DOCUMENTCI&OACUTE;N DE SERVICIOS EJECUTADOS CONTRATOS Y PRESUPUESTOS REGISTRADOS EN EL ERP Y M&OACUTE;DULOS EN LA WEB INTERNA	Acceso no autorizado a la documentación de servicios ejecutados	0.00
3.1.7 - ADMINISTRACION TECNOLOGICA	2.4 - INFRAESTRUCTURA TECNOLOGICA	2.4.1 - INSTALACION CENTRO DE DATOS MOVIL (SISTEMA DETECCION DE INCENDIO, 2 PUERTA DE SEGURIDAD, 5 RACKS NACIONALES PARA SERVIDORES, 1 RACK NACIONAL PARA TELECOMUNICACIONES, TABLERO ELECTRICO PRINCIPAL TDP, SISTEMA DE DISTRIBUCION ELECTRICA CON CANAL UNICO BUSWAY, SUPRESOR DE TRANSIENTES ACCUVAR, ACOMETIDAS Y CIRCUITOS ELECTRICOS, SWITCH DE TRANSFERENCIA AUTOMATICA ATS, ACOMETIDA HACIA EL CONTENEDOR, ESCALERILLAS, TABLERO DE TRANSFERENCIA AUTOMATICA MARCA ASCO SERIE 300ATS	climatización deficiente en centro de datos	4.00
			falla eléctrica en centro de datos	4.00
			falla parcial en funcionamiento del datacenter	4.00
			falta de contingencia a nivel del core de la red corporativa	4.00
			incendio en centro de datos	4.00
	3.1 - PROPIETARIO	3.1.1 - CORREO INSTITUCIONAL	indisponibilidad del correo electrónico institucional	3.33

Figura 5.71 Vista de las filas de la matriz de riesgos.

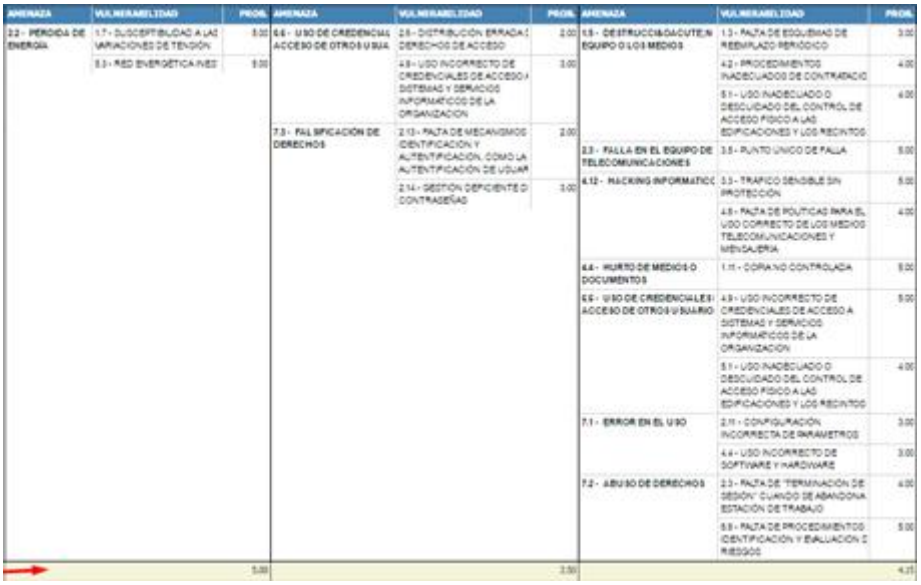


Figura 5.72 Vista de las columnas de la matriz de riesgos.

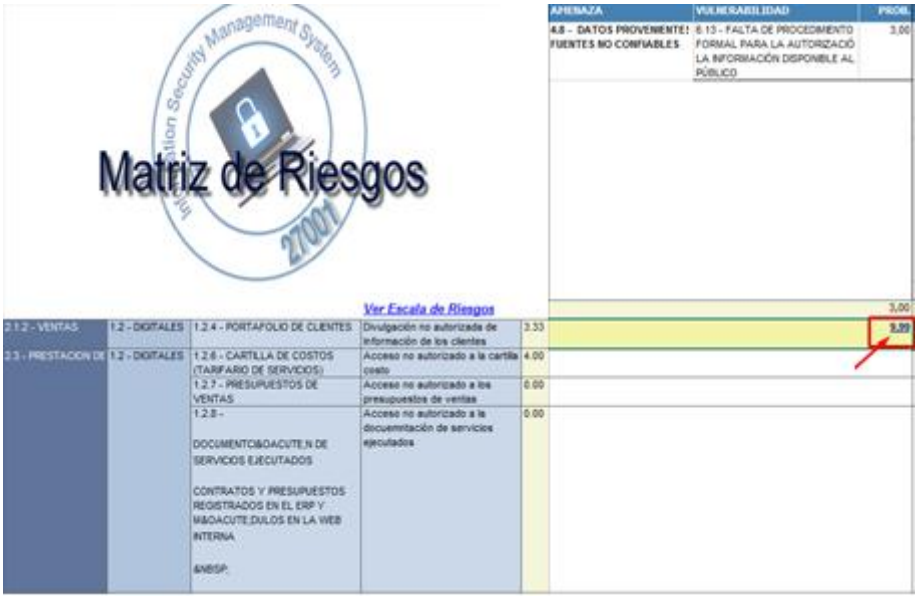


Figura 5.73 Vista de un riesgo en la matriz.

La matriz permite hacer drill down sobre el valor del riesgo, es decir, que cuando se da click sobre él el sistema muestra los planes de acción registrados y a su vez cuando se da click

sobre un plan se pueden desglosar las acciones realizadas para cumplir con el tratamiento. Ver Figura 5.74.

Figura 5.74 Vista en drill down de las acciones planeadas para el tratamiento.

Otra alternativa de seguimiento es el mapa de calor, el cual de forma rápida le dará al usuario una idea de la distribución de los riesgos; si se da click en alguno de los valores se mostrarán los riesgos que están con ese valor aproximado. La Figura 5.75 y la Figura 5.76 dan evidencia de cómo funciona el mapa de calor.

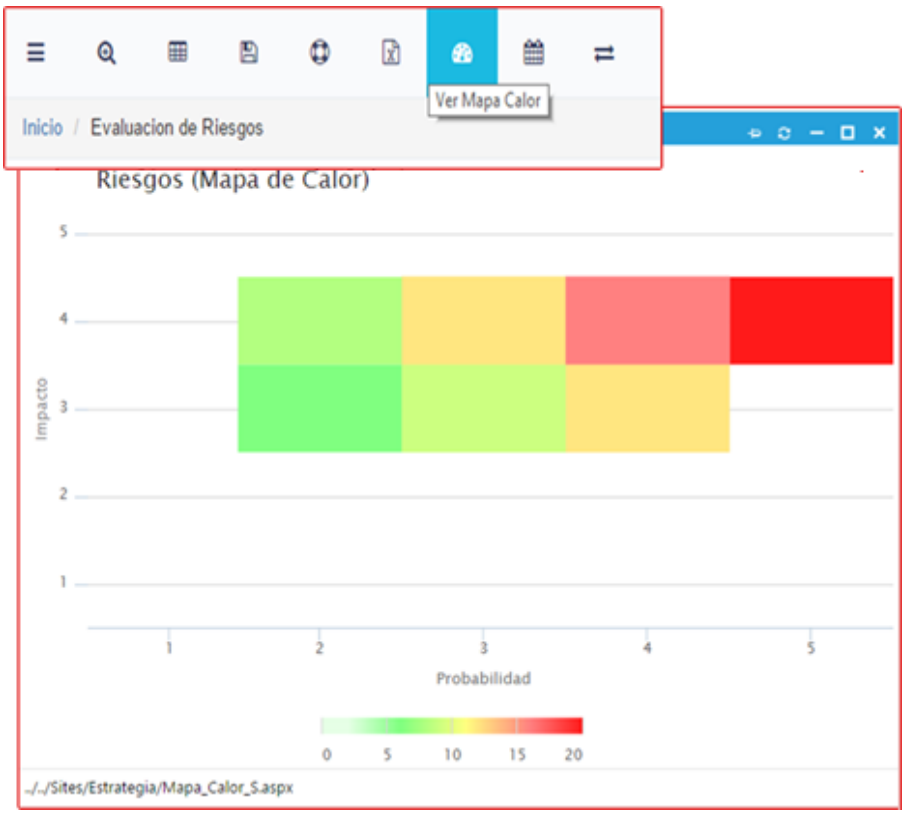


Figura 5.75 Vista del mapa de calor de los riesgos.

Figura 5.76 Identificación de los riesgos desde el mapa de calor.

Asimismo si se selecciona un riesgo se puede ver su línea de tiempo directamente, en esa línea de tiempo se verifica la trazabilidad completa del riesgo desde cuando se registró, los cambios que tendrá en su valores, planes de acciones, acciones realizadas, en fin, es usar la misma opción que se revisó desde la opción ‘Controles’ pero directamente tal como se muestra en la siguiente figura.

Figura 5.77 Vista de la línea de tiempo por riesgo.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

Una vez que la solución propuesta completó su fase de puesta en producción se pudieron recabar resultados importantes respecto a los objetivos planteados y al uso de la herramienta informática en sí. A continuación el análisis de los mismos.

6.1 Por objetivos Propuestos

En cada una de las fases contempladas: análisis, desarrollo e implementación de la solución propuesta, se tienen resultados relacionados a los 6 objetivos planteados en el capítulo 1, a saber:

1. **Dar el contexto general que sustenta el presente trabajo.-** se explicaron los antecedentes en los que se basó la solución

propuesta, así como la experiencia de los autores en temas relacionados a la seguridad de la información y como en base a esa experiencia proponían que gestionar la implantación y mantenimiento de un SGSI podría facilitarse y agilitarse con la ayuda de un sistema de información pensado justamente para ello. Se propuso entonces al menos automatizar las siguiente tareas:

a. Mantener el Inventario de activos de información.

b. Catalogar los procesos de la organización.

c. Gestionar el catálogo de amenazas y vulnerabilidades.

d. Calcular la tasación de activos de información.

e. Registrar y mantener la identificación de riesgos.

f. Gestionar la evaluación de riesgos.

g. Gestionar la asignación de responsables de seguimiento y de las acciones para el tratamiento de riesgos.

h. Registrar la asociación de evidencia documental.

i. Generar reportes y consultas de seguimiento para la gestión de controles de la Norma.

j. Generar la declaración de aplicabilidad.

2. **Presentar el marco teórico de la seguridad de la información y la Norma ISO 27001.-** Se consiguió explicar de manera extendida los conceptos de SGSI y su estrecha relación con el ciclo de Deming, activos de información, amenazas, vulnerabilidades, riesgos. Se explicó también el enfoque y la estructura de la norma que con los cambios adaptados en la versión 2013 dejó 114 controles en Anexo A, y las cláusulas del 4 al 10 en el Anexo SL; al final se hizo una comparativa sencilla con la versión del 2008 centrándose en los cambios sustanciales.

3. **Dar conocer la situación actual y los requerimientos con respecto al SGSI de la organización donde se propone la implementación.-** Se realizó un levantamiento completo de los factores que en la actualidad tienen algún tipo de incidencia sobre los proyectos de Sistemas de Gestión de Seguridad de la Información en las organizaciones de Ecuador. Se revisaron iniciativas de estado como el Esquema Gubernamental de la Seguridad de la Información y una resolución de la Junta Bancaria que dan obligatoriedad a las organizaciones del sector bancario-financiera de implementar Continuidad del Negocio y SGSI. Se revisaron también las estadísticas de acreditación de la norma a nivel país y comparativamente con la región, a nivel mundial el esfuerzo de Latinoamérica luce todavía muy marginal, obtenidas

del sitio web oficial de la organización ISO con base en las últimas estadísticas publicadas en el 2014. Como otro factor a analizar estuvo también el software que se usa actualmente para gestionar un SGSI, se mencionaron y compararon entre si 4 de los más conocidos. Todos los factores analizados se enfocaron al final a la situación de ASTINAVE EP, la organización a la cual se le hizo la propuesta de implementación. Se indicó que ASTINAVE EP es una empresa pública con gestión de recursos propios que desde el 2012 viene haciendo esfuerzos ingentes para estandarizar sus procesos al grado de tener un Sistema Integrado de Gestión con certificaciones en ISO 9001, ISO 14001 e ISO 18001, de allí que ya se tiene un terreno propicio para impulsar un SGSI tanto más si se considera que es una empresa que en su giro de negocio considera soluciones integrales para el sector de la defensa.

4. **Mostrar el análisis y diseño del sistema de información en base a los requerimientos de la norma y del contexto organizacional.-** se dedicó todo un capítulo para explicar con lujos de detalles las decisiones en cuestiones de metodología de trabajo para el esquema de desarrollo, arquitectura a emplearse en la solución, herramientas a utilizarse tanto en el modelado como en la codificación. Asimismo los módulos funcionales fueron expuestos desde los modelos de datos físicos y los casos de usos

correspondientes. A más de ello se estableció la metodología de gestión de activos y de sus respectivos riesgos en función de la norma ISO 27005; las reglas de negocio de los módulos funcionales correspondientes se programaron en base a esto al igual que las escalas de impacto, las escalas de probabilidad de ocurrencia y las zonas de riesgo.

5. **Detallar la implementación del sistema de información y su puesta en producción.-** Se dieron detalles propios de la implementación en los servidores de producción web, base de datos y de reportes, así como las consideraciones especiales de la puesta en producción. Entre esas consideraciones, al igual que lo hicieron en fase de diseño, resaltaron las integraciones con Sharepoint y con el ERP de la organización. Además se presentó evidencia de cómo funciona el sistema ya puesto en producción y siendo utilizado por los usuarios que integran el grupo metodológico del SGSI de ASTINAVE EP.

6. **Listar los resultados de las pruebas del sistema.-** El presente análisis de los resultados del trabajo íntegro tratado a minucia en los capítulos previos debería solventar el cumplimiento de este objetivo.

6.2 Por Uso del Sistema de Información

Manteniendo el orden en el cual se presentaron los módulos funcionales para su análisis diseño e implementación, se revisarán también los resultaron obtenidos en cada uno de ellos una vez que fueron usados en entorno de producción en la intranet de ASTINAVE EP, así que se tomará la evidencia presentada en el capítulo 5 respecto a la Pruebas de Aplicación y Uso de la Herramienta, a saber:

1. Gestión de Controles de la Norma:

    a. Generación de la declaración de aplicabilidad.

    b. Asignación de los responsables del seguimiento de los controles del Anexo A.

    c. Asociación de los documentos del gestor documental para los controles del Anexo A.

    d. Consulta general para seguimiento del SGSI.

    e. Consulta de la líneas de tiempo por control.

2. Gestión de Activos de Información:

    a. Registro y mantenimiento de procesos empresariales.

    b. Registro y mantenimiento del catálogo de activos.

c. Asociación de activos x proceso empresarial.

d. Reporte de activos x proceso.

e. Reporte de procesos empresariales.

f. Integración con bienes administrados por al área financiera (activos fijos y otros bienes de control).

g. Generación de encuestas para la valoración de activos de información.

h. Votación de dueños de procesos y propietarios de activos para valorar el impacto de los activos.

i. Registro de tasación directa por parte del responsable de seguridad de información.

j. Reporte de la tasación de activos.

3. Gestión de Riesgos:

a. Registro y mantenimiento de catálogo de amenazas de acuerdo al Anexo C de la ISO 27005.

b. Registro y mantenimiento del catálogo de vulnerabilidades de acuerdo al Anexo D de la ISO 27005.

c. Asociación de amenazas y vulnerabilidades para obtener los pares amenaza-vulnerabilidad que serán las causas de un riesgo a gestionarse.

d. Registro y mantenimiento del riesgo de un activo de información.

e. Registro y mantenimiento de los planes de acción para el tratamiento de los riesgos.

f. Registro de las acciones realizadas para el cumplimiento de planes de acción.

g. Generación de la matriz de riesgo.

h. Generación del mapa de calor.

i. Generación de historiales del riesgo.

j. Consulta directa por riesgo en la línea de tiempo.

k. Consulta de la evolución del riesgo de inherente a residual.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Se logró analizar el contexto interno y externo para la implantación de un SGSI de una organización en Ecuador considerando para ello los factores con incidencia directa. Uno de los factores que merece ser resaltado es el impulso que desde el gobierno se ha venido dando desde el 2013 para que las organizaciones acojan el estándar ISO 27001.

2. Se explicó de manera extensa y, hasta donde se pudo, simplificada, lo que es un sistema de gestión de la seguridad de la información y los conceptos involucrados como qué es un activo de información, cómo se gestionan sus riesgos frente a potenciales incidentes de seguridad y

cómo un SGSI se mantiene gracias a la mejora continua sustentada en un ciclo PHVA.

3. Se acogió la ISO 27005 como metodología para la gestión de riesgos y en base a este estándar se programaron todas las reglas de negocio relacionadas con la gestión de activos de información y la gestión riesgos. Es decir que se releva el hecho de que los activos estén relacionados con los procesos empresariales y que sus riesgos definan causas en función de pares amenaza-vulnerabilidad.

4. La propuesta realizada hacía referencia a que un sistema de información sería de ayuda para agilitar y gestionar en mejor manera una implantación de SGSI conservando la trazabilidad completa para cada activo de información, pues en base a ese planteamiento se realizó el análisis, el diseño y la implementación del software que desde Julio del 2015 está siendo usado por miembros de Comité de Seguridad de la información y del equipo de Gestión Integral en la empresa ASTINAVE EP, vale la pena recalcar que esta organización ya está recertificada con un Sistema Integrado de Gestión, por lo cual el hecho de que lo estén usando con buena acogida resulta aún más válido.

5. Se consigue con este sistema que la tasación de los activos de información que es el proceso de valoración del impacto que tiene cada activo en función de disponibilidad, confidencialidad e integridad y

haciendo uso de una escala predefinida, sea realizada por definición directa del responsable de seguridad de información pero también se brinda la alternativa de que los involucrados con el activo como los propietarios y dueños del proceso pueda realizar una valoración individual como en una votación y al final se tenga un valor consolidado en función de estas votaciones.

6. Se comprueba que la solución propuesta mantiene una trazabilidad completa de los riesgos para cada activo de información permitiendo incluso consultar líneas de tiempo en las cuales se pueden verificar los planes de acción para el tratamiento de los riesgos y las acciones que se realizan para su cumplimiento.

7. Se lograron exponer los resultados del presente trabajo de manera muy práctica y bajo el enfoque de los objetivos propuestos y del mismo uso del sistema. Estos resultados dan cuenta de todo el trabajo realizado por los maestrantes a fin de brindar una alternativa que automatice la mayoría de procesos propios de un SGSI como la generación del SOA, registros de catálogos de activos, registros y gestión de riesgos, etc.

8. En un plano más bien técnico, se consiguió integrar el software propuesto con el ERP y el gestor documental (Sharepoint) de modo tal que sea más robusto y de mayor utilidad para el usuario de ASTINAVE

EP, asimismo la autenticación de los usuarios se realiza contra el directorio activos de la organización.

9. La solución se diseñó bajo un esquema iterativo en lo que refiere a la metodología del desarrollo y una arquitectura de n-capas en lo respectivo a la programación de objetos; una combinación que en ingeniería de software viene dando buenos resultados por modularidad y rapidez.

Recomendaciones

1. Para un software como el propuesto para el presente trabajo de titulación sería muy bueno implementar al menos dos módulos funcionales más; uno que gestione las auditorias con la descripción de observaciones y no conformidades correspondientes y otro que sea un dashboard para verificar los indicadores del SGSI, al robustecerse de esta manera este software no tendría nada que pedirle a los ya conocidos ISO TOOLS, GLOBAL SUITE o ISOLUCIÓN.

BIBLIOGRAFÍA

[1] International Organitation for Standardization: ISO 27001 - information security management, «ISO/IEC 27001 - Information security management,» 2013. [En línea]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm. [Último acceso: 01 05 2016].

[2] Fiscalia General del Estado, «Los delitos informáticos van desde el fraude hasta el espionaje,» Fiscalia General del Estado, Quito, 2015.

[3] SGS United Kindom, Curso de formación de auditor/auditor líder en Sistemas de Gestión deSeguridad de Información, Guayaquil: SGS United Kindom, 2015.

[4] PMG-SSI, «Blog especializado en Sistemas de Gestión de Seguridad de la Información,» 18 08 2015. [En línea]. Available: http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/.

[5] D. G. Trejo, «ISO-27001:2013 ¿Qué hay de nuevo?,» 30 08 2013. [En línea]. Available: http://www.magazcitum.com.mx/?p=2397#.V0H7EuR3Xrl. [Último acceso: 20 05 2016].

[6] www.iso27000.es, «El portal de ISO 27001 en Español,» [En línea]. Available: http://www.iso27000.es/sgsi.html.

[7] UPTC, «UPTC - SIG,» [En línea]. Available: http://aplica.uptc.edu.co/SigmaII/Documents/2014/Guia para la Gesti%C3%B3n del Riesgo de Activos de Informacion Ver 03.pdf.

[8] Gobierno Electrónico Ecuador, «AUTORIZACIÓN TÉCNICA DE PROYECTOS TI,» 01 06 2016. [En línea]. Available: http://www.gobiernoelectronico.gob.ec/indicadores/. [Último acceso: 05 07 2016].

[9] B. S. Vanini, «Gestión,» 5 11 2014. [En línea]. Available: http://gestion.pe/tecnologia/tendencia-2015-seguridad-informatica-mundo-corporativo-se-encuentra-mira-cibercriminales-2113007. [Último acceso: 06 07 2016].

[10] ESET, «We live security,» 03 2015. [En línea]. Available: http://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf. [Último acceso: 08 07 016].

[11] A. Raso, «Shellshock: Hipertextual,» 16 09 2014. [En línea]. Available: https://hipertextual.com/archivo/2014/09/shellshock/. [Último acceso: 08 07 2016].

[12] M. G. Facti, «¿Qué es el heartbleed?,» [En línea]. Available: http://marvingarciafacti.jimdo.com/que-es-el-heartbleed/. [Último acceso: 08 07 2016].

[13] ESET, «We Live Security,» 15 10 2014. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/10/15/poodle-vulnerabilidad-ssl-3/. [Último acceso: 9 7 2016].

[14] Microsoft, «Información general sobre ASP.NET,» 11 2007. [En línea]. Available: https://msdn.microsoft.com/es-es/library/4w3ex9c2(v=vs.100).aspx. [Último acceso: 12 07 2016].

[15] M. Collazos Balaguer, «Colegio de Ingenieros del Perú,» 10 10 2013. [En línea]. Available: http://www.cip.org.pe/index.php/eventos/conferencias-ceremonias-y-patrocinios/item/download/125_2f7be404f0dba27dabc8efd91bd14668.html.