ESCUELA SUPERIOR POLITECNICA DEL LITORAL

Instituto de Ciencias Matemáticas

Auditoría y Control de Gestión

"Evaluación del sistema de mantenimiento asistido por computadora de una empresa del sector naviero"

TESIS DE GRADO

Previo a la obtención del título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentado por:

David Medardo Carrión Miranda

GUAYAQUIL – ECUADOR

Año: 2005

AGRADECIMIENTO

Quiero agradecer eternamente a Dios por permitirme tener vida, salud, por darme las fuerzas necesarias para iniciar, mantenerme y finalizar esta etapa de mi vida. A mis padres y a mis hermanos por apoyarme y sobre todo por el hermoso e inolvidable sacrificio que hicieron para darme mis estudios. A mi Directora de Tesis Ing. Alice Naranjo Sánchez por brindarme todos sus conocimientos, su inmensa paciencia, y sobre todo por la gran preocupación y sacrificio de dirigirme. A mi gran y eterna amiga mi enamorada Anita María H. por apoyarme, darme fuerza para seguir adelante. A mis buenos amigos Luis franco, Eduardo Falcónez, Annabell Alvarado por ayudarme en la culminación de mi tesis y a mis grandes amigos que de una y otra forma estuvieron junto a mí en varios momentos de mi vida Mariela, Wendy, Roxana, María, Ginger, Franklin, Johanna , Piedad, etc.

DEDICATORIA

Este trabajo se lo dedico con mucho cariño a Dios por cuidarme e iluminarme en cada paso de mi vida y a mis padres se los dedico en agradecimiento por todo el esfuerzo y sacrificio que han hecho para darme siempre lo mejor del mundo y sobre todo por el gran amor y confianza que han depositado en mi.

TRIBUNAL DE GRADUACIÓN

Ing. Félix Ramírez
Presidente Tribunal

Ing. Naranjo Sánchez Bertha Alice
Directora de Tesis

Dra. Saad Julia
Vocal Principal

Ing. Mejía Coronel Marco
Vocal Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma, a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

David Carrión Miranda

RESUMEN

El presente trabajo trata de la “Evaluación del sistema de mantenimiento asistido por computadora de una empresa del sector naviero” enfocada a la revisión de políticas, aplicación de controles generales y controles específicos para determinar la integridad, confidencialidad y disponibilidad de la información con el propósito de establecer las falencias y debilidades del sistema, y por ende instituir las respectivas recomendaciones para la mejora continua de esta aplicación.

En esta evaluación se analizó la aplicación se controles generales tales como políticas y procedimientos para la administración de acciones y la toma de decisiones que ayuden y eviten situaciones riesgosas en el manejo del sistema de aplicaciones. En lo que respecta a controles específicos tenemos el control de claves de acceso en diseño, asignación por perfiles y funciones de usuarios, la revisión de controles de validación y control de acceso a principales módulos del sistema.

Este tipo de evaluaciones especiales a sistemas de información contribuyen de manera positiva y efectiva a los objetivos y procedimientos institucionales, ya que por medio de ésta evaluación podemos determinar las debilidades y falencias del sistema y sugerir las mejoras correspondientes

INDICE GENERAL

ABREVIATURAS

IT	Information Technology
PED	Procesamiento Electrónico de datos
SMAC	Sistema de mantenimiento asistido por computadora.
CANOPUS	Control administrativo de partidas presupuestarias.
TI	Tecnología de Información
O/T	Orden de Trabajo
S/T	Solicitud de Trabajo
SRI	Stanford Ressearch Institute
ESCB	Evaluación del sistema caso Base
ITF	Facilidad de Prueba Integrada
SCARF	Archivo de revisión de Auditoría como control del sistema.
SARF	Archivo de revisión de Auditoría por muestreo
COBIT	Objetivos de Control para tecnología de Información.
ISO	Organización Internacional de Estandarización. (Internacional Standards Organization)
SAC	Systems Auditability and Control
IDEA	Interactive Data Extraction and Análisis
CAATS	Técnicas de Auditoría asistido por computadora.
CISA	Auditor Certificado de Sistemas de Información (Certified Informaron Systems Auditor)
ODBC	Open Database Connectivity
RAM	Memoria de acceso aleatorio (Random Access Memory)
DOS	Sistema Operativo de Disco (Disk Operating System)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCION

Durante mucho tiempo la información ha venido teniendo un papel muy relevante dentro del proceso de elección, determinación y decisión, así mismo la aparición de nuevos riesgos de pérdidas y competencia ha introducido la necesidad de establecer medidas de controles y seguridades de información. Toda esta idea de mantener y garantizar la efectividad, integridad, confiabilidad y disponibilidad de información ha incitado al desarrollo y aplicaciones de auditorías de sistemas de información.

La idea principal de este artículo es presentar un modelo de análisis y evaluación de una serie de controles generales y específicos a nivel de aplicaciones y administración del sistema, partiendo de una serie de controles y estándares basados en normas internacionales.

Este º teóricos para la aplicación de controles y técnicas de evaluación del sistema, en su tercera parte encontramos una serie de objetivos de controles expresado por las normas internacionales de tecnología de información y en la cuarta y última parte encontramos la parte práctica de la evaluación del sistema.

Para realizar dicha evaluación (Cuarta parte) nos hemos basado en las fases de estudio preliminar, revisión y evaluación de controles y seguridades, examen detallado de áreas críticas y comunicación de resultados, las cuales son muy similar a un proceso de auditoría. Todas estas fases las iremos explicando en el transcurso de esta tesis.

CAPITULO I

1. ANTECEDENTES

1.1. Evolución del Sistema de información.

La “información” comúnmente llamada amalgama de datos procesados, ha tenido una serie de cambios y evoluciones tanto en la elaboración como en el uso de la misma, es así que en la actualidad a finales de siglo XX la información cumple un papel muy importante y crucial en las actividades cotidianas de la vida humana.

Hoy en día las personas, las familias, las empresas y toda organización en general trabajan dependiendo directamente de la información generada y evaluada. Por ejemplo cuando diariamente leemos los periódicos, los informativos, escuchamos las noticias o nos enteramos por cualquier medio de las novedades existentes, procedemos a evaluar y a estudiar en nuestro ser interior la opción mas acertada para una correcta acción. Así mismo las organizaciones dependen

considerablemente de una veraz, adecuada, estructurada, oportuna y confiable fuente de información debido al entorno cambiante y a los procesos dinámicos que el mundo actual lo exige. Por lo que es cierto, que la globalización, la competitividad, la tecnología, los gustos, las costumbres y la sociedad en general está influyendo de manera directa en el desarrollo de nuevos caminos para poder afrontar los retos de la nueva era.

Es aquí donde nace una nueva revolución de la información hoy bien llamada tecnología de información (TI). Esta Tecnología de Información también conocida como sistema de información es una herramienta importante y esencial para el desempeño y funcionamiento de las actividades cotidianas,"extraen, filtran, comprimen y dan seguimiento a la información crítica del negocio", es tanto así que este tipo de Tecnología de Información cumple un papel importante en la toma de decisiones de los ejecutivos y directores de una organización.

Esta doctrina de implantar tecnología de información se está fortaleciendo y acoplando rápidamente a la cultura organizacional y a las actividades cotidianas de la empresa; pero justo aquí es donde

aparece un nuevo problema, que es evaluar y controlar la información que está siendo procesada.

Al evaluar y controlar la información procesada, efectuamos el seguimiento de todo el entorno humano, tecnológico y flujograma de procesos y procesamientos de datos, que hace que la información llegue a su destino final. De esta manera se están estableciendo varios mecanismos de control y seguridades a niveles primarios y superiores que en un determinado periodo serán evaluadas o auditados para verificar la secuencia general de las procedimientos realizados por estos sistemas, y así mismo realizar seguimientos, para detectar errores, deficiencias en procedimientos, riesgos de sabotaje, fraude o pérdidas económicas que en un momento dado podrán ser de considerable representación económica.

Ahora que ya hemos hablado y entendido más a fondo sobre los Sistemas de Información o Tecnología de Información, nos vamos a enfocar y profundizar directamente en todo lo que se refiere a la evaluación del sistema de información, o particularmente llamada auditoría de sistemas. Para esto procederemos a analizar, explicar y

ampliar brevemente varias definiciones que aclaren directamente lo que vamos a tratar en el presente trabajo.

1.2. Sistema de Información.

Existe una diversidad de sistemas de información tales como los sistemas de información operacional, sistemas de información estratégicos, sistemas gerenciales, entre otros. Estos tipos de sistemas tienen una característica en común que se enmarca en la concentración y disponibilidad de información para acertadas tomas de decisiones

Los sistemas de información operativos son sistemas a niveles de mandos medios. Éstos se enfocan directamente a la alimentación de información de los procesos, procedimientos, actividades y tareas de la compañía en forma diaria y muy detallada, Los sistemas de información estratégicos se orientan a la obtención de metas, operaciones, productos y a la forma de tomar ventaja frente a los competidores. Y, los sistemas de información gerencial están dirigidos a los niveles de alta gerencia para consultar y examinar mediante indicadores y semáforos la situación actual de la organización y establecer una planeación adecuada para el control de las actividades fundamentales de desempeño.

Entonces podemos decir que los sistemas de Información son herramientas para todo nivel de organización, en especial para el nivel Directorio-Administrativo el cual utiliza la información estructurada, oportuna y confiable para una correcta y adecuada toma de decisiones. Este instrumento puede generar muchas ventajas en relación a sus competidores tales como, mayor competitividad, seguridad de información, eficiencia, oportunidad y concentración de información, pero así mismo esta herramienta puede concebir mayores costos por la mala planificación del sistema, inseguridad de información, riesgo de vulnerabilidad, ausencia de controles, pérdidas y fraudes de información en caso de no ser evaluada, monitoreada, actualizada y controlada continuamente.

Como es natural dentro de la organización existen o deben existir medidas de control de los procesos y procedimientos donde intervienen los recursos humanos, tecnológicos y de infraestructuras. Es por eso que se habla del término Control Interno y Control Externo. El control interno generalmente se lo considera como medio que reduce el impacto de la probabilidad de que se produzcan fraudes, errores o malversaciones de información valedera, a esta actividad se la considera como auditoría interna o evaluación dentro de la organización; en cambio los estudios,

evaluaciones y medidas de control diseñados por entes externos a la organización se la considera como auditoría externa, en la cual el auditor externo presta sus servicios profesionales en mutuo acuerdo entre las partes y el establecimiento de un precio por trabajo realizado. Es de aquí que parte la idea principal de evaluar y controlar los medios tecnológicos también llamado tecnología de información, incluyendo los sistemas de información.

Esta tecnología de Información se la evalúa en diferentes aspectos, para los cuales existen programas especiales, específicos y definidos que son desarrolladas por los diferentes tipos de auditorias tales como auditoría de redes informáticas, auditoría de sistemas informáticos, auditoría de las funciones del departamento de informática entre otras.

En este documento expondremos la diferencia entre auditoría informática y auditoría de sistemas informáticos las cuales son claves para el entendimiento del desarrollo de esta tesis.

Durante muchos años los gerentes, directores y las personas en general han confundido la actividad y los objetivos propios de la evaluación o auditoría de sistemas de información con la auditoría informática. Esta

diferencia radica básicamente en el campo de trabajo donde se va a ejecutar la evaluación. Se dice que depende del lugar o campo a trabajar porque la Auditoría de Sistemas de Información o de Sistemas se centra básicamente en el sistema aplicativo o software, en cambio la Auditoria Informática se enfoca directamente al entorno del sistema tales como las funciones del departamento de cómputo, la evaluación de los medios físicos o tangibles y los planes de contingencia.

Desde varios años atrás esta técnica de evaluación se ha venido desarrollando, ampliando e independizando debido al avance y desarrollo tecnológico que actualmente está despuntando. Sin lugar a duda nuestro esfuerzo y sacrificio tendrá como objetivo la maximización de recursos y la disminución de factores negativos que retrazan y complican las actividades diarias de la organización.

Independientemente podemos decir que la auditoria informática es la que tiene por objetivo evaluar los controles del entorno total del área de informática. Este tipo de auditoría evalúa los aspectos y seguridades físicas, y las seguridades lógicas del entorno informático. La auditoria de sistemas informáticos comprende el estudio de todos los aspectos propios del sistema tales como: tablas, relaciones, transacciones, base

de datos, accesos y perfiles. Con el objetivo de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse. Sin embargo esta evaluación requiere la revisión de los controles generales básicos de la operación del sistema o aplicativo.

1.3. ¿Qué busca y provee la auditoría de sistemas?

1.3.1. Objetivos generales de una auditoría de sistemas

En una auditoria de sistemas informáticos encontramos varias definiciones de objetivos que se requieren y se espera de manera general de una evaluación.

- Atender y evaluar las necesidades de los usuarios finales para mejorar e incrementar la satisfacción en la utilización de las mismas
- Evaluar y establecer nuevas directrices de control que provean de seguridad de personal, datos, hardware, software e instalaciones
- Reducir los riesgo de vulnerabilidad o acciones propensas a error
- Reducir la probabilidad de existencia de riesgo de información.

- Adquirir un nivel más alto de control y cultura organizacional, para estar preparado y prevenido en las actividades diarias y en caso de alguna contingencia o emergencia
- Establecer un mejor criterio para invertir o no en tecnología de información adicional.
- Mejorar el entorno informático para sumar esfuerzo para alcanzar y lograr el cumplimiento de los objetivos y planes institucionales.
- Evaluar y establecer medidas de seguridad que provean una adecuada integridad, seguridad, confiabilidad y disponibilidad de la información.
- Fomentar medidas de control mediante recomendaciones.
- Buscar una mejor relación costo-beneficio en la implementación y utilización de los sistemas de información computarizados.

1.3.2. Objetivos específicos.

- Conocer la Situación Actual del Sistema de Información y de las áreas relacionadas
- Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones.
- Identificar el proceso y Flujo de Información de las actividades de mantenimiento de la empresa.

- Evaluar la integridad de datos.
- Evaluar la administración de las claves de accesos a los módulos del sistema.
- Evaluar el plan de contingencia de la aplicación en caso de fallas.
- Evaluar las medidas de seguridad físicas y seguridad lógicas considerando los aspectos de confiabilidad y disponibilidad de la información.

1.4. Justificativos para efectuar una Auditoría de Sistemas.

Entre los motivos o justificativos más relevantes que incita y motiva a la ejecución de una auditoría de sistemas de información en las organizaciones son:

- Detección de posibles fraudes realizados por el computador.
- Falta de controles y validaciones que garanticen la veracidad e integridad de la información.
- Mejorar la calidad de control de los recursos informáticos.
- Desconocimiento del sistema por parte de los directivos.
- Aumento de quejas y reclamos por fallas del sistema por parte de los usuarios del sistema.

- Aumento del presupuesto del departamento de mantenimiento del sistema.
- Falta de políticas y objetivos de seguridad física y lógica.
- Falta de una adecuada planificación de los trabajos del departamento de sistemas.
- Falta de documentación y respaldo de información de los procedimientos y tareas ejecutas en el sistema.

1.5. Control interno informático en las organizaciones.

El control interno en las organizaciones es fundamental ya que por medio de este se reduce cualquier cantidad de material y procedimientos improductivos y se gestiona de manera más eficiente los recursos materiales, tecnológicos, humanos y financieros. Se dice que el control interno parte de un adecuado establecimiento de objetivos organizacionales y de una administración efectiva por objetivos.

Estos controles se los consideran como medidas de seguridades o disposiciones metódicas, para establecer y delimitar los niveles de accesos y permisos cuyo objetivo es salvaguardar las instalaciones de la organización y sus derivados; también nos referimos a las normas,

reglamentos y directrices que rigen y regularizan las funciones, actitudes y acciones del personal.

Con el transcurso del tiempo los ideales de controlar, evitar siniestros y riesgos han incentivado al desarrollo de planes debidamente elaborados y sustentados los cuales se identifican como sistemas de control Interno el cual comprende una serie de procesos y funciones basado en principios, reglas y normas para establecer y ejercer procedimientos efectivos y eficaces minimizando las debilidades, reduciendo los riesgos e incrementando y desarrollando las fortalezas y oportunidades.

Los controles informáticos son un subconjunto o parte del control integral de la organización sólo que este es enfocado al área de sistemas y procedimientos computacionales. Así como habíamos mencionado en el párrafo anterior, el control interno informático comprende un plan de organización y la totalidad de los métodos y procedimientos que en forma ordenada se aplican al área de cómputo para asegurar la protección de todos sus recursos tecnológicos e informáticos, para la obtención de información correcta, segura y oportuna, adhesión del personal a los objetivos y políticas debidamente predefinidos por la dirección.

Este capítulo nos ha explicado y enseñado varias interpretaciones de los factores más relevantes para el buen entendimiento de la auditoría de sistemas. Hemos tratado desde el Origen de la información, el desarrollo de sistemas de información hasta la necesidad de controlar dichos datos procesados mediante las auditorías y evaluaciones de sistemas informáticos. En el siguiente capítulo trataremos sobre la diversidad de tipos de controles que vamos aplicar en nuestra evaluación al sistema y una serie de definiciones que enriquecerán nuestro entendimiento y conocimiento de la auditoría de sistemas.

CAPITULO II

2. MARCO TEÓRICO

En este capítulo hablaremos sobre la evaluación del sistema y la diversidad de controles físicos y lógicos que utilizaremos en el ejercicio práctico. También trataremos la variedad de técnicas para seleccionar y monitorear transacciones para probar controles de aplicaciones en producción, para realizar exámenes de archivos y técnicas para examinar programas de aplicación. Adicionalmente explicaremos brevemente la sistemática de una auditoría de sistemas, mostraremos una gama de conceptos y estándares que ampliarán los términos que regularizan los sistemas de información.

2.1. Evaluación del sistema y su importancia.

La evaluación de sistema comprende la revisión completa o parcial de todos los controles existentes, dependiendo del alcance y objetivo de la auditoría. Como hemos visto en los párrafos anteriores, la evaluación del

sistema es realizada para evitar deficiencias, descontentos, pérdidas de recursos y fuga de información valedera.

Pero lo más relevante a tratar en el transcurso de este capítulo es tener muy en cuenta la existencia de controles adecuados que permitan filtrar todo tipo de acción, residuos o errores que puedan alterar la información de la compañía. Para esto hemos revisado la definición y hemos procedido a explicar en qué consisten los controles y cuáles son los tipos de controles generales y lógicos.

Partiendo de lo más importante podemos definir a los controles como medidas de seguridad o disposiciones metódicas que se establecen para delimitar los niveles de accesos y permisos. Dentro de estos se encuentran las normas, reglamentos y directrices que rigen y regularizan las funciones, actitudes y acciones del personal y la tecnología de información. El objetivo principal es salvaguardar las instalaciones de la organización y sus derivados para mejorar la eficiencia, eficacia, economía y productividad de las operaciones.

Características de los controles

Para desarrollar y establecer controles en la organización se debe tomar en cuenta las siguientes características que ayudarán a mantener un adecuado seguimiento de actividades.

Efectividad.

Enfocado al logro de las metas y objetivos

Eficiencia.

Enfocado a la realización de ejercicio en forma óptima y oportuna, es decir hacer las cosas bien desde el principio hasta el fin para lograr y alcanzar las metas y objetivos deseados.

Economía.

Enfocado a la evaluación de resultados y a la ejecución de las actividades mediante la reducción y utilización de costos más bajos.

El establecimiento de controles nace de la necesidad de poseer medidas de seguridad que mitiguen los riesgos de fraude y errores en los

procesos internos y externos de la empresa. Estas medidas de seguridad buscan conseguir una eficiente y efectiva Integridad, confidencialidad, y disponibilidad de la información. Por dicha razón debemos establecer y monitorear continuamente adecuados controles para la información.

Aquí podemos encontrar una explicación breve de la importancia y alcance de cada característica que se desea obtener con la aplicación de controles y seguridades.

Disponibilidad

Al referirnos a la disponibilidad de la información nos enfocamos al grado de alistamiento que posee la información para poder ser usada en cualquier tiempo determinado. Hay que tomar en cuenta que esta información esté disponible para todo personal que tenga definido un acceso predeterminado.

Integridad

La integridad de la Información es una de las cualidades y exigencia que busca la auditoría de sistemas. Consiste en la disponibilidad de la información en forma completa, sin cambios, alteraciones o manipulación

de datos, es decir en la forma natural en que fue o debió ser ingresada al sistema de información.

Confidencialidad

La confidencialidad es una de las características que debe poseer la información. Consiste en el carácter de reservado, secreto o no disponible. Para establecer acceso a esta información confidencial se autorizará mediante los controles a niveles de usuarios, perfil o rol y privilegios para con la información.

Hemos definido las tres características más importantes que la información debe poseer. Entonces podemos decir que si la información cumple con estos requisitos básicos, ésta será confiable en un gran porcentaje.

2.1.1. Clasificación general de los Controles.

Preventivos

Los controles preventivos son los que se anticipan a una acción ilícita o negativa, impidiendo que esta se realice o evitan el acceso no

autorizado a los sistemas. Este control no reduce en un 100% el riesgo de manipulación de información, pero si mitiga la probabilidad de vulnerabilidad de la misma.

Detectivos

Los controles Detectivos luego de ser aplicados identifican o detectan el error luego de ser realizada, básicamente funcionan como una pista de Auditoría y constituyen una información valiosa para el auditor ya que por medio de estos, él evalúa la efectividad de los controles preventivos. Hay que tomar en cuenta que este tipo de control no elimina el riesgo de fraude.

Correctivos

Los controles Correctivos básicamente constituyen una ayuda a la investigación y corrección de errores, fallos o fraudes. Se considera que este tipo de control debe estar ligado o precedido de los controles Detectivos ya que este va a indicarnos que tan eficientes y eficaz es el control correctivo.

2.1.2. Tipos de controles físicos y lógicos.

Son parámetros y directrices que regularizan el comportamiento humano y manejo de material enfocado a los bienes muebles e inmuebles de un centro de cómputo o sistema; Estos controles juegan un papel importante en la existencia y mantenimiento de los equipos y sistemas en general.

Entre los tipos de controles físicos y lógicos más importantes que utilizaremos en nuestra evaluación encontramos los siguientes:

Autenticidad.

Este tipo de control se enfoca principalmente en la legalidad de la identidad del acceso.

Encriptación

Es un medio de seguridad, el cual consiste en disfrazar o codificar mediante algoritmos las palabras y letras claves de los accesos, se lo presenta mediante varios signos, símbolos o asteriscos concatenados. El encriptamiento es considerado como una

herramienta efectiva para disminuir los riegos en el manejo o uso de tecnología de información.

Exactitud.

Este tipo de control guarda relación a los filtros, lo cuales no permiten recibir basura o información errónea, siempre guarda veracidad y coherencia de la información

Redundancia.

Este control se encarga de impedir la duplicación de información.

Privacidad.

Este control se lo obtiene con una política de confidencialidad. Garantiza y establece mecanismos que salvaguarden la generación y modificación de información.

Existencia.

Este control nos garantiza la disponibilidad de los datos o información en el momento y lugar deseado. Es un tipo de control de

uso común ya que por lo general se conoce que se almacena en una base de datos.

Protección de activos.

Básicamente este control está dirigido a proteger, cuidar y salvaguardar los activos financieros y no financieros.

TABLA 1
EJEMPLOS DE CONTROLES

Encriptación	Hasp Hardware key
Autenticidad	Número o código de identidad definido.
Exactitud	Validación de Campos Mensajes o Semáforos
Redundancia	Verificación de secuencias Filtro por registros
Privacidad	Password Encriptación
Existencia	Backup Historial Bitácora de registro
Protección de activos	Políticas Planes de contingencia Extintores Cámara de humo

2.1.3. Control automático o lógico

2.1.3.1. Claves y contraseñas.

Los controles de claves de acceso son importantes para evitar la vulnerabilidad del sistema.

Las claves o contraseñas en un sistema son generalmente de tipo automático, se las considera como claves de identificación ya que es la forma de expresar nuestra identidad y nuestro perfil con el propósito de obtener un permiso o acceso a fuentes confidenciales.

Desde el punto de vista del control y administración de las claves y usuarios, se debe valorar y tomar en cuenta factores importantes para el establecimiento de claves o password, como:

- Una clave (password y user) para cada usuario.
- Actualización y/o cambios de claves de acceso periódicamente.
- Combinación alfanumérica en clave de acceso, se recomienda que estas claves sean de letras y números.

- Las claves deben ser conocidas sólo y exclusivamente por los usuarios autorizados.
- Restringir el acceso a los datos en el sistema de acuerdo a las funciones de cada persona.

Como medida de seguridad los jefes, administradores y los empleados debemos acostumbrarnos a cambiar continuamente nuestros accesos para evitar problemas y pérdidas irreparables.

Características de las claves al momento de definirlas

Para definir las claves a todos los usuarios se deberá tomar en cuenta que las claves deben ser:

- Individuales
- Confidenciales
- No Significativas

Individuales

Esta clave es personal, no debe ser transmitida, ni divulgada. Cada persona es responsable de su clave.

Confidenciales

Son claves de carácter más formal y restringida, aquí se maneja información reservada, la cual no debe ser comentada.

No significativas

Son claves que no deben estar integrados por números secuénciales, ni nombres, ni fechas que sean de fácil deducción.

2.1.3.2. Técnicas de control

Identificación de transacciones

Todas las acciones, operaciones o transacciones que se realicen mediante un computador o medio tecnológico deben estar debidamente identificadas para efecto de control interno. Esta

identificación puede realizarse de diferentes maneras, tales como números de secuencia, series, o códigos de transacciones.

Por ejemplo el número secuencial (lógico) de las Órdenes de Trabajo (O/T), las Solicitudes de Trabajo (S/T), Las solicitudes de herramientas, las facturas generadas, los reportes estadísticos.

Log de secuencia

Un Log interno que controle y haga seguimiento al Log de secuencia

Por ejemplo un Log que indique o cuente las veces que han accedido a las órdenes de Trabajo.

Identificación del usuario

Este control verifica la existencia de un identificador o código de seguridad por usuario, permitiendo y restringiendo el acceso de acuerdo a la necesidad del sistema, transacción y al perfil de usuario.

Número de identificación de los paquetes de documentos fuente

Este control se enfoca a que cada proceso Batch debería aplicar como norma de control interno una enumeración a cada paquete de datos en forma secuencial para evitar riesgo de pérdida de los datos.

Este tipo de control podría trabajar a la par con el Log de secuencia para comparar los datos o registros y detectar alguna inconsistencia.

Log de errores

Este tipo de control es muy importante ya que sirve como pista de auditoría el cual registra e identifica todos los errores que se presentan en el sistema y a su vez ayuda para las futuras correcciones.

Continuidad de los procesos

Este control verifica la existencia de adecuados procedimientos de respaldo en caso de caídas parciales o totales del sistema, Por ejemplo los servidores o computadores alternos, los

convenios con otros centros del departamento de procesamiento electrónico de datos (PED) que puedan ser compatibles con Hardware y Software.

Tabla de seguridad

Este control consiste en la existencia de una tabla o archivo donde se registre el historial y la secuencia de direcciones específicas de terminales para controlar las acciones de los usuarios y el acceso a archivos confidenciales.

Encriptación de los datos

Este tipo de control es una técnica muy efectiva ya que enmascara o codifica las claves y contraseñas de tal modo que impide que tengan entendimiento de estas.

Código de transacciones.

Este control consiste en que cada transacción que se somete a un procesamiento debe poseer un identificador único esto se lo conoce como código de transacción.

Rechazo de transacciones inconsistentes

Este control consiste en que el departamento de procesamiento electrónico de datos (PED) debe poseer un archivo ordenado y en forma secuencial de las transacciones inconsistentes. Todas estas transacciones inconsistentes deben someterse a un riguroso estudio para efecto de correcciones oportunas.

Validación de datos

Este control busca que los datos que sean ingresados al sistema puedan ser estandarizados y depurados para evitar inconsistencias de información en el sistema. Es por eso que los datos se someten a validaciones completas antes de procesarla en el sistema.

Existe una diversidad de controles de validación pero para efecto de nuestra tesis evaluaremos los controles de validación referentes a:

- Contar los campos de un registro y comparar el resultado con un número predeterminado.
- Verificar la razonabilidad de los datos de entrada a ciertos límites pre-establecidos
- Verificar la composición de los campos numéricos y alfabéticos.
- Verificar la completitud de los datos en los registros para evitar que haya espacios en blanco cuando no debe haberlos.
- Verificar la secuencia u orden de las transacciones de entrada a procesos.

Recuperación de archivos

Este control se enfoca a la obtención de respaldos o copia de manera continua de los archivos maestros para que en caso de pérdida o daños se los pueda recobrar de forma inmediata.

Clave de seguridad

Este control consiste en la creación y aplicación de claves de seguridad que impidan el ingreso o acceso no autorizado a determinadas áreas e información crítica.

Dígito auto verificador

Consiste en un algoritmo mediante el cual una serie de operaciones entre dígitos genera como resultado otro valor el mismo que va servir para verificar la veracidad de las claves.

Utilizar software de seguridad en los microcomputadores

Este tipo de clave o control es muy importante, pero también costoso ya que depende o funciona con la intervención de un sistema de control, el cual monitorea, recepta, proporciona los permisos o accesos previamente programados.

2.1.3.3. Control Administrativo de procesamiento de datos

Los controles administrativos de procesamiento de datos son de gran relevancia ya que estos son lo que van a delimitar y

establecer patrones en la forma de manejar recursos, tomar decisiones, ejecutar tareas, prevenir riesgo, dar mayor seguridad y por ende garantizar una adecuada administración de todos los aspectos referentes a tecnologías de información. Estos tipos de controles los podemos clasificar de la siguiente manera:

1. Controles de Preinstalación
2. Controles de Organización y Planificación
3. Controles de Sistemas en Desarrollo y Producción
4. Controles de Procesamiento
5. Controles de Operación
6. Controles de uso de Microcomputadores

1.- Controles de Preinstalación

El objetivo principal es adquirir de manera acertada los equipos de cómputo previo a una investigación a fondo, también es la de garantizar la selección y compra de equipos y sistemas adecuados de computación y a la vez elaborar un plan de actividades previo a la instalación de estos equipos.

2.- Controles de Organización y Planificación.

Este se encarga de la supervisión y control de todas las actividades que tiene que ver directamente con las funciones y responsabilidades del área del (PED) procesamiento electrónico de datos y a su vez del seguimiento de una adecuada organización y planificación de las tareas encomendadas.

3.- Controles de Sistemas en Desarrollo y Producción

Este consiste en demostrar que el sistema de información desarrollado por la empresa representa la mejor opción desde el punto de vista costo-beneficio. Proporciona información en forma oportuna y eficiente, que se ha desarrollado bajo un proceso planificado y se encuentra debidamente documentado. En fin, determinar si es más conveniente comprar un sistema o realizar un sistema a la medida de la empresa.

Así mismo los controles de sistemas en producción buscan el establecimiento de controles adecuados para el manejo, distribución, administración y mantenimiento del sistema. Para

esto deben estar debidamente documentados y actualizados los siguientes documentos:

- Diagrama de Bloques
- Diagrama de lógica del personal
- Manuales de usuarios
- Manuales del administrador

Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones.

4.- Controles de Procesamiento.

Los controles de Procesamiento son los que vigilan todo el proceso de información, (input-output) desde la entrada de información al sistema hasta la salida o resultado.

El objetivo primordial de este control es poseer una fuente de información veraz, confiable y oportuna lista para analizarla y tomar decisiones.

Entre los objetivos particulares tenemos:

- El ingreso de todos los datos al sistema de información el cual nos garantice que serán procesados de manera exitosa y exacta.
- Disponer de resultado o información resolutoria para los altos directivos de la organización, para que ellos tomen las decisiones más acertadas.
- Disponer de la información resolutoria para que lo resultados se entreguen a los usuarios en forma oportuna y en buenas condiciones.

5.- Controles de Operación.

Este control se enfoca directamente en el área de operaciones, específicamente en el centro de cómputo y los terminales de trabajo es decir donde se encuentren los procesadores principales, bases de datos, centros administrativos de los recursos informáticos.

Entre los objetivos más importantes de este control son:

- Mantener de manera óptima, segura y con alto grado de alistamiento todos los sistemas y equipos para cumplir con los objetivos organizacionales establecidos.
- Mantener un alto grado de seguridad contra riesgo de fraude, sabotaje, daños físicos, o daños producidos por la naturaleza.

6.- Controles de uso de Microcomputadores.

Este tipo de control se lo considera el más molestoso para los usuarios finales y a la vez el más complicado debido a la variedad, cantidad, y disponibilidad a otras personas.

Entre los objetivos principales tenemos:

- Se debe estandarizar los equipo de cómputo, para un mejor monitoreo, mantenimiento y adquisición de repuesto en el caso que se necesite.
- Mantener todas las computadoras con los respectivos software, antivirus.
- Mantener al día las actualizaciones de los Sistemas Operativos, Antivirus, software en general.

- Establecer Políticas y Normas de régimen cultural para el correcto manejo de los microcomputadores.

2.2. Técnicas de auditoría informática: Aplicaciones en producción.

Existen algunas técnicas para auditar aplicaciones en producción, según los lineamientos del Stanford Ressearch Institute (SRI) que es un Instituto de Investigación estadounidense para realizar innovaciones en tecnología de información, comunicaciones, la ingeniería, productos farmacéuticos, química, la física, la educación, la salud, y el desarrollo económico. Estas técnicas son:

- Técnicas administrativas
- Técnicas para probar controles de aplicaciones en producción
- Técnicas para seleccionar y monitorear transacciones
- Técnicas para el examen de archivos
- Técnicas para examinar programas de aplicación

Estas Técnicas son similares a las CAATs (Computer Assited audit. Techniques), que en español significa Técnicas de auditoría asistido por computadoras (TAACs). Según SAP 1009 (Statement of Auditing Practice) los define como programas de computadoras y datos que el

auditor usa como parte de los procedimientos de auditoría para procesar datos de significancia en un sistema de información.

2.2.1. Técnicas administrativas.

Para realizar una auditoria de aplicaciones en producción las técnicas Administrativas se dividen en 2 categorías:

1. Técnicas para establecer el orden de prioridades en el auditaje de aplicaciones en producción.

2. Técnicas para operacionalizar la función de auditoria de aplicaciones en producción.

2.2.1.1. Técnicas para establecer el orden de prioridad en el auditaje de aplicaciones en producción.

Dentro de las cuales se conocen:

- **Selección de áreas de auditoria**

Esta técnica es aplicable en empresas multinacionales o empresas con múltiples sucursales y que cuentan con un sistema integrado ya que facilita la determinación de las áreas auditables en orden prioritario con respecto a la información

clave obtenida a través de un programa de selección de información en las aplicaciones utilizadas en la empresa.

- **Simulación – modelaje**

Este es muy similar a la de selección de áreas de auditoría. Este tipo de análisis se basa en la utilización de razones o índices financieras para evaluar el incremento o decremento de las cuentas contables o áreas financieras en términos de ingresos, egresos y gastos en períodos determinados para determinar el nivel de crecimiento organizacional.

Compara estimaciones de valores esperados con valores actuales con el objeto de identificar desfases significativos lógicamente relacionados, en materia financiera (1).

---

(1) Pinilla Forero José Dagoberto, Auditoría Informática Aplicaciones en Producción, Ediciones ECOE 1997, Pág. 33

- **Sistema de puntajes – scoring**

Esta técnica se realiza manualmente, determina puntajes o valores numéricos a las características claves de los sistemas, evaluando las aplicaciones para calificarlas de acuerdo al criterio de la auditoria y comparar los resultados, teniendo en cuenta los riesgos potenciales que permitan obtener un alto grado de confiabilidad de la información.

Para efecto de nuestra evaluación aplicaremos el Sistema de Puntajes-scoring, para establecer el orden de auditaje.

2.2.1.2. Técnicas para operacionalizar la función de auditoría de aplicaciones en producción.

- **Software de auditoria multisitio**

Esta técnica se aplica en organizaciones multinacionales que tienen diferentes centros de procesamiento electrónico de datos (PED). Consiste en instalar un programa o grupo de programas de auditoria en varios centros de PED para que sean utilizados por los auditores regionales.

- **Centros de competencia**

Esta técnica es utilizada en organizaciones que tienen algunas sucursales y cuentan con una matriz donde se centraliza la recepción de archivos de datos para utilizar un programa de auditoria. En este lugar los auditores realizan las respectivas evaluaciones, análisis e informes los cuales son enviados a las sucursales para la respectiva toma de decisiones. Es una técnica que funciona con un procedimiento inverso al del Software de auditoria multisitio.

Para efecto de nuestra evaluación y debido a las condiciones de la empresa aplicaremos la Técnica de Centros de Competencia para operacionalizar la función de auditoria de aplicaciones en producción con programas manuales de auditorías.

2.2.2. Técnicas para probar controles de aplicaciones en producción.

Dentro de este tipo de pruebas se encuentran las siguientes:

1. Método de datos de prueba

2. Evaluación del sistema de caso base
3. Operación paralela
4. Facilidad de prueba integrada
5. Simulación paralela
6. Método de datos de prueba

- **Método de datos de prueba**

Esta técnica es utilizada normalmente por los analistas-programadores antes de enviar los programas a producción. Consiste en ingresar un conjunto de datos para que sean verificados a través del procesamiento del sistema, esto sirve para detectar la entrega de resultados inconsistentes o no válidos, analizando las posibles combinaciones de archivos maestros, valores y lógica de procesamiento.

- **Evaluación del sistema de caso base (ESCB)**

Esta técnica también se utiliza para comprobar la lógica de los programas y precisión de cálculos pero con la cooperación de los usuarios, auditores y personal de sistemas por esta razón se vuelve más completa que la técnica de los datos de prueba. Se utiliza para

validar los sistemas antes de entrar a producción y para las auditorias a aplicaciones en producción.

- **Operación paralela**

Esta técnica es utilizada para probar nuevos sistemas y verificar su exactitud. Consiste en probar los mismos datos entre el sistema actual y el nuevo, el sistema antiguo no se desecha hasta que el sistema nuevo dé los resultados esperados.

- **Facilidad de prueba integrada (ITF)**

Es una técnica para probar los sistemas de aplicación en producción con datos reales evaluándolo en un ambiente normal de producción. Se procesan las transacciones de prueba de una entidad ficticia junto con las transacciones reales de producción. Por esta razón se llama prueba integrada.

- **Simulación en paralelo**

Esta técnica consiste en crear una rutina de uno o varios módulos del sistema a auditar. De esta forma las rutinas leen iguales datos de

entrada que los programas de aplicación, utilizan los mismos archivos y tratan de producir idénticos resultados que se someten a evaluaciones y comparaciones para determinar discrepancias o errores.

Para efecto de nuestra evaluación aplicaremos la técnica de facilidad de Prueba integrada (ITF) debido a que se logró realizar las pruebas con datos reales en el sistema normal de producción.

2.2.3. Técnicas para seleccionar y monitorear transacciones.

Estas técnicas son las más relevantes dentro del proceso de evaluación de un sistema. Estas técnicas son las que definen la forma, manera, cantidad y calidad de capturar una muestra del sistema de información para ser evaluada.

Generalmente el auditor utiliza pruebas de rangos, técnicas de muestreo y condiciones de error. Esto lo hace en base a criterio y experiencia profesional.

Dentro de las técnicas más importante tenemos:

1. Selección de transacciones de entrada.

2. Archivo de revisión de auditoría como control del sistema (SCARF).
3. Archivo de revisión de auditoría por muestreo (SARF).
4. Registros extendidos.

- **Selección de transacciones de entrada.**

Esta técnica se la ejecuta mediante un software de auditoría, que es independiente al sistema en producción. Consiste en seleccionar y separar datos de entrada que son parte de las aplicaciones. Y se las hace en base al criterio profesional y experimentado del auditor. Estas transacciones separadas son sometidas a un riguroso examen establecido por una adecuada planificación del auditor.

Cabe mencionar que esta técnica es muy segura ya que no existe el riesgo de la alteración de los datos del sistema de información.

- **Archivo de revisión de auditoría como control del sistema (SCARF).**

Esta técnica consiste en incorporar aplicaciones de auditoría en el sistema de producción para que ejecute distintos tipo de supervisiones y monitoreo de transacciones en forma permanente.

La aplicación de este software se la conoce como subrutina. Una vez que esta subrutina cargue las transacciones se procederá a la selección mediante muestreos previamente definidos por el auditor.

- **Archivo de revisión de auditoría por muestreo (SARF).**

Esta técnica (SARF) es muy similar a la anterior (SCARF), lo único que cambia es la selección de las transacciones mediante el software ya que no son en forma automática y no son predefinidas, sino que la selección de la muestra se la realiza al azar. Su objetivo es capturar archivos representativos para proceder a evaluarlos, esta técnica es muy utilizada por los auditores externos ya que permite analizar las transacciones y seleccionar los archivos en forma aleatoria o apoyándose con el muestreo estadístico.

Para realizar este tipo de muestra se requiere de un analista de sistema o programador para que preparen los módulos a decisión del auditor.

- **Registros extendidos.**

Esta técnica consiste en la aplicación de pequeñas rutinas que permiten recoger todos los datos que han afectado una transacción. Estas rutinas son conocidas como pistas de auditorías completas que son instaladas por el personal de sistema y programación al momento de preparar el sistema en producción, estos tipos de registros permiten tener un historial de todas las actividades, secuencias y/o fallos del sistema.

La técnica que utilizaremos en el transcurso de este proyecto será el "Archivo de revisión de auditoría por muestreo (SARF) y registros expandibles."

2.2.4. Técnicas para el examen de archivos.

Dentro de las técnicas más importante para el examen de archivos, tenemos las siguientes:

1. Programas Generalizado de auditoría
2. Programa de utilería o de servicios
3. Programa de auditoría a la Medida.
4. Vaciado de archivos.

- **Programas Generalizado de auditoría**

Esta técnica para evaluar archivos es muy general, se basa en procesos y procedimientos estándar para evaluar e investigar las deficiencias y falencias, ya que

La esencia del examen se concreta en actividades, tales, como: clasificar, resumir, extraer, insertar, mezclar (intercalar), compartir, calcular, seleccionar, evaluar y otras actividades similares (2).

Este tipo de programa no altera o modifica los datos evaluados.

(2) Pinilla Forero José Dagoberto, Auditoría Informática Aplicaciones en Producción, Ediciones ECOE 1997, Pág. 56

- **Programa de utilería o de servicios**

La técnica Programa de utilería o de servicios consiste en un software que muchas de las instalaciones de procesamiento electrónico de datos (PED) lo poseen como parte de sus herramientas para CLASIFICAR, SELECCIONAR, INSERTAR, COPIAR, FUSIONAR, IMPRIMIR, BUSCAR, INTERCALAR. En la actualidad la mayoría de los auditores utilizan herramientas o utilitarios como parte de su apoyo informático que cumplen y realizan funciones iguales a las del PED, pero así mismo a este tipo de utilitarios o herramientas hay que ponerle mucho control debido a que muchos de estos utilitarios pueden hacer gran cantidad de modificaciones y no dejar rastro, pero así mismo existen otros programas que no alteran los datos de prueba.

- **Programa de auditoría a la Medida.**

Son rutinas diseñadas para evaluar los procesos sistematizados de la empresa. Se dividen en dos tipos, la primera es diseñada por el departamento de programación o sistema de la empresa para monitorear o diseñar medidas de control y el segundo es realizado

por el mismo auditor. Este programa es diseñado a la necesidad de la empresa y la disponibilidad del auditor.

- **Vaciado de archivos.**

Esta técnica permite al auditor examinar el contenido de los archivos mediante una copia o vaciado de los datos a un medio de almacenamiento secundario, este vaciado se lo puede realizar en cualquier medio de almacenamiento computarizado. Generalmente el auditor realiza transacciones para hacerle el respectivo seguimiento para luego verificar la secuencia y resultado lógico en los archivos maestros.

La técnica que utilizaremos para el examen de archivo en el transcurso de este proyecto será el “Programa de utilería o de servicios.” Por efecto de cantidad de datos, tiempo de análisis, manipulación de información y para que las pruebas sean neutrales, confiables e efectivas, se procederá a la utilización de un software de Auditoría denominado IDEA para DOS versión 5.0 (Interactive Data Extraction and Analysis). Este software es reconocido a nivel internacional por el Instituto Canadiense de Contadores Certificados para el uso de auditorías y evaluación de sistemas.

2.2.5. Técnicas para examinar programas de aplicación.

Se define a los programas de aplicación como aquellos que siendo estandarizados y/o a la medida tienen como objetivo resolver problemas usando el computador.

1. Snapshot (Imagen instantánea)
2. Mapping (Mapeo)
3. Tracing (Rastreo)
4. Flujogramas DE CONTROL (Control Flowcharting)
5. Comparaciones de Códigos.
6. Control de bytes.
7. Análisis de la lógica de los programas.

- **Snapshot (Imagen instantánea)**

Es la técnica que permite una copia o fotografía de la memoria del computador que contiene todos los elementos de un proceso de decisión en el momento de su ejecución. El SNAPSHOT es un programa utilitario que opera en sistema de producciones en los sistemas Interactivos y de proceso Batch. Esta técnica describe los problemas de programas en las computadoras, además proporciona

un método para examinar la memoria de la computadora durante el procesamiento.

- **Mapping (Mapeo)**

> ***Es una técnica ejecutada por una herramienta de medición de software que analiza un programa de computador, durante su ejecución para determinar si son utilizadas todas las instrucciones del programa (3).***

Posee un contador de números de veces que es ejecutada cada instrucción y mide el tiempo consumido de cada instrucción del computador. Esta técnica es la que se encarga de aislar o deshabilitar funciones que pudieran haber sido ingresada con propósitos ilícitos, además identifica instrucciones no utilizadas y ejecuta procedimiento de depuración de software.

---

(3) Pinilla Forero José Dagoberto, Auditoría Informática Aplicaciones en Producción, Ediciones ECOE 1997, Pág. 74.

- **Tracing (Rastreo)**

Esta técnica se muestra en un lenguaje de programación y permite realizar un seguimiento ya que identifica y muestra en forma secuencial las instrucciones que han sido ejecutadas, como resultado nos arroja un listado de todas las transacciones efectuadas que servirá como evidencia de todas las acciones y transacciones realizadas para el auditor.

- **Flujogramas DE CONTROL (Control Flowcharting)**

Este tipo de técnica permite evaluar de forma integral al sistema, a su vez permite relacionar e interpretar los controles lógicos con los controles manuales y realizar un seguimiento para verificar la operación de los mismos (controles).

- **Comparación de códigos.**

Sirve para comparar dos tipos de versiones de un mismo programa, también para revisar la copia del sistema que va ser entregado al auditor para que lo evalúe o para revisar las secuencias de las actualizaciones de un sistema; esto permite verificar los procedimientos de mantenimiento y cambios de los programas. Esta

técnica no proporciona evidencia de la confiabilidad de los archivos de datos ni sobre la eficiencia y eficacia de los programas. La ejecución de éste programa se lo puede realizar en código fuente y/o código objeto.

- **Control de bytes.**

Es una de los más seguros y adoptados por los auditores debido a que se somete al conteo de números de Bytes para detectar por medio de este, variaciones o alteraciones del sistema no autorizadas. ***"Este control ofrece un alto grado de confidencialidad en materia de integridad y de inviolabilidad (4)"***

---

(4) Pinilla Forero José Dagoberto, Auditoría Informática Aplicaciones en Producción, Ediciones ECOE 1997, Pág. 81.

Para poder alterar el sistema sin ser detectado deberían borrar una cantidad lógica de aplicaciones para reducir los bits y luego proceder a ingresar instrucciones fraudulentas, que reemplazarían estos bits, pero aún así es casi imposible hacerlo, ya que el sistema debe tener la misma secuencia lógica y aplicaciones y también porque sería difícilmente alterar un sistema cuando existe un eficiente y efectivo control interno informático.

Por dicha razón se dice que este sistema garantiza un alto grado de confiabilidad de los programas y de la inalteración de su contenido.

- **Análisis de la lógica de los programas.**

Esta nos expresa que si los controles de los programas están funcionando de forma eficiente y efectiva y que los procesos de los datos se encuentran de acuerdo a las políticas establecidas basta con la revisión profunda de la lógica del sistema mediante varios de los manuales y documentos del sistema tales como: una narración descriptiva y detallada del programa, el diagrama de la lógica de los programas detallados y los listados de los programas.

Ahora que, para que el auditor pueda analizar él sistema en forma lógica debe poseer sólidos conocimientos de computación, como por ejemplo:

- ✓ Conocimiento suficiente del lenguaje en que están escritos los programas con el fin de alcanzar los objetivos de la auditoria dentro de un tiempo razonable.

- ✓ Un alto grado de familiaridad con los sistemas totales que se están examinando, con el fin de entender la relación existente entre los varios módulos de programas y los programas principales, así como la relación de todos los programas con el sistema total.

- ✓ Y que el auditor se encuentre satisfecho de los controles que se aplicaron para mantener en custodia y actualización los manuales del sistema.

Como control general de los sistemas o aplicativos instalados en los computadores usuarios del sistema, aplicaremos la técnica Control de bytes.

2.3. Metodología de una Auditoría de Sistemas

2.3.1. Aspectos Metodológicos

Actualmente contamos con varías metodologías las cuales nos sirven como guía en el desarrollo de una evaluación de sistema. El presente trabajo basará su estudio en la sistemática de las 4 fases de un proceso de revisión las mismas que son principales y fundamentales en una auditoria de sistemas.

Estas fases son las siguientes:

- ✓ Estudio preliminar
- ✓ Revisión y evaluación de controles y seguridades
- ✓ Examen detallado de áreas criticas
- ✓ Comunicación de resultados.

Estudio preliminar.- El estudio preliminar es parte vital en un proceso de investigación ya que por medio de esta fase se tendrá una idea general en lo que respecta a la Unidad informática la cual vamos a auditar. En este ciclo se define el grupo de trabajo, se realiza el programa de auditoria, se efectúan visitas a la unidad

correspondiente con el fin de conocer mayores detalles de la misma, como también se elaboran los cuestionarios oportunos que servirán para obtener información detallada lo que permitirá evaluar preliminarmente el control interno, los manuales de políticas, reglamentos, etcétera . En esta fase se elabora el plan de actividades a realizar.

Revisión y evaluación de controles y seguridades.- Abarca la revisión de los diferentes diagramas de flujo de procesos como la realización de pruebas de cumplimiento de las seguridades informáticas existentes, la revisión de aplicaciones de las áreas criticas, la revisión de procesos históricos (backups), la revisión de documentación y archivos, entre otras actividades de importancia que nos permitan tener una idea más clara del entorno.

Examen detallado de áreas criticas.- Con las fases anteriormente detalladas el auditor determina las áreas críticas existentes y sobre éstas realiza un estudio y análisis de fondo el mismo que permitirá definir de manera concreta el grupo de trabajo y su distribución de carga, como también le permitirá establecer los motivos, objetivos, alcance, los recursos que usará, definirá la metodología de trabajo y

la duración de la auditoria. Una vez realizado el proceso correspondiente, presentará el plan de trabajo y analizará detalladamente cada hallazgo encontrado.

Comunicación de resultados.- Una vez efectuadas las fases anteriores se procede a elaborar un borrador del informe, éste será estudiado por parte de las autoridades de la empresa con el fin de llegar a confeccionar un informe final y definitivo, este debe ser presentado de manera esquemática, puede ser en forma de matriz, cuadros o mediante una redacción sencilla pero concreta donde se detalle de manera explícita los hallazgos encontrados con los respectivos efectos y las debidas recomendaciones por parte de la Auditoria..

El informe a elaborar debe contener los siguientes detalles:

1. Antecedentes
2. Objetivos de la Auditoría
3. Resultados de la Evaluación
    - Situación actual
    - Efectos
    - Recomendaciones

2.4. Definiciones Conceptuales.

Auditor: Persona capacitada para realizar auditorías en empresas u otras instituciones.

Auditoria: Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.

Auditoría Externa: Es la revisión independiente que realiza un profesional de la auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como la razonabilidad en la emisión de sus resultados financieros.

Auditoría Interna: Es la revisión que realiza un profesional de la auditoria, cuya relación de trabajo es directa y subordinada a la institución donde se aplicará la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros.

Auditoria de sistemas: Está dirigida a evaluar los sistemas y procedimientos de uso en una empresa, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse.

Auditoria Informática: Auditoría Informática es aquella que tiene como objetivos evaluar los controles de la función informática, analizar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente.

Se entiende por Auditoría Informática una serie de exámenes periódicos o esporádicos de un sistema informático cuya finalidad es analizar y evaluar la planificación, el control, la eficacia, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa".

Archivo de Revisión de Auditoria como Control de Sistema: Consiste en la incorporación de módulos de rutinas auditadas en los programas aplicativos para que ejecuten funciones de supervisión de transacciones en forma permanente

Archivo de Revisión de Auditoria por Muestreo: Consiste en la selección al azar de los registros que han de ser llevados a un archivo para análisis de auditoria

Administración de sistemas: Son controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

Actividades de control gerencial: Se refieren a las acciones que realizan la gerencia y otro personal de la entidad para cumplir diariamente con las funciones asignadas. Son importantes porque implican la forma correcta de hacer las cosas, así como también porque el dictado de políticas y procedimientos y la evaluación de su cumplimiento, constituyen el medio más idóneo para asegurar el logro de objetivos de la entidad.

Alcance: Implica la selección de aquellas áreas o asuntos que serán revisados a profundidad en la fase de ejecución. Esta decisión debe ser efectuada teniendo en cuenta la materialidad, sensibilidad, riesgo, factibilidad y costo, así como la trascendencia de los posibles resultados a informar.

Áreas generales de revisión: Son aquellos asuntos seleccionados en las etapas de la auditoría. Tales áreas están referidas a:

- ✓ Protección y control de recursos públicos.
- ✓ Cumplimiento de leyes, normas y regulaciones aplicables.
- ✓ Economía y eficiencia.
- ✓ Procedimientos para medir e informar sobre la efectividad el programa o actividad.

- ✓ Evaluación del programa o actividad.
- ✓ Procesamiento y control del sistema de administración financiera y el sistema de información computarizada-SIC.
- ✓ Auditoría interna.

Asuntos más importantes: Representan aquellas actividades clave de los sistemas y controles aplicados que, de acuerdo a la opinión del auditor, resultan vitales para el éxito del ente a ser examinada. Constituyen asuntos que tienen importancia en esta etapa, pero que deben ser examinados y confirmados en la fase de ejecución de la auditoría.

Base De Datos: Base de datos es cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora, está diseñado para facilitar su mantenimiento y acceso de una forma estándar**.**

Carta de representación: Documento mediante el cual el nivel competente de la entidad examinada reconoce haber puesto a disposición del auditor toda la información requerida, así como cualquier hecho significativo ocurrido durante el período bajo

examen. Si se ha examinado varias áreas de la entidad, deberá recabarse varias cartas de representación.

Conclusiones: Son juicios del auditor, de carácter profesional, basados en las observaciones formuladas como resultado del examen. Estarán referidas a la evaluación de la gestión en la entidad examinada en cuanto al logro de las metas y objetivos, utilización de los recursos públicos en términos de eficiencia, economía y cumplimiento de la normativa legal.

Confidencialidad: Responsabilidad de los individuos autorizados para consultar o para bajar archivos importantes para micro computadores sin divulgar su contenido.

Control Interno Informático: Comprende el plan de organización y la totalidad de los métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización para asegurar la protección de todos sus recursos, la obtención de información correcta, segura y oportuna, así como la adhesión del personal a los objetivos y políticas debidamente predefinidos por la dirección.

Configuración del ordenador base: Configuración del soporte físico en torno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.

Controles: Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Criterios de auditoría: Comprende la norma con la cual el auditor mide la condición. Es también la meta que la entidad está tratando de alcanzar o representa la unidad de medida que permite la evaluación de la condición actual.

Disponibilidad: Responsabilidad de los individuos autorizados para alterar los parámetros de control de acceso al sistema operativo, al sistema manejador de base de datos, al monitoreo de teleproceso o al software de telecomunicación

Diagnóstico: Es un criterio de prioridades de eficiencia o de responsabilidad, respecto del impacto de la naturaleza legal financiera. El auditor calificará la situación hallada en materia de debilidades de control interno de la aplicación examinada.

Economía: La economía está relacionada con los términos y condiciones en los cuales se adquiere recursos, sean éstos financieros, humanos, físicos o de sistemas computarizados, obteniendo la cantidad y nivel apropiado de calidad al menor costo en la oportunidad requerida y en el lugar apropiado.

Ejecución (fase): Fase de la auditoría de gestión focalizada, básicamente, en la obtención de evidencia suficiente y competente sobre los asuntos significativos (líneas de auditoría) aprobados en el plan de auditoría.

Efectividad: Se refiere al grado en el cual un programa o actividad logra sus objetivos y metas u otros beneficios que pretendían alcanzarse, previstos en la legislación o fijados por otra autoridad.

Ética: Está conformada por valores morales que permiten a la persona adoptar decisiones y tener un comportamiento correcto en las actividades que le corresponde cumplir en la entidad.

Eficiencia: Está referida a la relación existente entre los bienes o servicios producidos o entregados y los recursos utilizados para ese fin, en comparación con un estándar de desempeño establecido.

Efecto: Constituye el resultado adverso o potencial que resulta de la condición encontrada. Generalmente, representa la pérdida en términos monetarios originada por el incumplimiento en el logro de la meta. La identificación del efecto es un factor importante al auditor, por cuanto le permite persuadir a la gerencia acerca de la necesidad de adoptar una acción correctiva oportuna para alcanzar el criterio o la meta.

Entorno de red: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan

aplicaciones críticas y consideraciones relativas a la seguridad de la red.

Entorno de aplicaciones: Procesos de transacciones, sistemas de gestión de base de datos y entornos de procesos distribuidos.

Enfoque Técnico de Software de Auditoria Multisitio: Es un staff centralizado la cual se encarga del desarrollo de sistemas, programación de computadores y la distribución del software de auditoria para ser utilizado después, en forma descentralizada en las localizaciones remotas.

Enfoque Técnico de Centro de Competencia: Estos son responsables de la ejecución centralizada de los programas de auditoría de sistemas; el centro de competencia recibe los archivos de datos procedentes de las localizaciones remotas, les aplica los programas de auditoria pertinentes y después, distribuye los informes resultantes a los auditores regionales para su análisis, evaluación y decisiones consecuentes.

Gestión de sistema de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

Hallazgo de auditoria: Este concepto es utilizado para describir el resultado de la comparación que se realiza entre un criterio y la situación actual encontrada durante el examen a un área, actividad u operación o circunstancias en las cuales el criterio fue aplicado. Un hallazgo de auditoría representa algo que el auditor ha encontrado durante su examen y comprende una reunión lógica de datos, así como la presentación objetiva de los hechos y otra información pertinente. Es toda información que a juicio del auditor, permite identificar hechos o circunstancias importantes que inciden en forma significativa en la gestión de la entidad auditada, tales como debilidades o deficiencias en los controles gerenciales o financieros y que, por lo tanto, merecen ser comunicados en el informe; siendo sus elementos: condición, criterio, causa y efecto.

Hasp: (Houston Automatic Spooling Program) Programa de devanado automático de Houston. Este programa es utilizado principalmente en el mainframe (Computador Principal) para que

provea funciones de administración de tareas, de trabajos y de datos. También es conocido como un candado se seguridad lógica.

Integridad Profesional: Constituye una calidad de la persona que mantiene principios morales sólidos y vive en un marco de valores.

Monitoreo: Representa al proceso que evalúa la calidad del control interno en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancias así lo requieran. Se orienta a la identificación de controles débiles, insuficientes o innecesarios y, promueve su reforzamiento. El monitoreo se lleva a cabo de tres formas:

- ✓ Durante la realización de actividades diarias en los distintos niveles de la entidad;
- ✓ De manera separada por personal que no es el responsable directo de la ejecución de las actividades, incluidas las de control.
- ✓ Mediante la combinación de ambas modalidades.

Observación: Esta referida a hechos o circunstancias significativos identificados durante el examen que pueden motivar oportunidades de mejoras. Si bien el resultado obtenido adquiere la denominación de hallazgo, para fines de presentación en el informe se convierte en observación.

Papeles de trabajo: Documentos que contienen la evidencia que respalda los hallazgos, observaciones, opiniones de funcionarios responsables de la entidad examinada, conclusiones y recomendaciones del auditor. Deben incluir toda la evidencia que se haya obtenido durante la auditoría.

Planeamiento: Fase de la auditoría durante la cual el auditor se aboca a la identificación de que examinar, como, cuando y con que recursos, así como la determinación del enfoque de la auditoría, objetivos, criterios y estrategia.

Plan de revisión estratégica: Acciones limitadas de evaluación, durante la fase Planeamiento, tendientes a determinar el alcance del examen así como su auditabilidad.

Plan de Auditoría: Tiene por propósito definir el alcance global de la auditoría de gestión, en términos de objetivos generales y objetivos específicos por áreas que serán materia de examen. Este documento incluye:

- ✓ Origen de la acción
- ✓ Objetivos de la auditoría
- ✓ Alcance de la auditoría, especificando períodos
- ✓ Áreas que serán examinadas, incluye objetivos específicos y alcance
- ✓ Criterios de auditoría a utilizarse
- ✓ Recursos de personal y especialistas que se necesitan
- ✓ Información administrativa
- ✓ Presupuesto de tiempo
- ✓ Informes a emitir y fechas de entrega
- ✓ Formato tentativo del informe.

Política: Se define como la declaración general que guía el pensamiento durante la toma de decisiones. La política es una línea de conducta predeterminada que se aplica en una entidad para llevar a cabo todas las actividades, incluyendo aquellas no previstas.

Productos y herramientas: Software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

Políticas de Seguridad Informática: Es un conjunto de normas que establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Programa de auditoría: Documento, preparado por el auditor encargado y el supervisor encargado, donde se señala las tareas

específicas que deben ser cumplidas por el equipo de auditoría para llevar a cabo el examen, así como los responsables de su ejecución y los plazos fijados para cada actividad.

Procedimientos de auditoría: Son operaciones específicas que se aplican en una auditoría e incluyen técnicas y prácticas que son considerados necesarios en las circunstancias.

Recomendaciones: Constituyen las medidas sugeridas por el auditor a la administración de la entidad examinada para la superación de las observaciones identificadas. Deben estar dirigidas a los funcionarios que tengan competencia para disponer su adopción y estar encaminadas a superar la condición y las causas de los problemas.

Prueba de Consentimiento: Es el determinar si los controles internos operan como fueron diseñados para operar. El auditor debe determinar si los controles declarados en realidad existen y si realmente trabajan confiablemente.

Pruebas Sustantivas: Es obtener evidencia suficiente que permita al auditor emitir su juicio en las conclusiones acerca de cuándo pueden ocurrir pérdidas materiales durante el procesamiento de la información.

Red Informática: Conjunto de técnicas, conexiones físicas y programas informáticos empleados para conectar dos o más ordenadores o computadoras. Los usuarios de una red pueden compartir ficheros, impresoras y otros recursos, enviar mensajes electrónicos y ejecutar programas en otros ordenadores.

Seguridad del ordenador base: Identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad (control de acceso) y disponibilidad.

Sistema de Control Interno: Un conjunto de procesos, funciones, actividades, subsistemas y gente que son agrupados para asegurar el logro efectivo de los objetivos y metas.

Sistema de Información: Es una herramienta estratégica que brinda rentabilidad y ventaja competitiva a los negocios frente a sus similares en el mercado, así mismo esta herramienta puede general costos y ventajas competitivas si no son bien administradas y dirigidas por personal adecuado.

Síntesis: Tiene como objetivo hacer que el informe sea de mayor utilidad para los usuarios. Como de los receptores de los informes sólo leerán la síntesis, es importante que ésta refleje el contenido del informe de manera clara y precisa. La síntesis debe presentar en forma exacta, clara y justa los aspectos más importantes del informe, a fin de evitar errores de interpretación.

Seguridad Informática: Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

Técnicas de auditoría: Son métodos prácticos de investigación y prueba que utiliza el auditor para obtener evidencia necesaria que fundamente su opinión.

Técnica de Registros Extendidos: Es una técnica que permite recoger o seleccionar por medio de rutinas especiales, todos los datos significativos que han afectado una transacción individual

COBIT (Objetivo de Control para tecnología de información): Es un estándar generalmente aplicable y aceptado para la práctica del Control de tecnología de Información de todas las empresas.

COSO Report "Committee of Sponsoring Organizations of the Treadway Commission": Es un Marco referencial que se concentra en el control interno de manera integrada y comprensiva.

SAC (Systems Auditability and Control): El informe SAC es el resultado de los esfuerzos continuos donde se define, evalúa, reporta y mejora el control interno.

IDEA (Interactive Data Extraction and Analysis): Es una poderosa herramienta de productividad de origen Canadiense, que permite visualizar, analizar, manipular, muestrear o extraer datos de virtualmente cualquier tipo de archivo, sin importar su tamaño.

CAPITULO III

3. NORMATIVA Y ESTÁNDARES INTERNACIONALES

Por efecto de estudio y análisis de esta tesis nos hemos enfocado directamente en la Normas de standardización COBIT. (Control Objectives for Information and related Technology) de la Information Systems Audit. and Control Foundation; lo que significa Objetivos de control para la Información y la Tecnología relacionada. Pero previamente revisaremos las definiciones de control y los objetivos de control que nos presenta COSO report (Committee of Sponsoring Organizations of the Treadway Commission) y SAC (Systems Auditability and Control).

3.1. COSO Y SAC

3.1.1. COSO Report

COSO (1992) es el marco más extendido y utilizado, que se concentra en el control interno de manera integrada y comprensiva.

Brinda recomendaciones a la dirección sobre cómo evaluar, reportar y mejorar los sistemas de control.

3.1.1.1. Clasificación de Controles

Según COSO, algunos controles pueden ser:

- Preventivos, Detectivos, Correctivos
- Discrecionales, No Discrecionales
- Voluntarios, Obligatorios
- Manuales, Automatizados
- Aplicación, General

3.1.1.1.1. Controles Preventivo, Detectivo, Correctivo.

Enfoque de la clasificación**:** Momento en que se aplica el control. Antes, durante o después de que ocurra un error.

- Se requiere el uso de claves privadas para acceder a los sistemas (Preventivo)
- Preparación de informes de excepción para revisiones subsecuentes (Detectivo)

- Procedimientos automáticos de recuperación de archivos para recrear archivos dañados (Correctivo)

3.1.1.1.2. Discrecional vs No Discrecional.

Enfoque de la clasificación: Quien realiza el control (Ser humano vs automatizado) y el grado al cual puede ser evitado.

- Revisión de firmas autorizadas (Discrecional)
- Requerimiento de ingreso de número de identificación personal (PIN) para el uso de cajeros automáticos (ATMs) (No discrecional)

3.1.1.1.3. Voluntario vs Mandatario

Enfoque de la clasificación**:** Quien impone la necesidad de control (interno vs externo)

- Controles de razonabilidad sobre los volúmenes de desembolso (Voluntario)

- Los informes de transacciones significativas deben cumplir con los requerimientos de las instituciones financieras (Mandatorio)

3.1.1.1.4. Manual vs Automático

Enfoque de la clasificación: Cuando se implementa el control con o sin automatización.

- Reconciliaciones efectuadas por empleados (Manual).
- Actualización automática de la cuenta corriente al momento de ingresar una factura (Automático)

3.1.1.1.5. Aplicación vs General

Enfoque de la clasificación**:** Transacción individual vs ambiente en el cual se procesan las transacciones.

- Procedimientos de balanceo computarizados entre subfunciones de un sistema automatizado (Aplicación)
- Mantenimiento de una fuerte función de seguridad de sistemas de información (General)

3.1.2. SAC

El informe SAC (1991, revisado en 1994) es el resultado de los esfuerzos continuos donde se define, evalúa, reporta y mejora el control Interno. Ofrece asistencia a los auditores internos sobre el control y auditoría de los sistemas y tecnologías informáticas.

3.1.2.1. Clasificación de Controles

Según SAC los controles se clasifican en:

- Preventivos, Detectivos, Correctivos
- Discrecionales, No Discrecionales
- Voluntarios, Obligatorios
- Manuales, Automatizados
- Aplicación, General

3.1.2.2. Objetivo de Control y Riesgo

Los riesgos incluyen fraudes, errores, interrupción del negocio, y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad, y el cumplimiento. La integridad de la

información es resguardada por los controles de calidad del input, procesamiento, output y software. Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran conformidad con las leyes y regulaciones, los estándares contables y de auditoría, y las políticas y procedimientos internos.

3.2. Normas Internas de Auditorias (COBIT).

Estándar COBIT (Control Objectives for Information and related Technology) es un estándar que está comprendida por una serie de normas y directrices enfocadas a la preservación, control, armonización y gestión de la Tecnología de Información. COBIT es considerada una herramienta a nivel de gerencia, Auditores y Usuarios, porque establece parámetros definidos, vincula la tecnología Informática y las prácticas de control.

La misión y objetivo de COBIT es investigar, desarrollar, publicitar y promocionar objetivos de control de tecnología de información a nivel internacional, actualizados a la realidad actual para ser usado por los gerentes de negocios y auditores.

Usuarios:

COBIT se dirige a tres públicos distintos: dirección, usuarios y auditores de sistemas de información.

- ✓ La Gerencia: es la que se encarga de analizar, evaluar y autorizar las inversiones de Tecnología de Información y la que se encarga de controlar el rendimiento de las mismas para determinar el costo beneficio generado por dicha inversión.

- ✓ Los Auditores: evalúan y se respaldan en los parámetros predefinidos para el análisis de los controles y seguridades de la Tecnología de Información en la organización.

- ✓ Los Usuarios finales: son los que trabajan directamente con las disposiciones establecidas por las normas de standardización.

Características

COBIT: Objetivos de control para la Información y la Tecnología relacionada

El objetivo principal es proporcionar una estructura sólida donde se desarrollen y se establezcan políticas claras y buenas prácticas en las empresas a nivel mundial.

En COBIT se establecen los siguientes recursos en Tecnología de Información necesarios para alcanzar los objetivos de negocio:

- Datos:
- Aplicaciones
- Tecnología:
- Instalaciones:
- Recurso Humano:
- Procesos de TI

COBIT impulsa y promueve la aplicación de controles en los procesos incluyendo políticas, procedimientos, prácticas y estructuras orgánicas que apoyan procesos comerciales y objetivos.

COBIT considera a las personas como parte del sistema de control interior, es así que clasifica a las personas como uno de los recursos primarios manejado por varios procesos de tecnología de información.

(Las habilidades de las personas, los conocimientos, la productividad para planear, para organizar, adquirir, entregar y apoyar son el factor primordial en el sistema de control interno).

COBIT establece que los objetivos son apoyados por los procesos de negocio. Estos procesos, a su vez, son apoyados por información proporcionada a través del uso de recursos de tecnología de información. Los requisitos comerciales para esa información sólo están satisfechos a través de las medidas de controles adecuados.

El enfoque exclusivo de COBIT es el establecimiento de una estructura de seguridad y control en la tecnología de información, la cual Define una unión clara entre los controles de los sistemas de información y los objetivos comerciales.

COBIT también proporciona una vía para facilitar la comunicación entre la dirección, los usuarios y auditores con respecto a los controles de sistemas de información.

COBIT dirige la responsabilidad a la dirección para supervisar toda la tecnología de información procesada y la necesidad de obtener convicción independiente en los controles.

3.3. Normas Relativas a la Planificación de la auditoría informáticas.

A continuación estableceremos ciertas normas expedidas por COBIT en lo que refiere a la Planificación de la revisión de sistemas de aplicaciones.

La información que veremos a continuación es la traducción de inglés a español más cercana que hemos podido realizar de ciertos ítems de el estándar COBIT, tratando de contribuir con datos más certeros**.**

El objetivo Primordial de la planificación es identificar los niveles de riesgos en las aplicaciones de los sistemas. Los niveles de riesgos influyen en las evidencias requeridas en una auditoría, es decir a mayor riesgo, mayor cantidad de pruebas y evidencia.

Los niveles de riesgos aplicados a los sistemas y a los niveles de información o datos incluye situaciones como:

- Falta de capacidad operacional en el sistema.
- Los accesos desautorizados a los sistemas y/o datos.
- Sistemas incompletos, inexactos.
- Sistemas en los que no se ha incluido niveles de autorización.
- Incapacidad de tener actualizado el sistema.
- Falta de integridad, confidencialidad y exactitud en el proceso de información.

Los diferentes tipos de aplicaciones para tratar los diferentes niveles de riesgos pueden incluir en la forma de controles computarizados desarrollados dentro del sistema, controles realizados manualmente, o de una combinación de ambos.

Establecer la confianza en los controles programados se torna importante ya que los controles generales de Tecnología de información, puede ser considerado tan efectivo como los controles específicos pertinentes al objetivo de la evaluación.

Los controles generales podrían ser un tema para una revisión independiente, que incluiría entre otros los controles físicos, sistema la

seguridad, red, respaldos en copia de seguridad y la planificación de contingencia. Dependiendo de los objetivos de control de la revisión, el auditor de TI evaluará la conveniencia de aplicar los que considere favorable al sistema.

Pueden realizarse las revisiones de sistema de aplicación cuando:

- un sistema de aplicación o un paquete comercial está siendo evaluado para su adquisición,
- Antes de que el sistema de aplicación entre en la producción (pre-aplicación) y después de que el sistema de aplicación vaya a producción (post-aplicación). La pre-producción del sistema revisa todo incluyendo la aplicación de la seguridad en todo nivel, los planes para la aplicación de seguridad, suficiente documentación del sistema y la documentación de los usuarios en forma suficiente para una adecuada aceptación y asignación user y password.
- La revisión de post-aplicación incluye el nivel de la aplicación
- La seguridad después de la aplicación puede cubrir la conversión del sistema si ha habido un traslado de datos y archivos maestros del viejo al nuevo sistema.

Los objetivos y alcances de una revisión/Auditoria de un sistema de aplicación generalmente forman parte de los términos de la referencia. La forma y el contenido de los términos de la referencia pueden variar pero deben incluir:

- Los objetivos y el alcance de la auditoría
- Auditores de sistemas de información que realizan la revisión
- Una declaración con respecto a la independencia de Auditor de sistemas de información del proyecto.
- El tiempo en que comenzará la revisión
- El horario de la revisión
- Informes, reportes o avances acordados.
- Reuniones de cierre acordadas

Se debe desarrollar objetivos para tratar los 7 criterios de la información de COBIT y después aplicar a la organización. Los 7 criterios de la información de COBIT son los siguientes:

- Efectividad
- Eficacia

- Confidencialidad
- Integridad
- Disponibilidad
- Conformidad
- Confiabilidad de la información

Cuando los Auditores de sistemas de información han estado implicados previamente en el desarrollo, adquisición, puesta en práctica o el mantenimiento de un sistema de aplicación y es asignado a un compromiso de auditoría, La independencia de los auditores de sistemas de información puede verse afectada.

Los auditores de sistemas de información pueden referirse a apropiados lineamientos para ocuparse de tales circunstancias.

3.4. Normas Relativas a la ejecución de la auditoría.

En este punto trataremos sobre ciertas normas expedidas por COBIT en lo que refiere a la Ejecución de la auditoría de sistemas de aplicaciones.

Documentando el Flujo de Transacciones.

La información recopilada debe incluir los aspectos automatizados y manuales del sistema. El foco debe estar en entrada de datos (si es electrónico o manual), el proceso, el almacenaje, y la salida que sean de significación para el objetivo de la intervención. El auditor de sistemas de información puede encontrar, dependiendo de los procesos del negocio y el uso de la tecnología, qué documentación del flujo de transacciones puede ser o no práctica. En este caso, el auditor debe elaborar un diagrama de flujo de datos o narrativa y/o utilizar la documentación del sistema. También se debería dar consideración a la documentación de las aplicaciones que hacen interfase con otros sistemas.

El auditor de sistemas de información puede confirmar la documentación realizando procedimientos tales como un seguimiento a través de prueba.

Identificando y Probando los controles de los Sistemas de Aplicación

Los controles específicos que mitigan los riesgos de las aplicaciones pueden ser identificados y obtener una evidencia de auditoría suficiente

para asegurar al auditor que los controles están funcionando según lo previsto.

Esto se puede lograr con procedimientos por ejemplo:

- Preguntas y observación
- Revisión de documentación
- Probando los controles de los sistemas de aplicación donde fueron programados y donde fueron probados; el uso de CAATs (Computer Assisted Audit. Techniques -Técnicas de auditorias asistida por Computadora) puede ser considerado para estas pruebas.

La naturaleza, la sincronización y el grado de la prueba se deben basar en el nivel del riesgo del área bajo la revisión y objetivos de la intervención. Si no existieran controles, El auditor de sistemas debe reconocer la debilidad y la confiabilidad de los controles existentes.

Si el auditor encuentra debilidades en los controles de las aplicaciones automatizadas, éste deberá tener u obtener medidas de seguridad

(dependiendo del objetivo de la intervención), o si es posible, obtener estas medidas de los controles del proceso manual.

La eficacia de controles automatizados es dependiente de los controles generales de la tecnología de información. Por lo tanto, si no hay controles existentes, la capacidad de poner confianza en los controles de aplicación puede ser seriamente limitado, por ende el auditor de sistemas deberá considerar procedimientos alternativos.

3.5. Normas Relativas al informe de auditoría.

Para finalizar trataremos sobre ciertas normas expedidas por COBIT en lo que refiere al informe de auditoria de la evaluación de los sistemas de aplicación.

Las Debilidades identificadas en la revisión se deben a una ausencia de controles o al incumplimiento de las mismas, se debe llamar la atención del dueño del proceso del negocio y al gerente responsable de emitir los soportes de Sistemas si las debilidades identificadas durante la revisión de sistemas de aplicación se consideran significativas o materiales, se

debe aconsejar de tomar una medida inmediata correctiva a las autoridades correspondientes.

Los controles computarizados, son dependientes de los controles generales Informáticos, y si se llegare a encontrar debilidades en esas área deben también ser reportadas. En caso de que no hayan sido revisados los controles, se debe incluir este punto en el informe final del auditor.

El auditor de sistemas debe emitir las recomendaciones apropiadas referentes a los controles claves para la empresa. Estas recomendaciones deben ser incluidas en el reporte.

3.6. Objetivo de control de COBIT.

3.6.1. Planeación y organización.

Responsabilidad de la Seguridad Lógica y Física

La Gerencia deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un Gerente de seguridad de la información, quien

reportará a la alta gerencia. Como mínimo, la responsabilidad de la Gerencia de seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

Cumplimiento de Políticas, Procedimientos y Estándares

La Gerencia deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la Alta Gerencia y promoverse a través del ejemplo.

3.6.2. Adquisición e implementación.

Documentación y Procedimientos en la administración de cambios

El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

3.6.3. Entrega de servicio y soporte.

Almacenamiento de respaldo en el sitio alterno (Off-site)

El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio. Los propietarios de los procesos del negocio y el personal de la función de TI deben involucrarse en determinar que recursos de respaldo deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo debe contar con medidas ambientales para los medios y otros recursos almacenados; y debe tener un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. La

Gerencia de TI debe asegurar que los acuerdos/ contratos del sitio alterno son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental.

Administrar Medidas de Seguridad

La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI; Implementar el plan de seguridad de TI; Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI; Evaluar el impacto de las solicitudes de cambio en la seguridad de TI; Monitorear la implementación del plan de seguridad de TI; y Alinear los procedimientos de seguridad de TI a otras políticas y procedimientos.

Identificación, Autenticación y Acceso

El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso. Dicho mecanismo deberá

evitar que personal no autorizado, conexiones telefónicas por marcado y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de autorizar usuarios para usar múltiples sign-ons. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).

Seguridad de Acceso a Datos en Línea

En un ambiente de tecnología de información en línea, la Gerencia de TI deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

Administración de Cuentas de Usuario

La Gerencia deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá incluirse

un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso. La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación. Los acuerdos de outsourcing deben considerar los riesgos, los controles sobre seguridad y los procedimientos para los sistemas de información y las redes en el contrato que se establece entre las partes.

Sistema de Administración de Problemas

La Gerencia de TI deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados, analizados y resueltos oportunamente. Los procedimientos de cambios de emergencia a programas se deben probar, documentar, aprobar y reportar prontamente. Deberán emitirse reportes de incidentes en caso de problemas significativos.

Procedimientos de Autorización de Entrada de Datos

La organización deberá establecer procedimientos apropiados para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.

Validación y Edición de Procesamiento de Datos

La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubicados en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.

Manejo de Errores en el Procesamiento de Datos

La organización deberá establecer procedimientos para el manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

Respaldo (Back-up) y Restauración

La Gerencia deberá implementar una estrategia apropiada de respaldo y recuperación para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente. De Internet u otra red pública, la Gerencia deberá definir e implementar procedimientos y protocolos que deben ser utilizados para el aseguramiento de la integridad, confidencialidad y “no negación/rechazo” de mensajes sensitivos.

Funciones de Respaldo

Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que las copias de respaldo sean verificadas regularmente.

Integridad de Transacciones Electrónicas

Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la Gerencia deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, que permitan asegurar su integridad y autenticidad de: atomicidad (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan) consistencia (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial); aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir a fallas de sistema)

Seguridad Física

Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información incluyendo el uso de dispositivos de información off-site en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que

contenga el hardware del sistema sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.

Control de Visitantes

Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de la función de servicios de información sean controladas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

Protección contra Factores Ambientales

La Gerencia de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas

para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

Suministro Ininterrumpido de Energía

La Gerencia deberá evaluar regularmente la necesidad de contar con generadores y baterías de suministro ininterrumpido de energía (UPS) para las aplicaciones críticas de tecnología de información, con el fin de protegerse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

Manual de Instrucciones y Procedimientos de las Operaciones de Procesamiento

La Gerencia de TI deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red). Todas las soluciones y plataformas de tecnología de información con que cuente la empresa deberán ser operadas utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

Bitácoras de Operación

Los controles de la Gerencia deberán garantizar que se almacene en bitácoras suficiente información cronológica de las operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que rodean y soportan el procesamiento.

3.6.4. Monitoreo

Referente a proveer auditoría independiente

Estatuto de Auditoría

La alta gerencia de la organización deberá establecer el estatuto para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría. Asimismo este documento deberá ser revisado periódicamente para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoría.

Independencia

El auditor deberá ser independiente del auditado tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoría deberá ser suficientemente independiente del área auditada para concluir una auditoría en forma objetiva.

Ética y Estándares Profesionales

La función de auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (Ej. Código de Ética de la Information Systems Audit and Control Association) y estándares de auditoría (Ej. Estándares de la Information Systems Audit and Control Association) en todo lo que el auditor lleve a cabo. El debido cuidado profesional deberá observarse en todos los aspectos del trabajo de auditoría, incluyendo el respeto de estándares aplicables sobre auditoría y tecnología de información.

Competencia

La Gerencia deberá asegurar que los auditores responsables de las revisiones de las actividades de la función de servicios de información de la organización, sean técnicamente competentes y cuenten en forma general con las habilidades y conocimientos (Ej. dominios requeridos para obtener el CISA) necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. La Gerencia deberá asegurar que el personal asignado a tareas de auditoría de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

Planeación

La alta gerencia deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la Gerencia para controlar las actividades de la función de servicios de información. Dentro de este plan la Gerencia deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoría

para alcanzar los objetivos de auditoría y cumplir con los estándares profesionales correspondientes.

Ejecución del Trabajo de Auditoría

Las auditorías deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo considerados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportados por un análisis apropiado y una correcta interpretación de esta evidencia.

Reporte

La función de auditoría de la organización deberá entregar un reporte, en un formato adecuado, a todo el personal interesado una vez concluida su revisión. El reporte de auditoría deberá mostrar los objetivos de la auditoría, el período de cobertura y la naturaleza y extensión de trabajo de auditoría realizado. El reporte deberá identificar la Organización, los destinatarios del informe y cualquier

restricción en su circulación. El reporte de auditoría deberá también mostrar los hallazgos, conclusiones y recomendaciones relacionadas con el trabajo de auditoría llevado a cabo, así como cualquier salvedad o comentario que el auditor tenga con respecto a la auditoría.

Actividades de Seguimiento

La resolución y atención de los comentarios sobre la auditoría depende de la Gerencia. Los auditores deberán solicitar y evaluar la relación con los hallazgos, conclusiones y recomendaciones de auditorías anteriores para determinar si las acciones apropiadas han sido implementadas de manera oportuna.

CAPITULO IV

4. CASO PRÁCTICO

4.1. Información Preliminar

Introducción

Por motivo de ética, acuerdo entre la empresa y el que desarrolla esta auditoría no se podrá mencionar el nombre de la empresa. Para efecto de estudio la empresa se llamará TALLERES INTEGRADOS y el sistema se llamará “SMAC” Sistema de Mantenimiento Asistido por Computadora.

Talleres Integrados es una empresa dedicada a dar mantenimiento preventivo, correctivo y de mejoras a las unidades navales las cuales son consideradas como parte del activo de una de las compañías de la misma corporación. Esta empresa es reconocida a nivel nacional, posee una gran cantidad de unidades navales tales como: veleros, remolcadores y fragatas entre otras, en todo el litoral Ecuatoriano.

La sede de esta empresa está ubicada en Guayaquil, posee un extenso territorio para ejecutar todas las operaciones de mantenimiento y cuenta con una gama de empleados en calidad de especialistas encargados de las diferentes tareas encomendadas.

En vista del incremento y creación de nuevas empresas en todo el mundo y por ende la aparición de los factores que incitan al desarrollo y competencia del mercado, las compañías están aplicando nuevas estrategias, planes, desarrollo de habilidades y la adaptación de nuevas herramientas e instrumentos de gestión. Dentro de estas herramientas de gestión encontramos la adopción de Tecnología de Información la cual es de suma importancia ya que estas son las que van agilitar los procesos, actividades e información de manera confiable, completa y oportuna para una correcta y acertada toma de decisiones; así como también permiten alcanzar en forma eficiente y efectiva la gestión de los recursos materiales y humanos. La empresa Talleres Integrados adquirió un sistema de gestión y control de las actividades de mantenimiento para controlar y monitorear el tiempo de ejecución, la mano de obra utilizada, los materiales requeridos y el control de los procesos.

Luego de la adquisición del sistema no se efectuó evaluación alguna, lo que contribuyó a que este sistema no haya sido previamente estudiado y valorado en factores de riesgo y control de información, lo cual ha venido afectando la visión e idea de implantar un sistema de información.

Debido a dichos acontecimientos, surge la necesidad de evaluar el sistema para evitar y controlar posibles riesgos de pérdida, sabotaje o mal manejo de información confidencial de la organización. Por esta razón durante el desarrollo de esta evaluación plantearemos una serie de recomendaciones de controles a todas las deficiencias encontradas.

Motivos

Entre los principales motivos o justificativos para ejecutar esta evaluación encontramos los siguientes:

- Desconocimiento del sistema por parte de los directivos.
- Desconocimiento de la existencia de adecuados procedimientos en la asignación, actualización y eliminación de claves de acceso.
- Desconocimiento de la existencia de la documentación del sistema y los procedimientos y tareas de respaldo de información.

- Desconocimiento de la existencia de controles generales y específicos que garanticen la veracidad e integridad de la información.
- Desconocimiento de la existencia de un plan de contingencia donde se establezcan los procedimientos para resolver fallas.
- Desconocimiento de políticas y objetivos de seguridad física y lógica.
- Desconocimiento del proceso y flujo de información de las actividades de mantenimiento de la empresa por parte de los usuarios y directivos.

Objetivo General.

Realizar una evaluación al SMAC (Sistema de Mantenimiento Asistido por Computadora) para que permita emitir una serie de criterios que sirvan como apoyo y sustento para la mejora del sistema de información de la organización.

Objetivos Específicos.

- Conocer la situación actual del sistema de información y de las áreas relacionadas

- Evaluar la administración de las claves de accesos a los módulos del sistema.
- Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones al momento de hacer cambios.
- Determinar el ambiente del hardware y software del servidor de aplicaciones, del servidor de datos y equipos de ciertos usuarios, en términos de disponibilidad y requisitos técnicos.
- Evaluar la integridad y validez de los datos de entrada a los módulos del sistema
- Evaluar el plan de contingencia de la aplicación en caso de fallas del sistema.
- Evaluar las medidas de seguridad físicas considerando los aspectos de integridad, confiabilidad y disponibilidad de la información.
- Identificar el proceso y flujo de Información del sistema.

Alcance

El presente trabajo comprende exclusivamente la evaluación del módulo de mantenimiento con los respectivos submódulos e ítems:

Ingreso de Mantenimiento

- Generación de Solicitud de Trabajo
- Generación de Ordenes de trabajo

Búsqueda de Mantenimiento

- Consultas de Solicitudes de trabajo
- Consultas de Ordenes de trabajo

El análisis de los datos e información del sistema corresponde al período comprendido desde el 1er de enero del 2004 hasta el 31 de Diciembre del mismo año.

En base a los objetivos y justificativos planteados anteriormente el trabajo a realizar comprende lo siguiente:

1. Evaluar los controles de entrada, procesamiento y salida implantados en el sistema de mantenimiento de forma que tiendan a:

    - Asegurar la compatibilidad de los datos más no su exactitud o precisión, tal es el caso, de la validación del tipo de datos que contiene los campos o verificar si se encuentran dentro

de un rango específico, verificación de seguridad para el acceso a terminales, programas, archivos, datos e información confidencial.

- Asegurar que la totalidad de los datos sean procesados por el computador.
- Asegurar que los datos procesados por el computador estén debidamente autorizados.
- Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones

2. Evaluar los controles implementados, entre los cuales deben existir:

    - Controles sobre el acceso de usuarios.
    - Controles de claves de acceso
    - Controles de datos ingresados
    - Controles de documentos de procesos y procedimientos importantes del sistemas.
    - Controles de transacciones mal efectuadas.

3. Emitir un informe estableciendo las recomendaciones sobre los hallazgos encontrados.

Como resultado de los motivos, objetivos y alcance de la auditoría, mencionados recientemente, se ha elaborado un programa de trabajo para la evaluación del sistema, en el cual se detalla cada uno de los objetivos y procedimientos que se seguirá para la aplicación del programa de evaluación. Ver el Programa de Trabajo de Auditoría que se encuentra en (ANEXO 1)

4.2. Descripción del sistema.

El sistema de mantenimiento surge de la necesidad de "Alcanzar la máxima eficiencia posible del material y llevar el control de la administración del mantenimiento de las unidades navales y repartos de tierras". Es así que para septiembre del 2001 la empresa Talleres Integrados adquirió un software específico para el control de mantenimiento planificado, este contrato se efectuó con la compañía FABRIL SYSTEMS el cual incluía el desarrollo e implementación a una unidad naval tipo corbeta, asesoramiento técnico y capacitación del personal finalizando los trabajos para marzo del 2002. Para inicio del 2003 las unidades navales adquirieron el proceso Batch del sistema. En esa época Talleres Integrados adquirió 15 licencias para hacer uso del sistema pero debido a la gran necesidad de implementar el SMAC en

todas las áreas de la empresa se procedió a la adquisición de 10 licencias más en el 2004.

El propósito principal de Talleres Integrados fue el de adquirir un software de mantenimiento planificado, para optimizar los procesos de mantenimiento correctivo e incrementar el control estadístico y de costeo de las actividades, además que permita optimizar recursos, mejorar la planificación, controlar el mantenimiento de equipos o sistemas instalados en unidades a flote y repartos en tierra.

SMAC versión 2002, Sistema de Mantenimiento Asistido por Computadora es un sistema que está en la capacidad de administrar la gestión de mantenimiento de los activos de la institución, brinda la oportunidad de reducir costos a través de la planificación preventiva y anticipada de todas las tareas de mantenimiento, garantiza el manejo adecuado de los activos, lo que prolonga su vida útil al servicio de los usuarios, ofrece información acerca de los costos totales en los que se incurre al realizar el mantenimiento de los activos.

SMAC está en la capacidad de administrar toda la gestión de mantenimiento de una empresa y llegar a convertirse en una herramienta

de trabajo irremplazable para la gerencia, jefaturas y usuarios claves de mantenimiento, ya que fue creado para ayudar y alcanzar el mantenimiento productivo total.

SMAC tiene una gran ventaja de poder adaptarse a cualquier tipo de organización ya que las Instalaciones pueden ser centralizadas o dispersas, puede aplicarse a entornos multiempresas, líneas, bodegas, etc. Es Completamente parametrizado: en código de máquina, en configuración de formatos de O/T, fichas, hojas de campo, etc. El mantenimiento puede ser centralizado o no centralizado, se aplica a cualquier tipo de Infraestructura tales como industrial, hospitalaria, vial, automotriz, naviera, aérea, etc. Con regímenes de trabajo continuo o parcial, En resumen el usuario personaliza SMAC a sus necesidades.

4.2.1. Ambiente del entorno informático

4.2.1.1. Equipos disponibles

Talleres Integrados posee un total de 3 servidores y 40 terminales inteligentes, las cuales se encuentran distribuidas de la siguiente manera

TABLA 2
COMPUTADORAS MASTER DESTINADAS
COMO SERVIDORES DEL SISTEMA.

Servidor de aplicaciones	1
Servidor de base de datos	1
Respaldo servidor base de datos	1
TOTAL	3

TABLA 3
DISTRIBUCIÓN DE LOS EQUIPOS DE CÓMPUTO

Control y Monitoreo de la Información	03
Unidades navales	11
Repartos	07
Talleres y laboratorios	19
TOTAL	40

Para tener una mayor apreciación de la distribución de las computadoras destinadas para la ejecución o utilización del SMAC podemos apreciar las siguientes tablas.

TABLA 4
TERMINALES INTELIGENTES DESTINADAS
AL CONTROL Y MONITOREO DE LA INFORMACIÓN

Estadísticos	1
Control de proceso	1
Monitoreo y ayuda a usuarios	1
TOTAL	3

TABLA 5
TERMINALES INTELIGENTES UBICADAS
EN LOS BARCOS

UNIDADES NAVALES	PC UNIDAD NAVAL
Unidad naval x	1
Unidad naval y	1
Unidad naval z	1
Unidad naval a	1
Unidad naval b	1
Unidad naval c	1
Unidad naval d	1
Unidad naval e	1
Unidad naval f	1
Unidad naval g	1
Unidad naval h	1
TOTAL	11

TABLA 6
TERMINALES INTELIGENTES UBICADAS
EN LOS REPARTOS O EMPRESAS

Repartos (empresas)	PC por reparto
Reparto ABC	1
Reparto DCF	1
Reparto GFR	1
Reparto FRS	1
Reparto GTT	1
Reparto SDE	1
Reparto DAV	1
TOTAL	7

TABLA 7
TERMINALES INTELIGENTES UBICADAS EN LOS TALLERES Y LABORATORIOS QUE DAN MANTENIMIENTO

Talleres y laboratorios	15
Otros talleres	4
TOTAL	19

4.2.1.2. Entorno de Red

La empresa Talleres Integrados cuenta con una red de Fibra óptica la cual conecta el servidor de aplicación y el servidor de datos con los diferentes repartos; las unidades navales que se encuentra en los muelles se enlazan mediante conexión inalámbrica.

Ver conexión global (FIGURA 4.1) y conexión de la red de fibra óptica (FIGURA 4.2)

FIGURA 4.1
CONEXIÓN GLOBAL

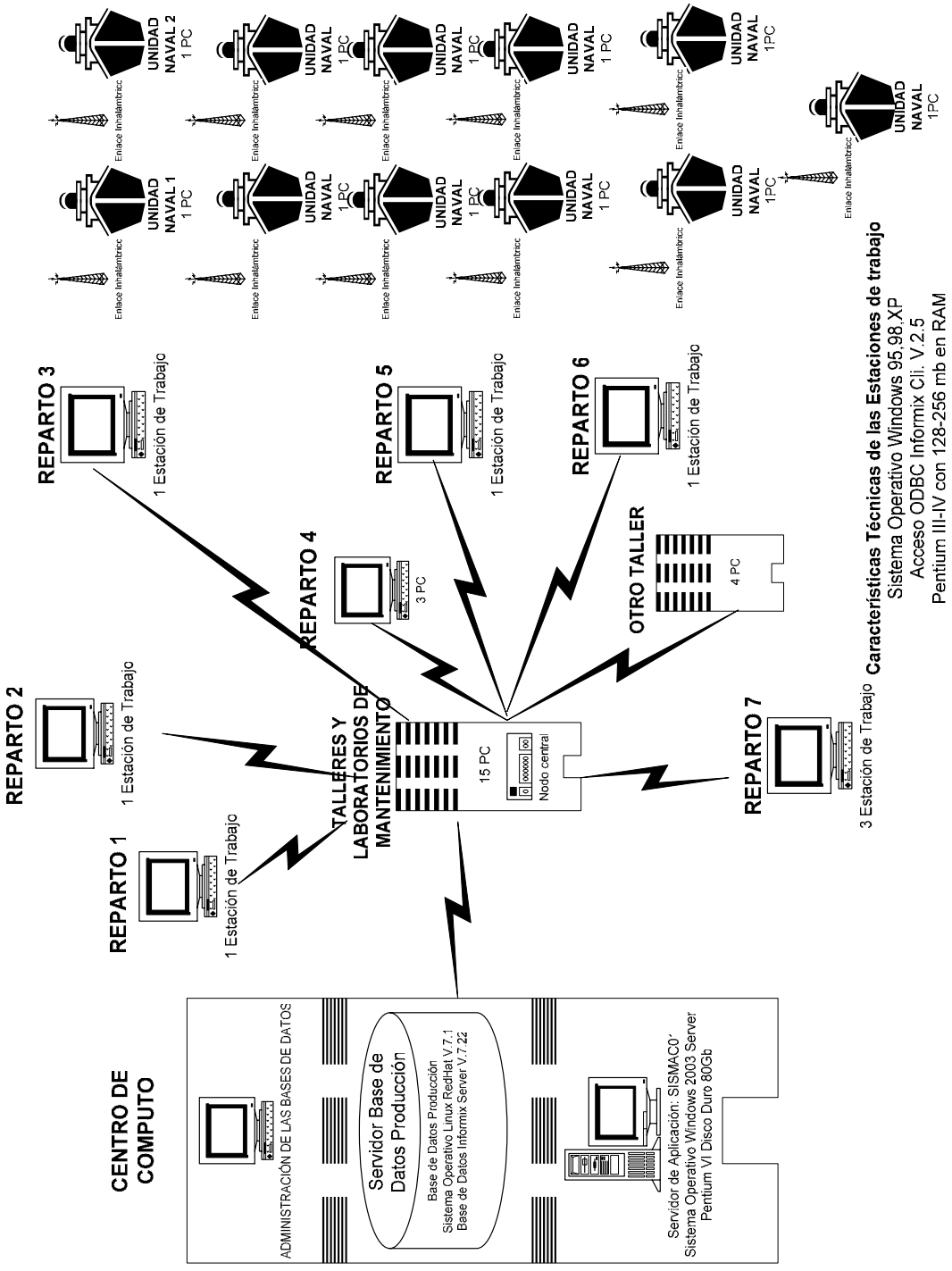
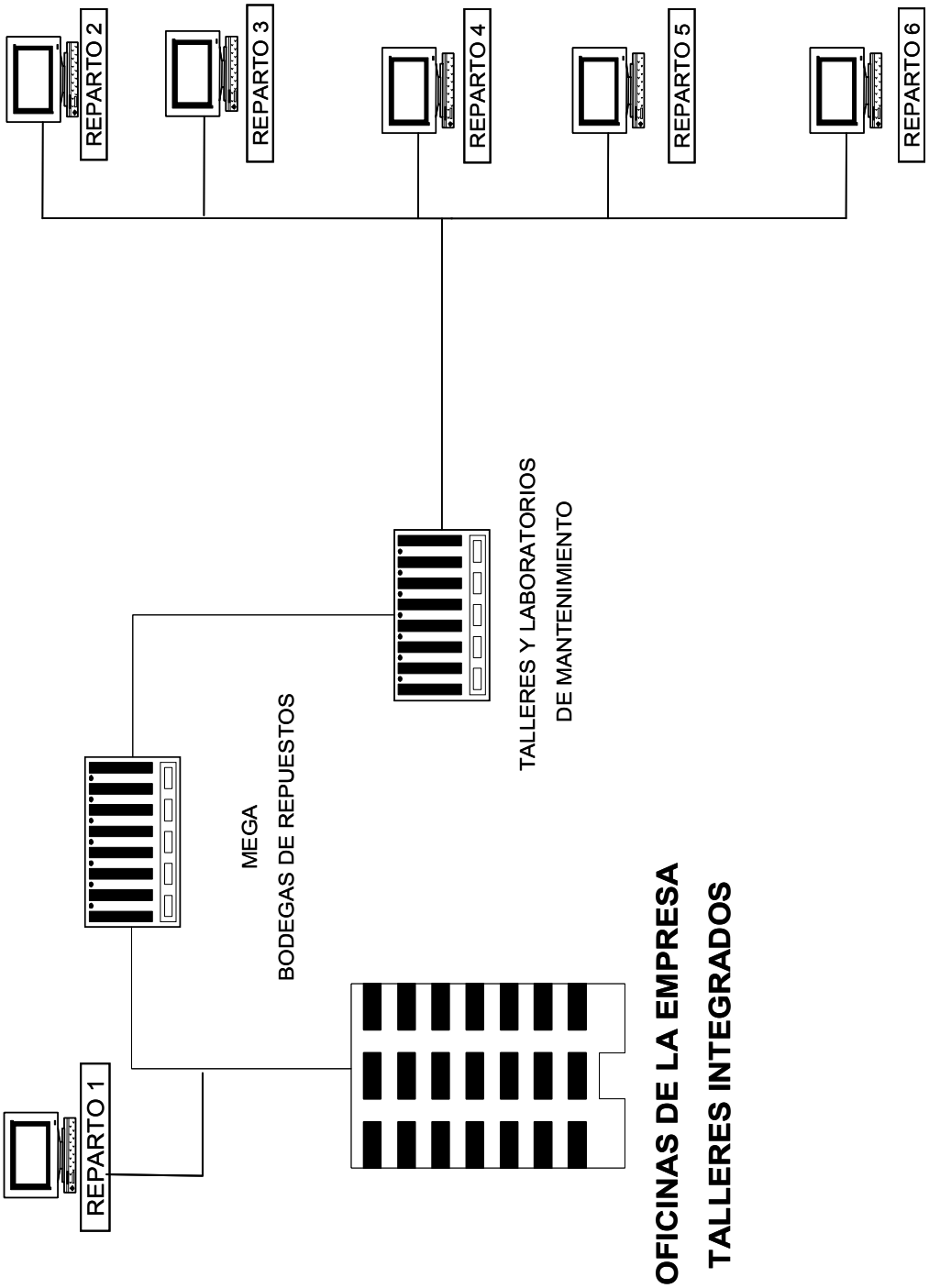


FIGURA 4.2
CONEXIÓN DE LA RED DE FIBRA OPTICA
DE LA EMPRESA "TALLERES INTEGRADOS"
AREA OPERATIVA



4.2.1.3. Hardware

Las características básicas que deben poseer los terminales inteligentes para instalar y ejecutar el SMAC son:

Pentium 1 o su equivalente

32 MB RAM, Mínimo

Sin embargo las características técnicas de las computadoras que posee Talleres Integrados son avanzadas y actualizadas.

TABLA 8
CARACTERÍSTICAS TÉCNICAS DE LAS COMPUTADORAS DE TALLERES INTEGRADOS

Componente	Marca	Modelo	Capacidad
Disco Duro	Maxtor	9043202	40Gb.
Disquetera	Mitsumi	D359M3	1.44Mb.
CD- Rom	Microsoft	CRMC-FX3205	56X
Tarjeta de Red	Netgear	FA310TX	10/100
Tarjeta de Video	CE	1F9-53765PCI	
Tarjeta de Sonido	Creative	CT452Dt452ddjdd45	
Memoria DRAM	Simple	A004445	250MB.
CPU	Intel	PENTIUM III	600Mhz.
Case	Premio	PREMIO MTPGA	
Monitor	Sansung	SyncMaster 753s	Digital
Teclado	Omega	264412	125 teclas
Mouse	Genius	NetScroll	3botones

Las características básicas que poseen los servidores para ejecutar el SMAC son:

Servidor de Aplicaciones

Procesador: Pentium IV 2.4 GHZ

Al procesador le respalda una memoria RAM de 1 GHZ de velocidad.

En dos Discos Duros de 35 GB c/u se almacena las aplicaciones que el servidor ejecuta en sus tareas

Espacio Utilizado 10.1 GB

Espacio Libres 24.9 GB

Tarjeta de red: PRO/1000 xt Intel

Módem Externo

Servidor de Base de Datos

Modelo Intel SCB2

Procesador: Pentium III

Procesadores Instalados: Dos

Número de Procesadores que soporta: Dos

Velocidad de procesamiento: 1.26 GHZ

Memoria Cache L2: 512 Kb

Memoria RAM: 1 GB

Tipo de memoria RAM: ECC SDRAM PC 133

Disco Duro: 2 discos de 18 GB Hot Swap 45 GB Total

Espacio Utilizado 25 GB

Espacio Libre 20,12 GB

Controladora de disco duro: Ultra SCSI 160

Red: 10/100 integrada Chipset Intel

Memoria de video 8 MB

4.2.1.4. Sistema Operativo

EL Sistema Operativo necesario para los terminales inteligentes puede ser:

Windows 95, 98, millennium, 2000 profesional, XP

El servidor de Base de Datos posee un Sistema Operativo Windows 2000 Server OEM (licencia)

El servidor de Aplicaciones posee un Sistema Operativo Windows 2003 Server (Licencia)

4.2.1.5. Plataforma del Sistema

Entorno: Multiusuario

Base de Datos: Informix Server V.7.22

Lenguaje: Visual Basic 6.0 utilizando ADO 2.6

Estructura: ADO (cliente servidor o únicamente cliente)

Las terminales inteligentes utilizan el acceso ODBC: Informix Cliente V 2.5 para poder hacer conexión con el servidor de aplicaciones y de Base de datos.

4.2.1.6. Software utilitario

Entre los utilitarios Básicos que poseen los computadores están:

1. **Microsoft Office 2000 Professional en Español:**

- Microsoft Word
- Microsoft Excel
- Microsoft Power Point
- Microsoft Access
- Microsoft Project
- Microsoft Outlook
- Microsoft Photo Editor

2. **Software de Internet**

   - Microsoft Internet Explorer 6.0

3. **Software Compresor**

   - Winzip 8.0

4. **Software Entretenimiento y Comunicaciones**

   - Winamp

5. **Otros**

   - Northon antivirus Auto Project

4.2.2. Funcionamiento del Sistema.

SMAC, Sistema de mantenimiento asistido por computadora está enfocado a optimizar recursos, mejorar la planificación, controlar el mantenimiento de equipos e sistemas instalados en unidades navales y repartos (empresas). Este sistema cuenta con 5 módulos

importantes, tres Submódulos y tres utilitarios habilitados o adquiridos, que a continuación indicaremos (VER FIGURA 4.3):

- Módulo de Inventario
- Módulo de Fichas Técnicas
- Módulo de Lista de Base de Recambios
- Módulo de Mantenimiento
- Módulo de Personal
- Utilitarios Global Documentación Técnica
- Utilitarios Reporte Gestión
- Utilitarios Referencias Gráficas

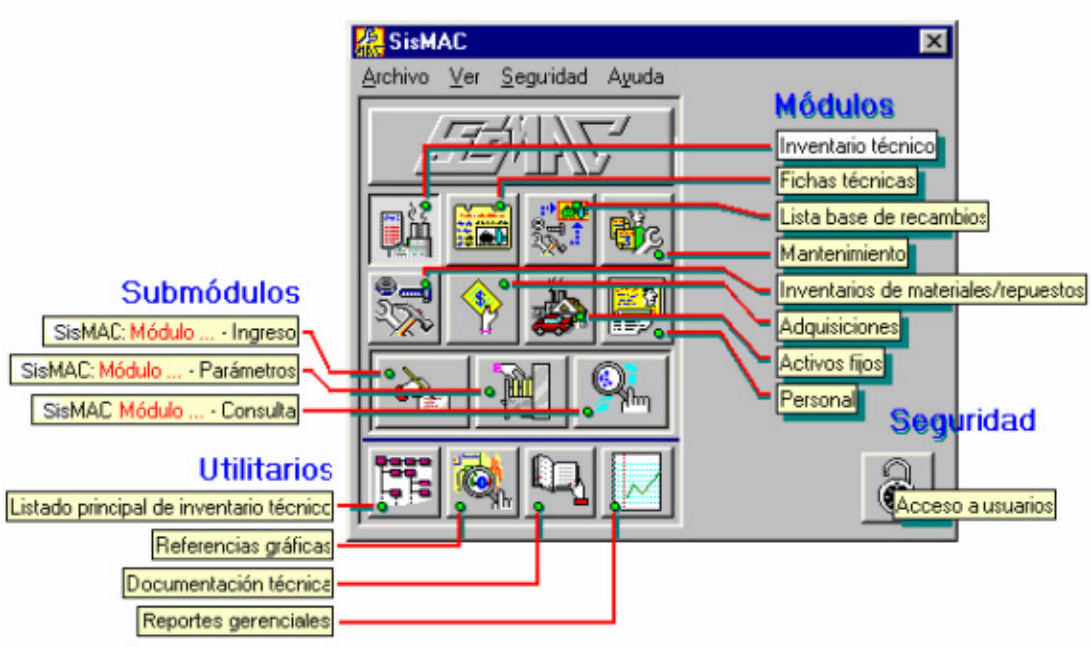
SMAC cuenta con una aplicación que permite ejecutar de manera automática la recepción de información con el CANOPUS (Control Administrativo de las Partidas Presupuestarias) a través de consultas definidas o parametrizadas que reflejen datos en el SMAC.

El SMAC interactúa con módulos preexistentes del sistema CANOPUS las cuales son:

- Módulo Inventario de materiales

- Módulo de Recursos Humanos
- Módulo de Inventario Repuestos
- Módulo de Adquisiciones

FIGURA 4.3
DESCRIPCION DE LOS MODULOS Y SUBMODULOS DEL SMAC



4.2.2.1. Descripción del proceso.

Como habíamos definido anteriormente en el alcance de esta auditoría, el análisis está enfocado a la evaluación de la opción orden de Trabajo y solicitud de trabajo en la acción de ingreso y consulta del módulo principal del SMAC que es el de mantenimiento.

Para dicho análisis, procederemos a explicar de manera breve el proceso de información que ejecuta el SMAC.

El SMAC cuenta con varios módulos tales como los módulos de Inventario, módulo de Ficha Técnica, módulo de Lista Base de Recambio, módulo de Personal y el módulo de Mantenimiento, las cuales permiten ingresar información parametrizada y puntual.

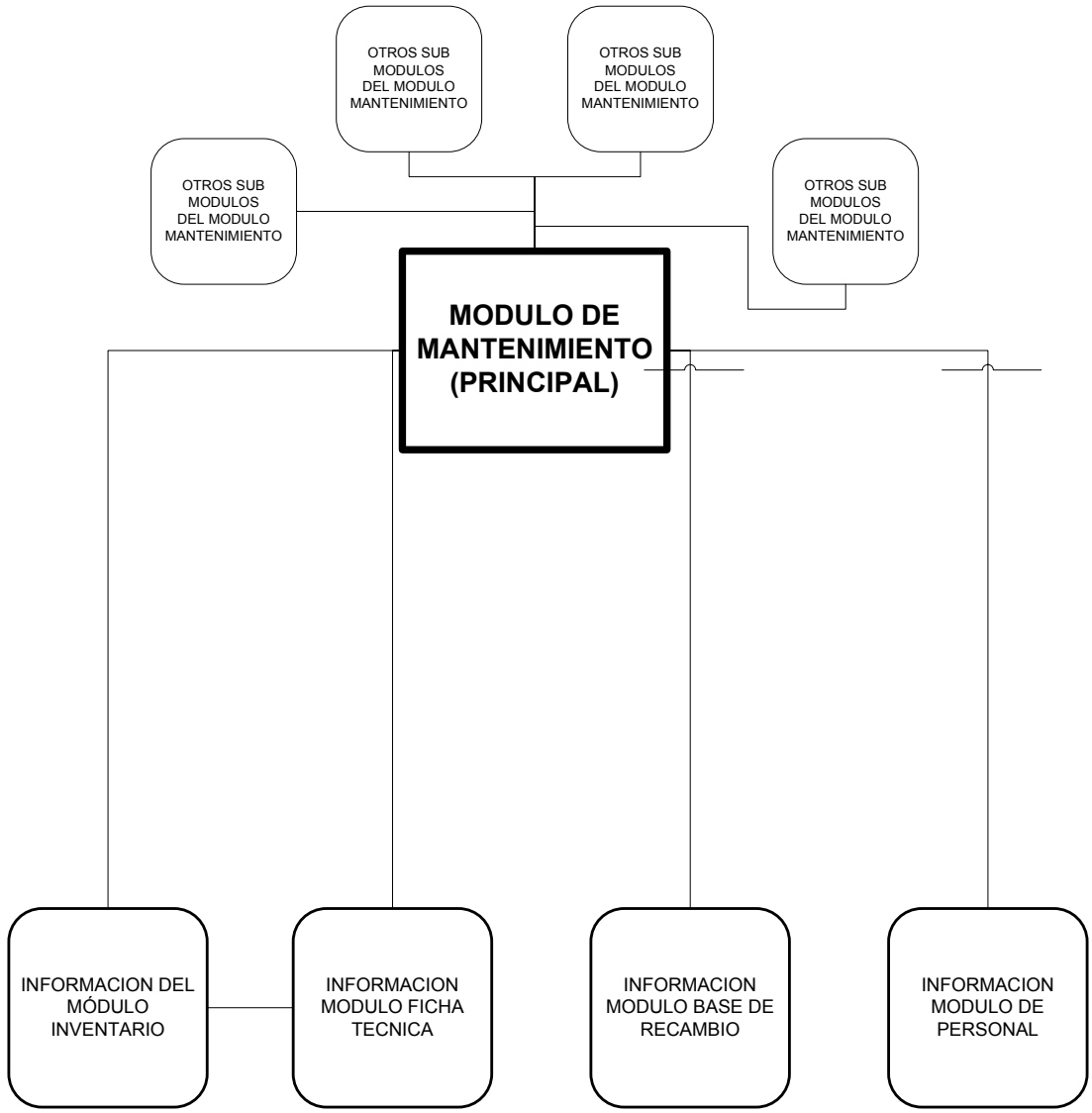
Dentro del módulo de mantenimiento se encuentra dos opciones fundamentales que son las que le van a dar vida y sentido al sistema de mantenimiento: SOLICITUD DE TRABAJO (S/T) Y ORDEN DE TRABAJO (O/T).

Estas dos opciones trabajan en forma lógica y secuencial ya que el reparto o unidad naval solicitante emite y envía una S/T con toda la información específica y necesaria del equipo o sistema a reparar, la cual es seleccionada y elegida desde los módulos ya mencionados anteriormente (módulos de Inventario, módulo de Ficha Técnica, módulo de Lista Base de Recambio, módulo de

Personal y el módulo de Mantenimiento), luego esta S/T es recibida, consultada y atendida por los laboratorios y talleres mediante el SMAC, para lo cual se emite una O/T que trabaja en forma interna para los trabajos de los laboratorios y talleres especializados a dar mantenimiento. Esta O/T es emitida, aprobada, programada y cerrada para lo cual se registra información con las características de cada mantenimiento tales como: los técnicos especialistas, las tareas a realizar, las fallas encontradas, los equipos y repuestos a necesitar, las horas hombres, el porcentaje de avance de cada Trabajo y otras observaciones pertinentes al caso.

Es muy importante destacar que cada S/T y O/T del módulo de mantenimiento recibe información de los otros módulos tales como: Ubicación específica de los equipos y sistemas de las unidades navales y repartos, las características técnicas de los equipos y sistemas, la vinculación de los repuestos, materiales y herramientas que se van a utilizar para dar mantenimiento, el personal asignado para dar mantenimiento y las tareas a ejecutar para dar dicho mantenimiento. (VER FIGURA 4.4)

FIGURA 4.4
FLUJO DE INFORMACIÓN DEL SMAC



4.2.2.2. Descripción de los módulos que integra el Sistema

4.2.2.2.1. Módulo de Inventarios

Del módulo de Inventario se recibe la información exacta de la ubicación de los bienes, equipos y sistemas que se encuentra en las unidades navales y repartos. Se debe codificar e inventariar todos los equipos y bienes de la empresa.

4.2.2.2.2. Módulo de Ficha Técnica.

Del módulo de Fichas técnica se recibe la información exacta de las características técnicas más relevantes de los equipos y sistemas, los cuales ayudará para una mejor identificación de los daños y repuestos a necesitar. Se debe codificar, registrar las características técnicas de cada equipo que se compre o que exista (part Number, serial; model, etc.)

4.2.2.2.3. Módulo Lista Base de Recambio.

Del módulo Lista Base de Recambio se recibe la información que vincula los repuestos, materiales, herramientas que

están registradas, clasificadas y codificadas en el inventario de bodega y hace relación con cada uno de los equipos, componentes y elementos de la empresa.

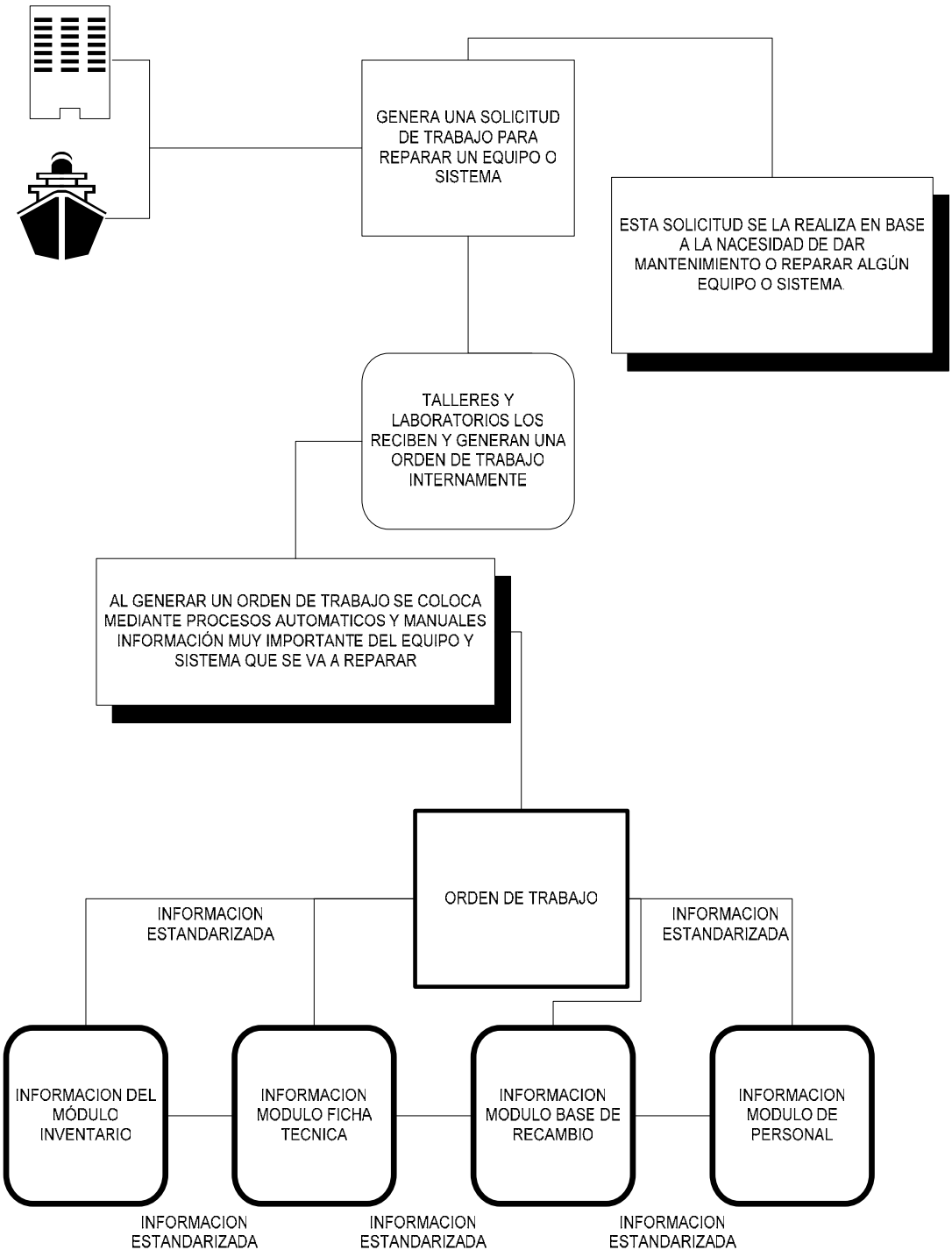
4.2.2.2.4. Módulo del Personal.

Del módulo del Personal se recibe información del tipo de empleado, técnico y especialización, para la asignación de una tarea de mantenimiento.

4.2.2.2.5. Módulo de Mantenimiento.

El módulo de mantenimiento es el más importante ya que este es el que va integrar toda la información pertinente y exacta de una acción, programación o ejecución de mantenimiento (VER FIGURA 4.5).

FIGURA 4.5
FLUJO DE INFORMACIÓN
DEL MODULO DE MANTENIMIENTO



Según el alcance establecido para dicha evaluación planteado anteriormente se tomará en consideración las opciones de Solicitud de Trabajo y Orden de Trabajo en la acción de ingreso y consulta.

Solicitud de Trabajo

La Solicitud de trabajo es el documento que da inicio al proceso de mantenimiento, ya que este es el que va establecer la necesidad de la unidad naval o reparto a reparar.

La solicitud de trabajo cuenta con 4 estados, los cuales son:

Emitida.- Esta Indica que la Solicitud de trabajo ha sido generada y emitida por una persona encargada de la unidad o reparto solicitante.

Ejecución.- Este estado se activa cuando el taller ha recibido la S/T y se ha generado una O/T para la ejecución del trabajo.

Cerrada.- Este estado se activa al momento de que el taller o técnico ha entregado el trabajo y el solicitante queda satisfecho.

Anulada.- Este estado es elegido cuando desean eliminar un S/T que no desean enviar a los talleres.

Orden de Trabajo

Una Orden de Trabajo es la orden documentada que mediante una aprobación se procede a ejecutarla. Existen dos tipos de denominación de Órdenes de trabajo:

- Ordenes de Trabajo Directa
- Ordenes de Trabajo No Directa.

Estos dos tipos de denominaciones de Órdenes de Trabajo cumplen las mismas funciones, pero la diferencia radica en la forma de emitirlo. La Orden de Trabajo Directa es creada o emitida sin la necesidad previa de una Solicitud de Trabajo, esta es usada cuando se realizan trabajos entre los diferentes laboratorios y talleres. En cambio la Orden de

Trabajo No Directa es la que nace de la creación de una Solicitud de Trabajo, este tipo de Ordenes son realizadas entre el cliente (unidad Naval o solicitante) y el laboratorio o taller.

Los estados de las Orden de trabajos son:

Emitida.- Esta Indica que la orden de trabajo ha sido generada y emitida para que el técnico o taller proceda al análisis previo para ejecutar el trabajo.

Aprobada.- Este estado indica que la orden de trabajo ya está autorizada para dar mantenimiento, esta acción dependerá de jefe de cada laboratorio.

Ejecución.- Este estado se activa cuando el técnico designado para reparar consulta la O/T y procede llenar los datos básicos del mantenimiento. Esto indica que el trabajo ya se está ejecutando.

Cerrada.- Es estado se activa cuando la O/T ha sido terminada. El técnico es el encargado de cerrar la O/T.

Anulada.- Este estado es elegido cuando desean eliminar un O/T que no desean generar.

Dentro de la Orden de trabajo encontramos las opciones para almacenar datos, las cuales son:

Editar O/T.- Esta opción permite Programar la Orden de Trabajo en tiempo, recurso y datos específicos de donde se va realizar el trabajo, los motivos y el centro de donde se leen los inventarios y la ubicación de sistema.

Editar Tareas.- Asignar las tareas a los equipos y sistemas en base a una lista clasificada e inventariada de los equipos.

Editar Materiales.- Asignar los materiales a utilizar en el mantenimiento de los equipos y sistemas en base a una lista clasificada e inventariada de las bodegas.

Editar Herramientas.- Asignar las herramientas a utilizar en el mantenimiento de los equipos y sistemas en base a una lista clasificada e inventariada de las bodegas.

Editar Mano de Hombre.- Asignar el número de los técnicos que intervienen en el trabajo y la asignación de las Horas Hombres utilizadas en esa O/T por día programado.

Editar Facturas. Registrar las facturas de los repuestos que se compraron y no pasaron por las bodegas, pero que sirve para reparar un equipo o sistema.

4.2.2.3. Procesos

4.2.2.3.1. Manuales

Los datos ingresados a las bases o tablas de los módulos de Inventario, Ficha técnica, Base de Recambio y de Personal son ingresados mediante digitación, por lo tanto son procesos manuales. Hay que tomar muy en cuenta que estos

procesos manuales sólo se los realizan una vez, específicamente cuando se codifica y se procede a inventariar e ingresar los equipos o sistemas en las bases de datos.

4.2.2.3.2. Automáticos.

Los procesos del sistema son automatizados pues toma la información de otros módulos y realiza las respectivas asignaciones y distribución a las demás bases de datos del sistema.

4.2.2.3.3. Descentralizados

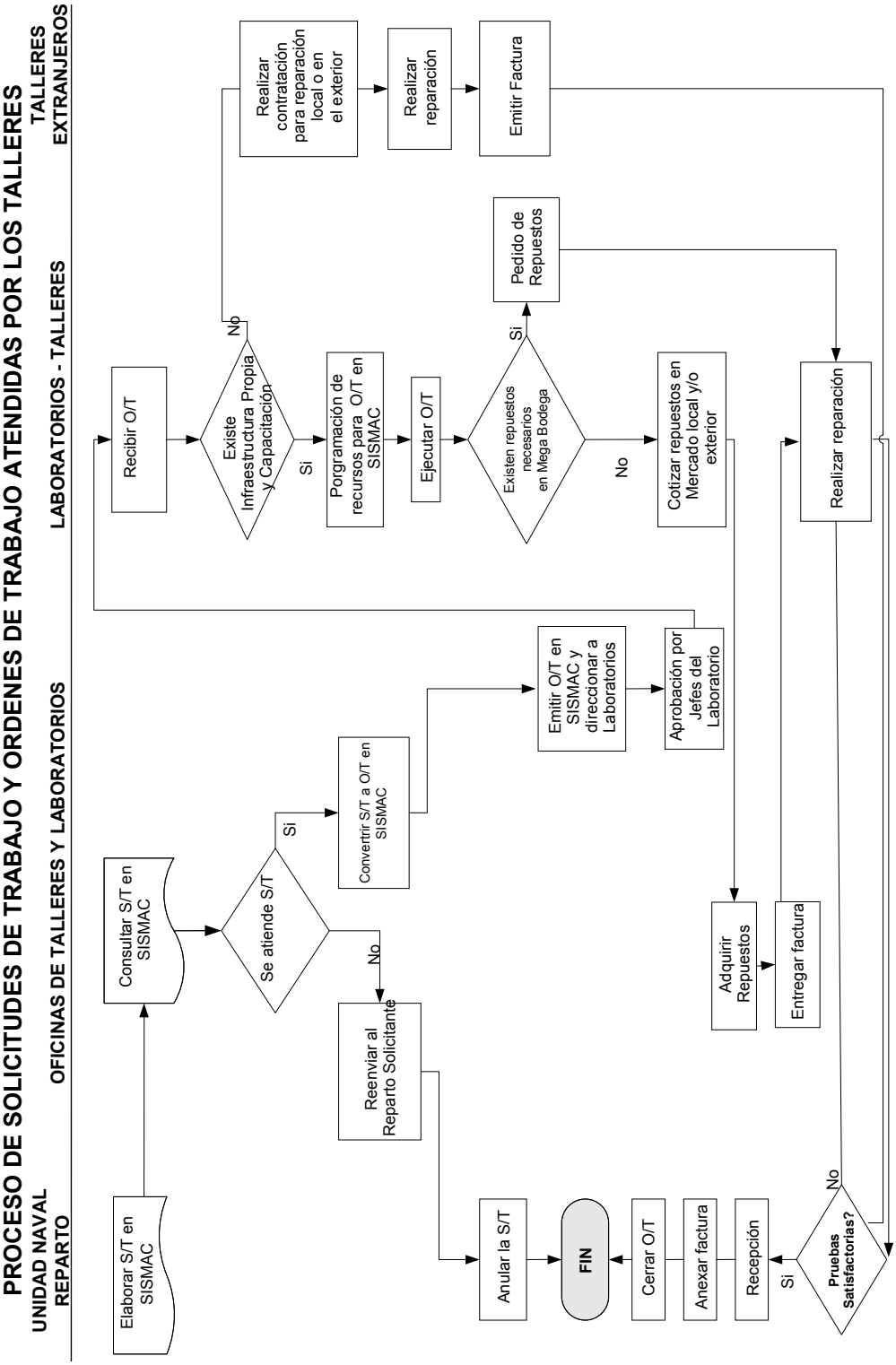
La generación del proceso que alimenta las otras bases de datos del sistema, al momento de crear, programar, ejecutar y cerrar las solicitudes y órdenes de trabajo se lo realiza por cada persona o técnico encargado que tenga permiso y acceso al sistema.

4.2.2.4. Diagrama de Procesos

4.2.2.4.1. Flujo de Información

El proceso de información en el sistema nace mediante la necesidad de los clientes que en este caso son las Unidades navales o repartos luego esta información es recibida por un encargado administrativo del SMAC y procede a elaborar o crear una orden de trabajo de mantenimiento la cual se le asigna los datos necesarios como el técnico y mano de obra a utilizar, los repuestos a necesitar, el tipo de mantenimiento a realizar de acuerdo a la ubicación del daño del sistema. Esta asignación se la realiza en base a los conocimientos y criterios de cada técnico especialista (VER FIGURA 4.6).

FIGURA 4.6
PROCESO DE LAS SOLICITUDES Y ÓRDENES DE TRABAJO ATENDIDAS POR LOS TALLERES



4.2.2.4.2. Proceso Batch.

Previamente sabemos que cada unidad naval posee cierta cantidad de computadoras conectadas al SMAC para solicitar todo tipo de mantenimiento.

El proceso Batch se lo realiza al momento en que una unidad naval llega de una navegación, esto se debe a la falta de alcance de la señal inalámbrica del SMAC con las respectivas bases de datos y de aplicación. Debido a esto se procede a instalar un servidor de aplicaciones y servidor de datos a cada unidad, para que cuando regresen se proceda a la consolidación de los lotes de transacción que en este caso sería todas las Solicitudes de Trabajos emitidas, cerradas y anuladas que se presentaron en dicha navegación. Esta consolidación de lotes de datos es realizada en forma manual, monitoreada y ejecutada por la red o también llevando los computadores al centro de administración de los servidores master y allí realizar el proceso Batch.

1. Proceso de solicitudes de trabajo
2. Proceso de Orden de Trabajo

4.2.2.4.3. Consulta de archivos.

Existe un diversidad de consultas que se las puede realizar mediante pantalla o bajando dicho archivo a Excel. Entre las consultas más importantes tenemos:

Órdenes de trabajo

Por número de O/T

Por Fecha de emisión

Por Fecha de Programación

Por Fecha de Ejecución

Por Fecha de Cierre

Por Actividad a realizar

Por mano de obra asignada (técnicos)

Por Unidad Naval o reparto solicitante

Por laboratorio que ejecuta

Solicitud de Trabajo

Por número de S/T

Por Fecha de emisión

Por Fecha de Cierre

Por Actividad a realizar

Por Unidad Naval o reparto solicitante

4.2.2.4.4. Salidas Impresas.

Entre los principales listados que se generan de este sistema tenemos:

- Formato Orden de trabajo (llenos)
- Formato Solicitud de trabajo (llenos)
- Formato Pedido de material (llenos)
- Consultas de Orden de trabajo
- Consultas de Solicitud de trabajo
- Informes estadísticos del estado de las Órdenes de trabajo
- Informe de los costos por unidad y orden de trabajo

4.3. Evaluación de Controles y Seguridades.

Pare efecto de trabajo se ha procedido a evaluar y analizar los controles y seguridades mínimas que deben poseer los sistemas de información y

en cierto grado los controles generales de la administración de un sistema.

Cabe mencionar que para la ejecución de las diferentes pruebas realizadas nos hemos basado en las Técnicas de Auditoría Informática de Aplicaciones en Producción, las cuales son muy similares a las CAATs Técnicas de Auditoría Asistida por Computadoras.

A continuación mostraremos una pequeña guía de todas las técnicas de auditoría informática para aplicaciones en producción que usaremos en nuestra evaluación al sistema, la cual nos ayudará a tener una mayor comprensión y orientación de todas las técnicas y las secciones donde serán utilizadas.

Técnica para establecer el orden de prioridad en el Auditaje.

Debido a las situaciones de tiempo, recursos, alcance y a las indagaciones realizadas, decidimos aplicar la Técnica Sistema de Puntaje (SCORING) para seleccionar el módulo de mayor relevancia en confidencialidad, integridad y disponibilidad de información.

Esta técnica consiste en valorar las características más importantes de los módulos del sistema, para lo cual hemos establecido estas 3 variables de mayor importancia.

- Emite y registra la información de las órdenes de mantenimiento
- Mayor riesgo de manipulación de datos
- Permite controlar las acciones de mantenimiento.

La valoración de cada módulo del sistema mediante el Sistema de Puntaje SCORING nos ha dado como resultado que el módulo de mantenimiento es el que ejecuta y guarda información de mayor relevancia para el sistema. Ver papeles de trabajo ref PA que se encuentra en el (ANEXO 2).

Dentro del módulo de mantenimiento se evaluará la opción S/T y O/T, los cuales ya fueron mencionamos anteriormente.

Técnica para operacionalizar y ejecutar el Programa de auditoría.

Es muy importante establecer que para efecto de operacionalizar las funciones de auditoría nos hemos basado en Técnica Centro de Competencia, ya que la información esta centralizada en un mismo

sector, existe un servidor de datos y aplicación conectado a todas las computadores inteligente lo cual permite ejecutar el programa de auditoría en forma manual desde un solo sitio.

Técnicas para probar controles de aplicaciones en Producción

Esta técnica es utilizada para probar la efectividad de los controles existentes tales como: evaluación de controles específicos, verificación de validación, pruebas de perfiles de acceso, pruebas de transacciones seleccionadas entre otros. Por dicho efecto hemos seleccionado la Técnica de Facilidad de Prueba Integrada (ITF). Esta técnica sirve para realizar los tipos de pruebas antes mencionados, pero con la característica que estás pruebas se las ejecuta en el sistema de aplicación real, mezclando datos de pruebas con datos reales.

Esta técnica la utilizaremos en las secciones 4.3.2 Controles de acceso a principales programas del módulo y 4.3.3. Controles de Edición y validación de programas. Ya que, estas secciones son las que van a tratar la existencia y efectividad de los controles y seguridades en lo que se refiere a perfiles de acceso y validaciones de campos.

Técnicas para seleccionar y monitorear transacciones

Esta técnica es para seleccionar y evaluar las transacciones realizadas, ya sean reales o de pruebas. Es muy importante definir una técnica de selección y monitoreo, ya que esta es la que va a definir la forma de obtener pruebas suficientes que puedan garantizar y aseverar las debilidades encontradas y que posteriormente serán publicadas en el informe de auditoría. Para dicho efecto hemos seleccionado la Técnica Archivo de Revisión de Auditoría por Muestreo (SARF). Esta técnica consiste en seleccionar las transacciones para evaluarlas mediante cualquier técnica estadística por muestreo. Para dicho efecto utilizaremos el método estadístico muestreo aleatorio simple. Y la Técnica de Registros extendidos la cual consiste en la revisión y evaluación de los pequeños programas y archivos de control llamados LOG o también conocidos como pistas de auditoría.

Estas técnicas la utilizaremos en las secciones 4.3.2 Controles de acceso a principales programas del módulo y 4.3.3. Controles de Edición y validación de programas. Ya que en estas secciones vamos a trabajar con datos los cuales serán generados mediante la realización de transacciones de pruebas sobre todo en lo que refiere al acceso de usuarios por perfiles y la verificación de validación de los campos.

Técnica para el examen de archivos

Esta técnica es empleada para evaluar los diferentes tipos de archivos tales como: el archivo de permisos o claves de accesos, archivos generados por las transacciones realizadas, datos de las tablas de la base de datos, entre otros. Para este efecto hemos seleccionado la Técnica Programas Generalizados de Auditoría. Esta técnica consiste en utilizar un software o paquete de auditoría generalizado, enfocado a la recepción o importación, clasificación, extracción, inserción, mezcla, comparación, cálculo, selección, evaluación y otras actividades. Para una correcta y eficiente ejecución de pruebas. Este tipo de técnica es relevante ya que este software de auditoría especializado permite no alterar, no cambiar, no manipular los datos sacados para pruebas, lo cual va influenciar en la neutralidad de las pruebas.

Para efecto de rapidez, confiabilidad, neutralidad hemos procedido a utilizar el software IDEA (Interactive Data Extraction and Analyses) lo cual certifica la utilización de la Técnica Programas Generalizados de Auditoría.

Esta técnica la utilizaremos en las secciones 4.3.1 Controles de claves de acceso al Sistema y 4.3.3. Controles de Edición y validación de programas. Ya que en estas secciones vamos a trabajar con una serie de archivos generados, tales como el archivo de claves de acceso, los archivos de las tablas de la base de datos, los archivos generados por las pruebas de perfil de acceso a módulos.

Técnicas para examinar programas de aplicación.

De manera rápida y por control general se procederá a evaluar ciertas aplicaciones instaladas en los computadores, con el objetivo de verificar la exactitud o cambios que afecten total o parcialmente las acciones del sistema. Para dicho efecto utilizaremos la Técnica Control de Bytes.

Previamente se ha elaborado y aplicado un cuestionario de visita previa y posteriormente un programa de trabajo con sus respectivos cuestionarios de prueba en el cual evaluaremos todos los aspectos de conocimiento general concerniente al sistema, tales como la familiarización y documentación del sistema y las funciones prácticas que realiza. Ver Programa de Trabajo ref A que se encuentra en el (ANEXO 1) con los respectivos papeles de trabajo ref. CVP, CCG los cuales se encuentra en el (ANEXO 2)

4.3.1. Controles de claves de acceso al sistema.

Debemos tener en cuenta que las claves de acceso son controles que permiten poseer un mayor grado de seguridad en la integridad y confidencialidad de la información, esta medida de control ayuda a mitigar el riesgo de vulnerabilidad o fraude informático.

Para evaluar las claves de acceso del sistema nos hemos enfocado en los siguientes puntos en lo que se refiere a su creación.

- Las claves de acceso no deben estar compuestas por códigos o nombres de empleados ya que es de fácil deducción.
- Las Claves de acceso deben ser individuales, es decir que esta pertenezca a un solo usuario, esto ayuda a establecer responsabilidades y permite hacer un seguimiento de transacciones.
- Las claves de acceso deben ser confidenciales, no deben ser divulgadas.
- Las claves no deben ser significativas, estas deben estar realizadas en base a combinaciones de códigos, números y caracteres.

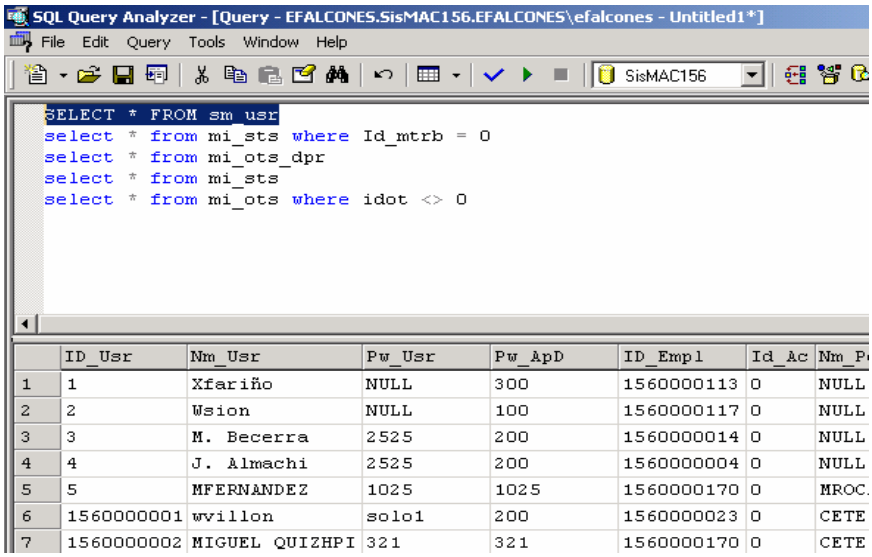
Una vez establecidos los aspectos de control procederemos realizar nuestro análisis de claves de accesos (password) mediante la ejecución de pruebas de control.

Para iniciar el proceso de evaluación procedimos a realizar las entrevistas con cada uno del personal que trabaja en el área de la administración del SMAC. Para esto aplicamos una serie de cuestionarios en las cuales consultamos información de tipo general y específica al sistema, por ejemplo ¿Quién o quienes administra el sistema?, ¿Cuántas personas Trabajan en el departamento que administra el sistema?, ¿Cuántos usuarios del sistema están activos?, ¿Cuál es la longitud de las claves de acceso?, ¿Existen claves de accesos debidamente elaboradas?, ¿Las claves de acceso son encriptadas?, etc. Para tener una mejor apreciación de las preguntas y evaluaciones realizadas deben ver los papeles de trabajo ref CCG, CP7 que se encuentra en el (ANEXO 2).

Ahora que ya pudimos tener mayor conocimiento y entendimiento de las funciones y aspectos que realiza el departamento que administra el sistema, procedimos a solicitar al administrador de la base de

datos y al de aplicaciones el archivo donde se encuentran todos los usuarios con sus respectivas claves de accesos (password) y permisos. Para esto procedimos a extraer todos los datos mediante una consulta de la tabla de claves de acceso mediante la utilización de la herramienta informática SQL.

Luego procedimos a evaluar dicho archivo mediante la utilización del software de auditoría IDEA.



	ID_Usr	Nm_Usr	Pw_Usr	Pw_ApD	ID_Empl	Id_Ac	Nm_P
1	1	Xfariño	NULL	300	1560000113	0	NULL
2	2	Wsion	NULL	100	1560000117	0	NULL
3	3	M. Becerra	2525	200	1560000014	0	NULL
4	4	J. Almachi	2525	200	1560000004	0	NULL
5	5	MFERNANDEZ	1025	1025	1560000170	0	MROC
6	1560000001	wvillon	solo1	200	1560000023	0	CETE
7	1560000002	MIGUEL QUIZHPI	321	321	1560000170	0	CETE

FIGURA 4.7 Consulta en la base de datos del SMAC

La figura 4.7 muestra la utilización de SQL para realizar la consulta para extraer los datos del archivo de claves de acceso y procederlos a evaluarlos.

4.3.1.1. Revisión de archivos (IDEA).

Una vez extraído el archivo de autorizaciones donde se encuentran todos los usuarios con las respectivas claves de acceso procedemos a evaluarlos mediante un software de auditoría llamado IDEA (Interactive Data extraction and analyze), la aplicación de este software se debe a que se son muchos datos, se desea que la evaluación sea lo más neutral posible y que se evita la manipulación de los datos, vale recalcar que mediante el uso de IDEA estamos recurriendo a un programa generalizado de auditoría, el cual muestra la aplicación de una de las técnicas de examen de archivo.

Una vez extraídos los datos del archivo a Access, lo procedemos a exportar en un archivo tipo TXT con el nombre de CLAVES en la carpeta C:\IDEA\DATA\CLAVES.TXT. Esta exportación se la realiza para poder leer los datos del Software IDEA. Una vez que exportamos pasamos a leerlo y conectarlo en el software IDEA. Ahora que ya esta conectado y leído por IDEA procedemos a elaborar una serie de instrucciones o ecuaciones de control, estas ecuaciones son las que van a definir los tipos de controles a evaluar. En este caso hemos definido instrucciones para

analizar el rango de claves de acceso, la repetición entre claves de acceso y aprobación, la repetición de claves por usuarios, y control del tipo de formato que deben tener las claves. Después de definir todas estas instrucciones procedemos a documentar todas estas pruebas realizadas para tenerlas como papeles de auditoría.

Para efecto de diseño y apreciación hemos documentado estas pruebas mediante pantallazos en Microsoft Excel los cuales están denominados como figuras.

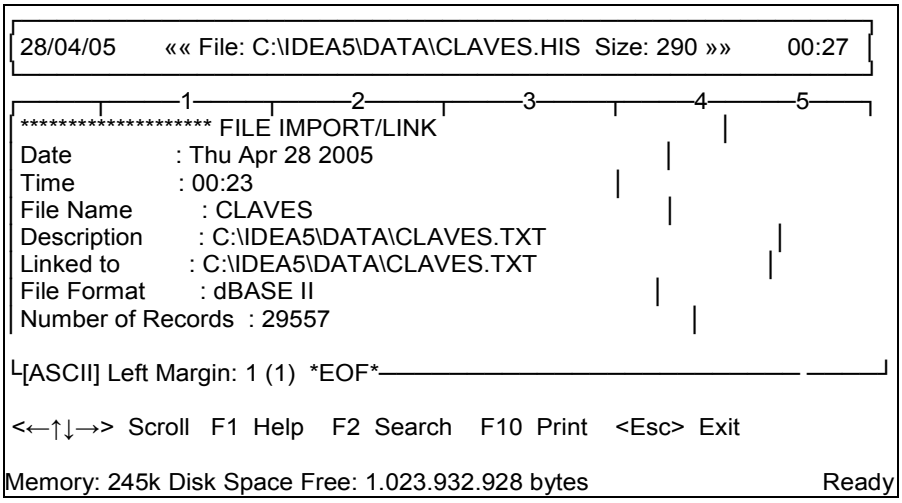
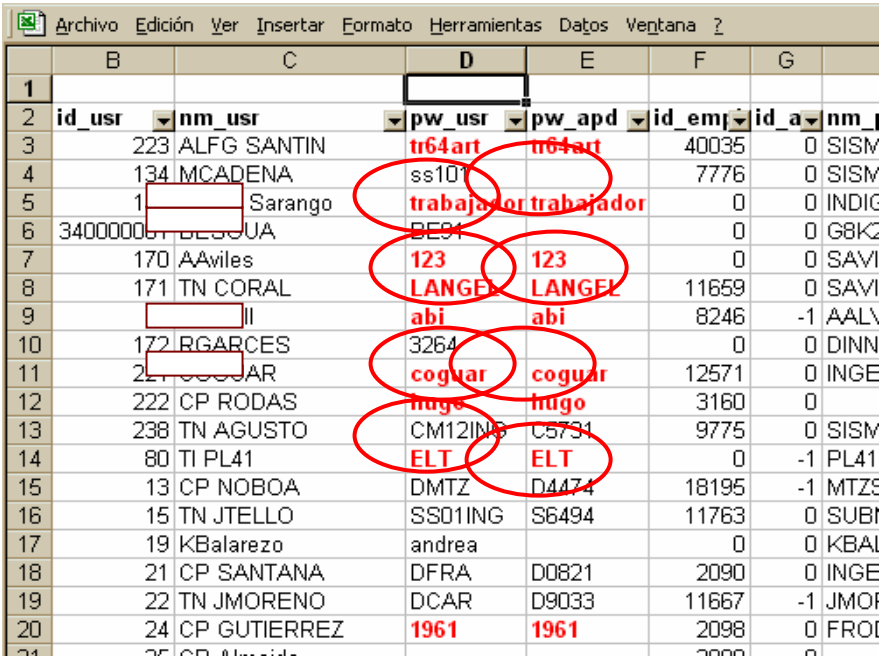


FIGURA 4.8 Prueba de Auditoría Aplicación de IDEA

La figura 4.8 nos muestra que se creo una base de datos tipo TXT llamado claves.txt para que sea leído por el Software de Auditoría IDEA. La ejecución de esta evaluación es la parte principal del estudio del archivo de autorización.

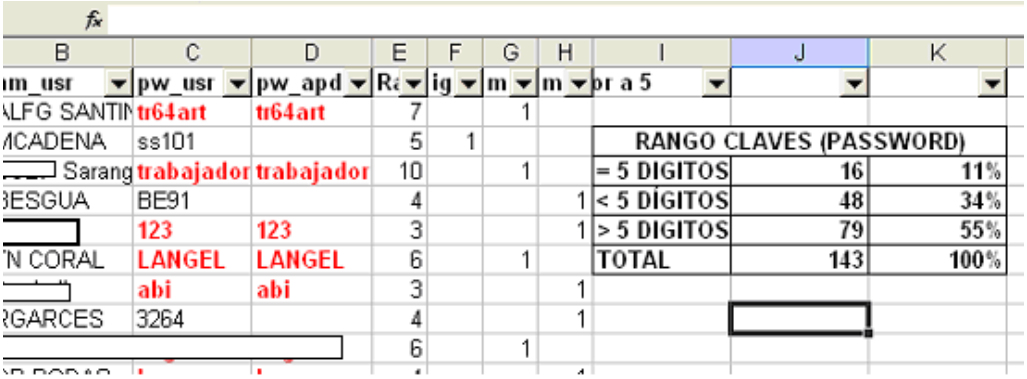


Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

	B	C	D	E	F	G
1						
2	id_usr	nm_usr	pw_usr	pw_apd	id_emp	id_a
3	223	ALFG SANTIN	tr64art	tr64art	40035	0
4	134	MCADENA	ss101		7776	0
5	1	Sarango	trabajador	trabajador	0	0
6	3400000	UA	BE91		0	0
7	170	AAviles	123	123	0	0
8	171	TN CORAL	LANGEL	LANGEL	11659	0
9			abi	abi	8246	-1
10	172	RGARCES	3264		0	0
11	22	AR	cogUar	cogUar	12571	0
12	222	CP RODAS	hugo	hugo	3160	0
13	238	TN AGUSTO	CM12ING	C5731	9775	0
14	80	TI PL41	ELT	ELT	0	-1
15	13	CP NOBOA	DMTZ	D4474	18195	-1
16	15	TN JTELLO	SS01ING	S6494	11763	0
17	19	KBalarezo	andrea		0	0
18	21	CP SANTANA	DFRA	D0821	2090	0
19	22	TN JMORENO	DCAR	D9033	11667	-1
20	24	CP GUTIERREZ	1961	1961	2098	0

FIGURA 4.9 Prueba de Auditoría-Consulta de claves de acceso

La figura 4.9 nos indica que se realizó la respectiva evaluación a las claves y contraseñas con respecto a la independencia, generación, longitud, y estandarización.



B	C	D	E	F	G	H	I	J	K
m_usr	pw_usr	pw_apd	R	ig	m	m	r a 5		
LFG SANTIN	tr64art	tr64art	7		1				
CADENA	ss101		5	1			RANGO CLAVES (PASSWORD)		
Sarang	trabajador	trabajador	10		1		= 5 DIGITOS	16	11%
ESGUA	BE91		4			1	< 5 DIGITOS	48	34%
	123	123	3			1	> 5 DIGITOS	79	55%
N CORAL	LANGEL	LANGEL	6		1		TOTAL	143	100%
	abi	abi	3			1			
RGARCES	3264		4			1			
			6		1				

FIGURA 4.10 Prueba de Auditoría- Longitud de las claves de acceso.

La figura 4.10 muestra la evaluación de la longitud de las claves de accesos, lo cual indica que solo el 11% del total de claves cumplía con la disposición verbal de que cada clave debe tener una longitud de 5 dígitos. Dicha disposición no se cumple.

Así mismo hemos procedido a evaluar el total de claves de acceso, para lo cual mostramos el siguiente análisis.

Análisis del Control de las claves de acceso al Sistema

Producto de la revisión y evaluación de la tabla donde se encuentra los usuarios con las respectivas claves de acceso al sistema y las claves para autorización, pudimos observar lo siguiente:

Existen 162 usuarios registrados en la base de datos, de los cuales el 9% se encuentra asignados a ciertos usuarios pero desactivados, el 1% no se encuentra asignado a ningún usuario (blanco). Quedando un total de 147 usuarios y claves activas.

De los 147 usuarios que se encuentran activos el 27% corresponden a usuarios que poseen claves con la Propiedad de solo acceso al sistema, el 2% corresponden a usuarios con claves de solo autorización y el 62% corresponden a usuarios con claves de acceso y claves para autorización.

Del Total de usuarios que poseen claves de acceso al sistema el 25% tienen claves repetidas.

Del Total de usuarios que poseen claves de acceso al sistema y claves de autorización el 40% posee claves idénticas.

Del Total de usuarios que poseen solo claves de acceso al sistema el 44% tienen adicionalmente una clave de tipo autorización pero desactivadas.

Producto de la aplicación del cuestionario ref CP6 y CP7 que se encuentra en el ANEXO 2 y de las evaluaciones realizadas mediante IDEA y Microsoft Excel hemos detectado lo siguiente:

- El archivo de autorización no posee un control de encriptación de las claves de acceso (passwords).

- No existe una política documentada y debidamente legalizada para la asignación, actualización, eliminación.
- Las claves de acceso no poseen un adecuado formato en lo que respecta a la elaboración ya que existen claves de todo tipo tales como: nombres de personas, números secuénciales, apodos, formato de fechas, etc.
- No cumplen con la longitud de 5 dígitos previamente manifestada en el cuestionario de trabajo.
- Existen claves y cuentas sin usar que no han sido suprimidas
- Existen claves repetidas entre usuarios
- Existen claves de acceso y aprobación repetidas entre sí.

Ver papeles de trabajo ref CP6, CP7 que se encuentran en el (ANEXO 2).

4.3.1.2 Periodicidad en cambio de claves de acceso.

La periodicidad de cambio de claves es considerada como una norma de control en los sistemas de información, debido a que estos van a evitar la probabilidad de que personas no

autorizadas consigan acceso a acciones e información no permitida.

Para efecto de evaluación hemos aplicado una serie de preguntas referentes a las claves, administración de claves, periodicidad de cambios y actualización, las cuales se reflejan en el cuestionario CP7 que se encuentra en el anexo 2. Estas preguntas están enfocadas a la obtención de conocimiento referente a si existe o no existe controles de periodicidad de claves, políticas y procedimientos de actualización de claves, el encargado de realizar los cambios y actualización y si las cuentas sin usar son suprimidas. Ver papeles de trabajo ref CP7 que se encuentra en el (ANEXO 2)

Entrevistando a la administradora del servidor de aplicaciones nos indicó que los cambios y actualizaciones de claves es realizada cada año, generalmente en el mes de enero ya que es ahí el momento en que contratan, cambian o integran nuevo personal. Así mismo nos manifestó que las actualizaciones y cambios son realizadas porque el personal interesado lo solicita.

Producto de las pruebas realizadas, hemos detectado que no existe una adecuada política de actualización y cambios de claves de acceso. Por ende no existe un procedimiento para quitar el acceso cuando un empleado deja una posición laboral.

4.3.1.3 Administración de claves de acceso.

La administración de las claves de acceso es una de las funciones de mayor relevancia que cumple el administrador del sistema, ya que esta es la que va definir el principal patrón de control en lo que se refiere al permiso de acceso a módulos, ejecución de acciones y disponibilidad de información.

Producto de la aplicación de cuestionarios hemos podido identificar que existe una persona encargada de la administración de las claves de acceso, quien es la misma que administra el servidor de aplicaciones. La administradora del sistema cuenta con dos asistentes, los cuales son los encargados de brindar asesoría, soporte técnico y asistencia en el manejo del sistema a usuarios. Entre las funciones principales del administrador estas las de evaluar, confeccionar, asignar,

autorizar, actualizar y eliminar las claves de acceso al sistema. Ver los papeles de trabajo ref. CP7 que se encuentra en el (ANEXO 2)

Para efecto de evaluación hemos identificado la siguiente prueba de administración de claves de acceso en lo que se refiere a su confección.

NAV		CLAVE GENERADA				2366
Nu	CLAV	ESTADO	RESP	UNIDAD	DPTO	FECHA E
241	D0242	X	IMAICELA	NAV	AUXILIARES	
820	D0821	X		INAV	FRAGATAS	
3070	D3071	X	GUERRERO	NAV	SUB	01/02/2005
7111	D7112	X		NAV	CORBETAS	

FIGURA 4.11 Prueba de Auditoría-Generación de Claves

La figura 4.11 nos muestra que a pesar de que existe un sistema de generación de claves de acceso desarrollado en Microsoft Excel, se observó y registró que no existe una adecuada standarización de formato de claves de acceso en el archivo de autorizaciones, las cuales están reflejadas en las figuras anteriores 4.9 y 4.10

En lo que respecta a la administración de claves de acceso hemos identificado las siguientes debilidades:

- Falta de procedimientos documentados para receptar y evaluar la necesidad del usuario de tener una clave de acceso.
- No existe una bitácora donde se registren los errores y fallas del sistema para luego dar tramite a la reparación.
- Falta de estandarización de todas las claves de acceso a un solo formato.

Todas estas pruebas realizadas dentro del contexto de evaluación de la administración y diseño de control de claves de acceso nos han permitido identificar que la administración de acceso no permite que la información que exista en el sistema sea confiable e integra ya que las claves y manejo de estas no son efectivamente controladas.

4.3.2. Controles de acceso a principales programas del módulo.

Los controles de acceso son los que autorizan el uso de principales programas, ya que estos son los que van a permitir o evitar el acceso

a un módulo o menú y ejecute una acción permitida. Los controles de acceso están completamente ligados al establecimiento y administración de las claves de acceso, ya que sin estos permisos reflejados por los passwords no se podrá ingresar o ejecutar una acción en el sistema. Adicional a esto existe el control del acceso al sistema mediante pequeñas y básicas aplicaciones del sistema principal como el SOFTLOCK SERVER o los comúnmente llamado Log de transacciones y de errores.

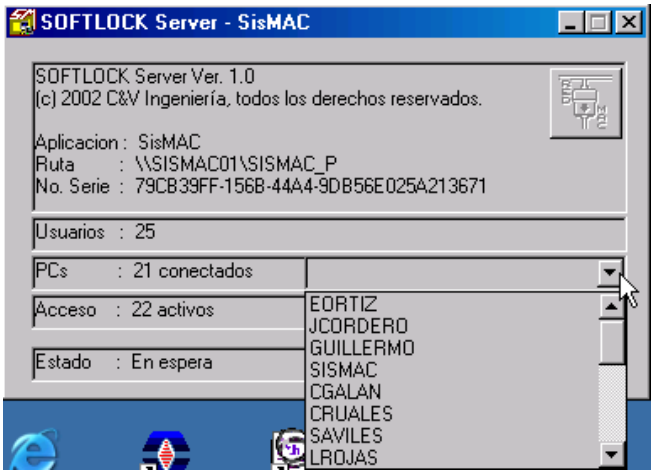


FIGURA 4.12 Monitoreo de los usuarios conectados al sistema

La figura 4.12 nos muestra la existencia del monitoreo y control adecuado de las acciones de los usuarios y máquinas que se encuentra conectados al servidor de aplicaciones.

FIGURA 4.13 Prueba de Auditoría- Log de errores y Log de transacciones

La figura 4.13 nos muestra la existencia de controles de secuencia e identificación de errores y transacciones reflejadas en Log de errores y Log de transacciones. Estos Log muestran la secuencia numérica y lógica de las transacciones realizadas, el usuario que generó dicho transacción o error, la hora, la fecha, la ubicación de la máquina, el tipo de acción o transacción y la falla generada.

Hay que tener claro que lo que se va a evaluar en esta sección es la correcta y efectiva determinación de permisos y perfiles de accesos de los usuarios de acuerdo al departamento, cargo, funciones y necesidades.

En esta evaluación de controles de acceso utilizaremos la técnica de facilidad de prueba integrada (ITF) para probar controles de aplicación en producción. Recordemos que esta técnica ITF es la que se aplica para evaluar controles específicos tales como pruebas de perfil de acceso, pruebas de transacción seleccionadas entre otros. Así mismo utilizaremos la técnica archivo de revisión de auditoría por muestreo para seleccionar y monitorear transacciones (SARF), ya que en esta sección realizaremos una serie de transacciones y ejecutaremos acciones para probar los perfiles y permisos de acceso que poseen ciertas claves.

Para efecto de evaluación hemos procedido a seleccionar una muestra considerable de claves de acceso según su perfil definido (basándonos en el muestreo aleatorio simple), para así proceder a probarlas y tratar de ejecutar acciones diferentes a las permitidas. Este tipo de prueba se la realizó en el aplicativo original con datos reales, simulando transacciones de pruebas para cumplir con las técnicas seleccionadas

Según las entrevistas previas los usuarios del SMAC tienen asignado los perfiles de acceso por unidades navales, repartos, talleres, sistemas y equipos de acuerdo a su función y ocupación en la estructura orgánica. Los tipos de usuarios de sistema son:

- Administrador del SMAC
- Asistencia al usuario
- Gerente de la empresa
- Jefe de talleres y laboratorios
- Jefe de secciones
- Técnicos
- Usuarios solicitantes (unidades navales y repartos)
- Jefe de los usuarios solicitantes

Solicitudes de Trabajo

Existen dos tipos de claves de acceso para las unidades navales y repartos solicitantes, una es para emitir, llenar datos y anular S/Ts. Y la otra es a nivel de jefe de usuarios solicitantes el cual sirve para consultar y eliminar S/Ts.

Ordenes de Trabajo

En las órdenes de trabajo también existen dos tipos de claves las cuales están enfocadas solo y exclusivamente a los talleres y laboratorios. Un tipo de clave es destinada al técnico y operador del sistema (administrativo), estas claves permite acceder al sistema, consultar S/T recibidas, generar y emitir O/Ts, programar O/Ts, anular y consultar. Y la otra es a nivel de jefes de Talleres y laboratorios el cual autoriza la aprobación y cierre de las O/Ts .

Previo al análisis y desarrollo de pruebas mencionaremos las opciones del módulo de mantenimiento con sus respectivos menús.

El módulo de Mantenimiento es el más importante de este sistema, este módulo consta de tres opciones que son las de Parámetros, Ingreso, Consultas. Cada opción cuenta con un menú muy particular, de los cuales mencionaremos los más importantes.

Parámetro

- Banco de tareas,
- Banco de mantenimiento
- Banco de medición.

Ingreso

- Solicitud de Trabajo (S/T)
- Orden de trabajo (O/T)

Consultas

- Orden de trabajo (O/T)

4.3.2.1. Parámetro.

En esta opción es donde se van a almacenar todas las directrices, lineamientos y parámetros para poder reparar un equipo o sistema, en esta opción se encuentran varias bases de datos en las cuales se van a registrar datos tales como:

- Los tipos de mantenimiento
- Los tipos de tareas
- Especialistas
- Rutinas de mantenimiento
- Modo de operación
- Documentos de mantenimientos

Todos estos datos son conocidos como bancos de Tareas, de mantenimientos, de medición, etc.

Aunque esta opción del módulo de mantenimiento no se encuentra en el alcance de la evaluación, hemos podido tener conocimiento general de que esta opción es uso exclusivo del jefe principal de Talleres Integrados, ya que este es el que va a delimitar todos los parámetros de mantenimiento al cual van a estar sujetos.

4.3.2.2. Ingreso.

Esta opción es de uso común y una de las más utilizadas e importantes. Dentro de este módulo encontramos el ingreso para generar una Solicitud de Trabajo y una Orden de Trabajo.

Solicitudes de Trabajo

Según lo investigado la solicitud de trabajo es el inicio de una acción de mantenimiento, esta es generada por una persona

responsable en la unidad naval o reparto solicitante, cabe mencionar que para que una persona pueda generar un S/T debe tener una clave de acceso al sistema la cual es entregada de acuerdo al tipo de permiso y acceso de acuerdo al reparto o unidad naval al que pertenece.

La solicitud de trabajo cuenta con 4 estados muy importantes, los cuales son monitoreados por el encargado de la asistencia al usuario.

Los estados de la S/T son:

- Emitida
- Ejecución
- Cerrada
- Anulada

Ordenes de Trabajo

Según lo indagado la orden de trabajo es el documento que se genera para realizar una reparación o mantenimiento, este nace

de la recepción de la S/T para luego ser generada, emitida, aprobada y cerrada. Cabe recalcar que para que una persona pueda emitir una O/T debe poseer una clave de acceso al sistema el cual es entregado de acuerdo al tipo de permiso y acceso por Talleres y laboratorios.

La orden de trabajo cuenta con 5 estados muy importantes, los cuales son monitoreados por el encargado de la asistencia al usuario.

Los estados de la O/T son:

- Emitida
- Aprobada
- Ejecución
- Cerrada
- Anulada

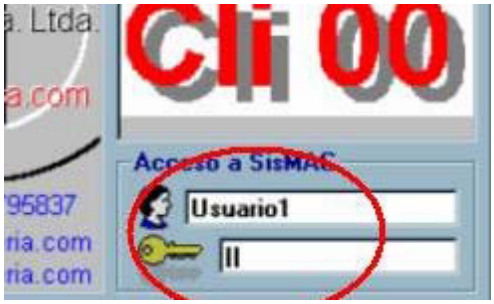


Figura 4.14 Prueba de Auditoría – Acceso al SMAC

La figura 4.14 nos muestra el módulo que permite o niega el ingreso al sistema.

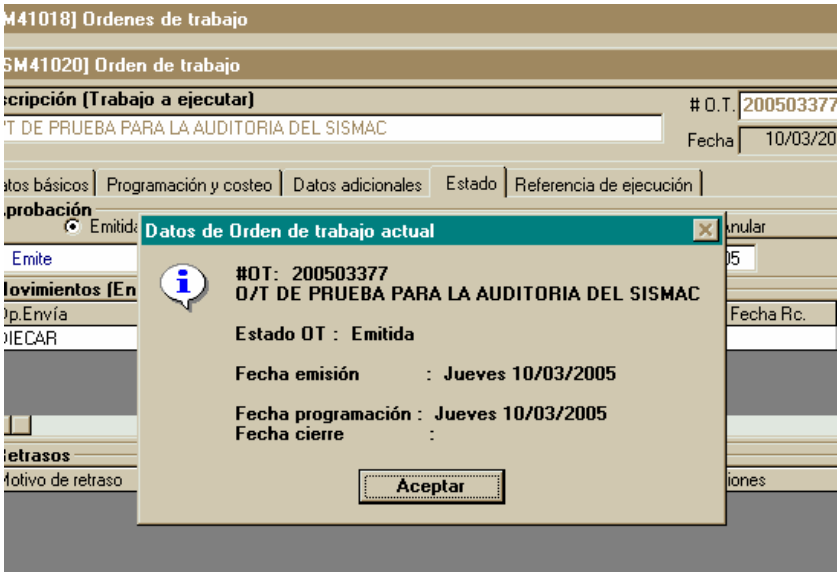


FIGURA 4.15 Prueba de Auditoría-Generación de una O/T de Prueba

La figura 4.15 nos indica de manera representativa la creación de O/Ts y S/Ts para comprobar los perfiles y permisos de acceso de

los usuarios, estás pruebas las explicaremos y enseñaremos a continuación.

Dentro de las pruebas realizadas pudimos detectar que toda clave de acceso al sistema puede generar una O/T utilizando una opción para emitir O/Ts seleccionado y colocando cualquier nombre de persona que se encuentra en un campo tipo combo. Esto nos indica que no guarda un debido nivel de acceso al sistema ya que cualquier persona puede generar y emitir órdenes de trabajo a conveniencia sobre todo en las O/Ts Directa. De esta forma le dará libertad a los técnicos para que pueda generar y emitir O/Ts inexistentes y aparentar carga de trabajo para luego hacerlas firmar como recibidas por amigos o conocidos de las unidades navales y repartos que supuestamente solicitaron.

Ver (FIGURA 4.16)

Figura 4.16 Prueba de Auditoría – facilidad para emitir O/T

La figura 4.16 nos muestra la facilidad que existe para que cualquier persona que tenga el acceso al sistema pueda generar y emitir una O/T mediante la selección de un nombre autorizado del combo – lista.

Debería existir una clave para emitir O/Ts que sean solos y exclusivos para las personas encargadas de emitir O/Ts ya que si no se da esto, puede que cualquier persona genere y emita O/Ts sin necesidad con Trabajos y conceptos errados y repetidos.

Hemos identificado que cualquier persona de un mismo taller y que tenga acceso al sistema puede controlar y manipular

fácilmente la información, ya sea programando, borrando, cambiando o anulando. Ver (FIGURA 4.17).

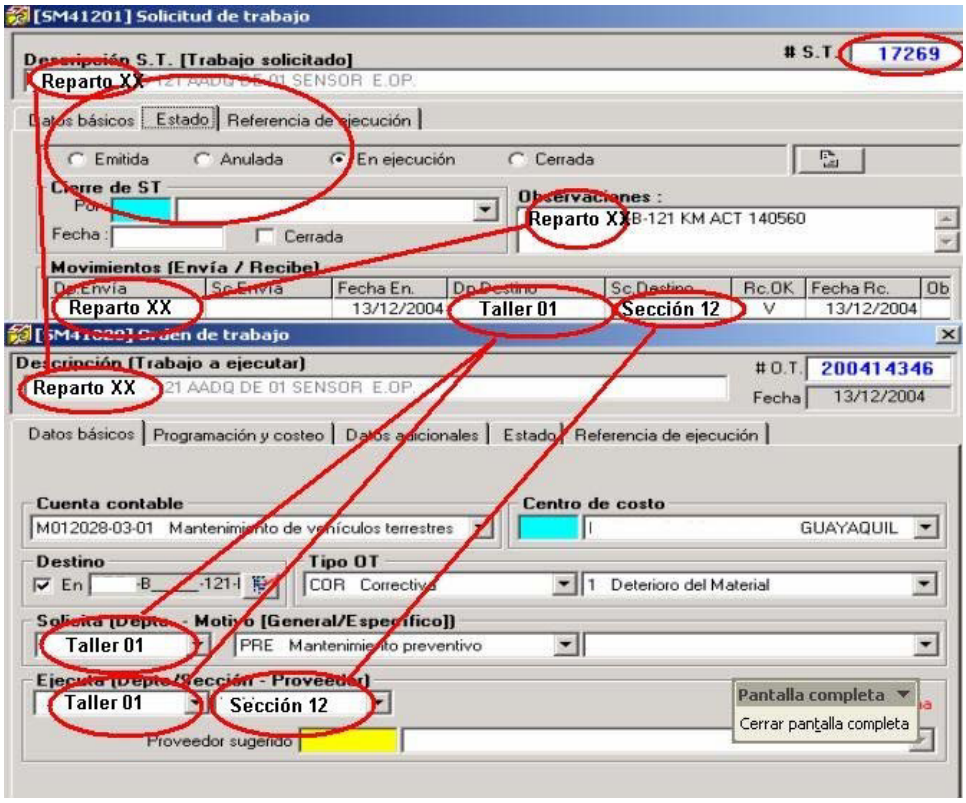


Figura 4.17 Prueba de Auditoría – facilidad para manipular la información

La figura 4.17 nos muestra la facilidad que existe para manipular la información entre personas y datos de un mismo taller, esta prueba se basa en ingresar con la clave de acceso de un usuario técnico y demostrar mediante la ejecución de S/T s y O/TS que tranquilamente puede hacerse uso y consulta de los datos deseados.

Enfocándonos a un solo taller, donde existen varias secciones como por ejemplo la electrónica y la de comunicación, se pudo probar que los jefes de una sección determinada que tiene clave de autorización (aprobar y cerrar) puede acceder a O/Ts de otras secciones y procederlas a autorizar aunque no sea de su sección establecida.

Otra de las pruebas realizadas nos muestra que entre talleres existe la posibilidad de generar una O/T Directa. Los encargados del sistema dicen que este tipo de O/T Directa es para que un taller solicite un trabajo o el complemento de un trabajo por medio de otro taller especializado. Producto de las pruebas realizadas hemos podido detectar que existen claves de acceso de personal de un taller que tiene permiso para generar una O/T directa, pero esta persona tiene acceso libre para emitir y manipular fácilmente dicha O/T. Es decir que puede programarla en tiempo y tareas, asignar los técnicos, registrar las horas hombres, selección de materiales, registro de observaciones, hasta la anulación de la misma O/T. También se da el caso de que estos talleres poseen claves de autorización (aprobación y cierre de O/T) para uso de su propio taller, pero mediante pruebas realizadas identificamos que el perfil de ciertos usuarios

permite autorizar O/Ts de otros talleres, es decir que en una O/T emitida por el Taller XX pudo ser autorizada (aprobada y cerrada) con una clave del Taller YY. Ver (FIGURA 4.18)

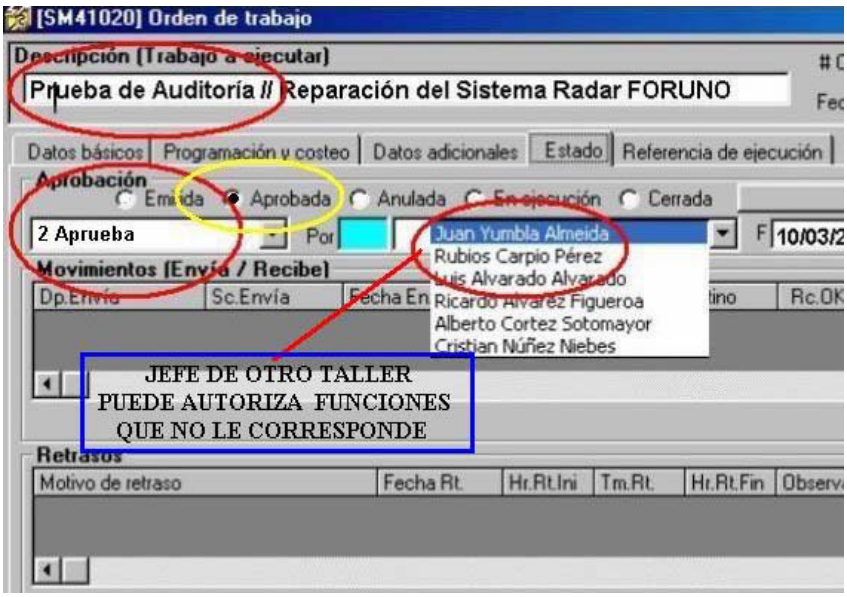


Figura 4.18 Prueba de Auditoría – Mal definido ciertos perfiles de autorización

La figura 4.18 nos muestra que existe una deficiencia en la asignación de perfiles de autorización de ciertos usuarios. La prueba realizada fue la de comprobar de que una persona de un Taller logre autorizar una O/T de otro taller, cosa que si se pudo.

Todas estas acciones muestran que el sistema permite fácil manipulación de datos por lo tanto la información no es integra y confiable. Esto se debe básicamente a la falta de una adecuada

asignación de perfiles de accesos a usuarios. Estos tipos de perfiles deben ser asignados en base a las funciones, departamento y cargo para así poder mantener un efectivo control a menús y acciones del sistema.

4.3.2.3. Consultas.

Producto de las pruebas realizadas hemos identificado que cualquier persona de cualquier reparto, unidad naval, talleres o laboratorios que tengan claves de acceso o de autorización puede consultar y tener conocimiento de la información referente a todas las solicitudes de trabajo y Ordenes de trabajos emitidos, en ejecución y cerradas. Ver (FIGURAS 4.19 Y 4.20)

A criterio del administrador y de varios usuarios expresan que este tipo de consulta permite tener una mayor visión y apreciación de lo que está en buen y mal estado y de lo que actualmente se está reparando.

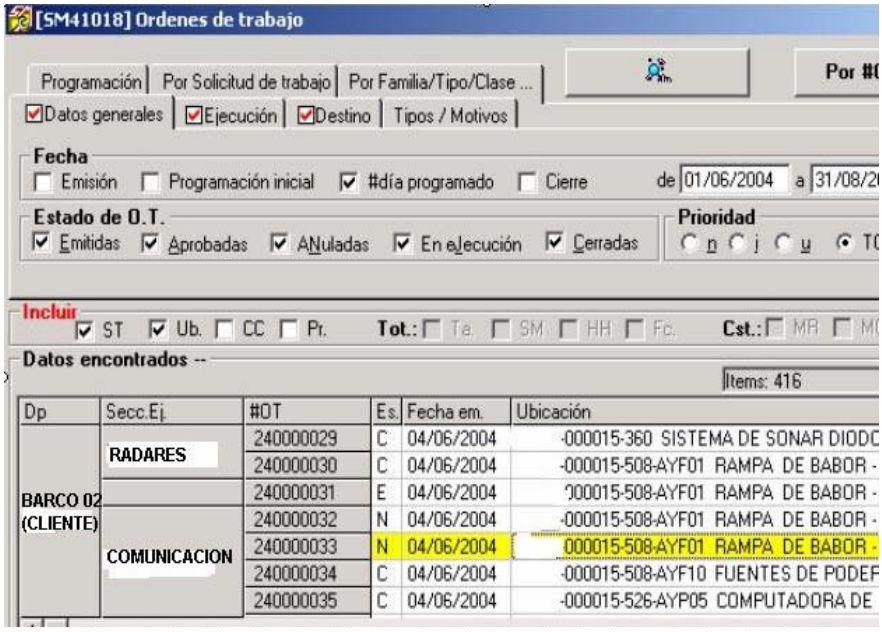


Figura 4.19 Prueba de Auditoría–Facilidad en ejecutar consultas de O/T

Figura 4.20 Prueba de Auditoría–Facilidad en ejecutar consultas de S/T

Las figuras 4.19 y 4.20 muestran los tipos de consultas que pueden realizarse. Esta prueba se la ejecutó con varias claves

de acceso y nos certificó que los perfiles de acceso están mal definidos.

Consideramos que este tipo de consulta no debería darse ya que personas ajenas a la institución ya sea la competencia, saboteadores o los propios empleados pueden acceder a información confidencial. Debería definirse en mayor y mejor grado el los perfiles de accesos para todas las consultas de acuerdo a las funciones y a el departamento.

4.3.3. Controles de Edición y Validación de Programas.

Verificación de datos en la opción de Ingreso y modificación

Este control garantiza la salida efectiva, íntegra, razonable y estándar de información dentro de un proceso sistemático establecido, previa al ingreso y modificación de datos en un sistema. Por dicha razón los campos más sensibles al sistema son sometidos a una evaluación previa antes de iniciar el proceso de información.

Existe una diversidad de controles de validación pero para efecto de nuestra evaluación hemos procedido a evaluar los siguientes controles de validaciones:

- Control de Formato
- Campo Faltante
- Razonabilidad

Es importante mencionar que para evaluar y realizar las pruebas pertinentes de control de validación nos hemos basado en la técnica facilidad de prueba integrada (ITF), recordemos que esta técnica se enfoca a probar y evaluar controles de aplicación en producción tales como controles específicos, verificación de validación, perfiles de acceso, pruebas de transacción seleccionadas, entre otros. Adicionalmente hemos utilizado la técnica archivo de revisión de auditoría por muestreo para seleccionar y monitorear transacciones y el Software IDEA ciertos campos de un archivo determinado.

Para efecto de evaluación hemos procedido a solicitar al administrador de la Base de Datos y al administrador del servidor de aplicaciones la autorización para que nos permita realizar una serie

de transacciones y consulta de datos reales y de prueba para verificar y analizar los campos de la O/T y S/T. Para efecto de pruebas hemos aplicado datos normales, ilógicos, imposibles y valores externos, para determinar la existencia o inexistencia de dichos controles de validaciones.

Control de Formato

La validación por control de formato es la que busca verificar que los campos cumplan con las características adecuadas de filtración para poder aceptar ciertos tipos de datos durante su ingreso, tales como Numérica, alfabética, alfanumérica, automático y que correspondan a una longitud específica. Basándonos en esta teoría hemos procedido a realizar varias pruebas de validación a varios campos de la opción Orden de trabajo y Solicitud de trabajo.

Esta prueba consiste en verificar el formato y la secuencia lógica de los números de las órdenes de trabajo y solicitudes de trabajo, para lo cual hemos procedido a extraer todos los datos de la tabla O/T y S/T de la Base de Dato e importarla a software IDEA para evaluar la secuencia lógica de los números y el tipo de formato de estos

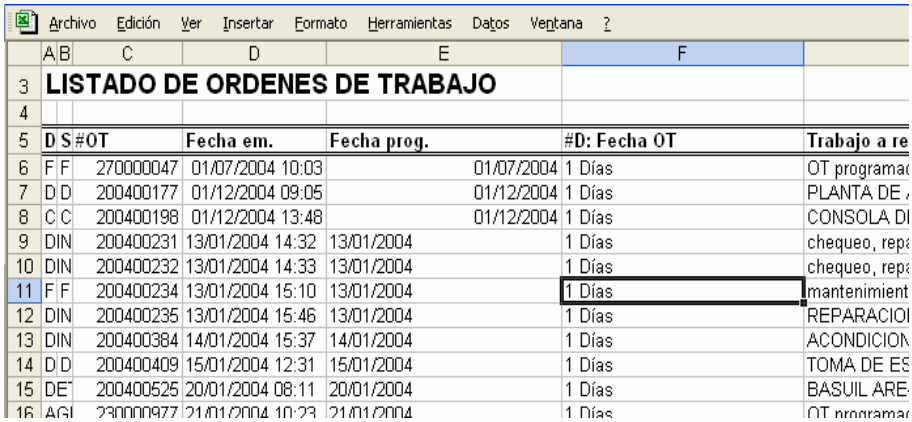
campos. Por efecto de presentación ver las (FIGURAS 4.21, 4.22, 4.23, 4.24).

Mediante la ejecución de esta prueba pudimos detectar que el número de la orden de trabajo es secuencial y autonumérico, pero existen distintos números de O/T y S/T al formato establecido. Esta diferencia se debe a los procesos batch realizados anteriormente por ende los cuales no afectaran al procesamiento de datos actual. Ver los papeles de trabajo ref. CP1, CP8 que se encuentra en el (ANEXO 2).

	id_ot	idot	id_pg	id_t	id_tc	id_tpr	id_p	
	149	149	3	4	0	3	0	MANTENIMIENTO DE LA COCINA (SISTEMA DE COCINA)
	156	156	3	4	0	3	0	(MOTOR ELECTRICO DE LOS CLIMATIZADORES CL3/A) CAI
	158	158	3	4	0	3	0	(ALTERNADOR DELCO N°1 E7370) CHEQUEO Y REPARACI
	164	164	3	4	0	3	0	cambio de rodamientos y confeccion del ventilador del motor el
	193	193	3	4	0	3	0	(ALTERNADOR DEL GENERADOR #3) MANTENIMIENTO PA
	194	194	3	4	0	3	0	PLANTA DE A/A #2 CHEQUEO DE FUGA DE FREON EN LA
	24370	200414824	3	4	0	3	0	MOTOR DETROIT 8V/71: INSPECCION Y MANTENIMIENTO D
	24371	200414825	3	4	0	3	0	INSPECCION, MEDICION Y EVALUACION DE 08 PISTONES,
	24372	200414826	3	4	0	3	0	CAMBIO DE ACEITE Y FILTROS
	24373	200414827	3	4	0	3	0	CHEQUEO Y REPARACION DEL AIRE ACONDICIONADO
	24374	200414828	3	4	0	3	0	CAMBIO DE 01 BATERIA; CAMBIO DE 04 LLANTAS, ALINEA
	24375	200414829	3	4	0	3	0	(MMPP #1) ENFRIADOR DE AGUA DULCE: CHEQUEO Y M
	24376	200414830	3	4	0	3	0	(MMPP #1) EFRIADOR DE AGUA DULCE: LAVADO DE 02
	24377	200414831	3	4	0	3	0	(MMPP #1) EFRIADOR DE AGUA DULCE: REPARACION D
	24378	200414832	3	4	0	3	0	CAMBIO DE 04 LLANTAS, ALINEACION Y BALANCEO
	24379	200414833	5	3	0	2	0	OT programada DE GAMMA ED
	24380	200414834	5	3	0	2	0	OT programada GAMMA ED
	24381	200414835	5	3	0	2	0	OT programada FURUNO
	24382	200414836	5	3	0	2	0	OT programada NA 21-PROA
	24383	200414837	3	4	0	3	0	REPARACION DE PARTE MECANICA DE LA ELECTROVALV
	24384	200414838	5	3	0	2	0	OT programada NA21-PROA
	24385	200414839	3	4	0	3	0	CAMBIO DE ACEITE DEL MOTOR Y FILTRO
	24386	200414840	5	3	0	2	0	OT programada NA21-PORA

FIGURA 4.21 Prueba de Auditoría –Consulta en la base la tabla orden de trabajo

La Figura 4.21 nos indica que se accesó a la Base de Datos y se procedió a consultar la tabla m_Ots donde se encuentra la numeración de las órdenes de trabajo.



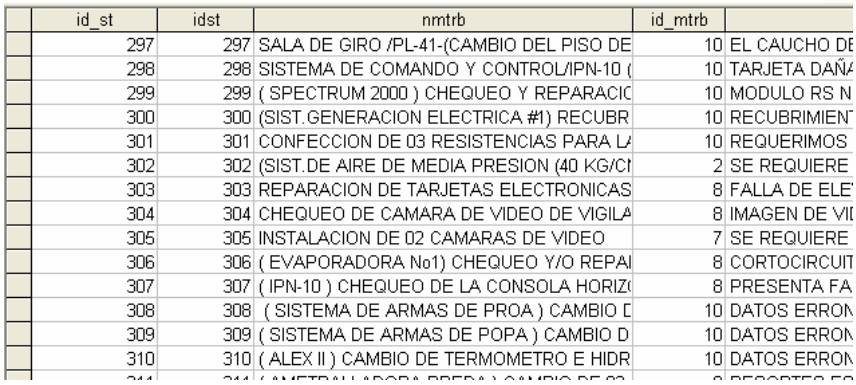
Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

LISTADO DE ORDENES DE TRABAJO

D	S	#OT	Fecha em.	Fecha prog.	#D: Fecha OT	Trabajo a re
F	F	270000047	01/07/2004 10:03	01/07/2004	1 Días	OT programac
D	D	200400177	01/12/2004 09:05	01/12/2004	1 Días	PLANTA DE
C	C	200400198	01/12/2004 13:48	01/12/2004	1 Días	CONSOLA DI
DIN		200400231	13/01/2004 14:32	13/01/2004	1 Días	chequeo, repa
DIN		200400232	13/01/2004 14:33	13/01/2004	1 Días	chequeo, repa
F	F	200400234	13/01/2004 15:10	13/01/2004	1 Días	mantenimient
DIN		200400235	13/01/2004 15:46	13/01/2004	1 Días	REPARACIO
DIN		200400384	14/01/2004 15:37	14/01/2004	1 Días	ACONDICIO
D	D	200400409	15/01/2004 12:31	15/01/2004	1 Días	TOMA DE ES
DE		200400525	20/01/2004 08:11	20/01/2004	1 Días	BASUIL ARE
AG		230000977	21/01/2004 10:23	21/01/2004	1 Días	OT programac

FIGURA 4.22 Prueba de Auditoría-Evaluación de las órdenes de trabajo

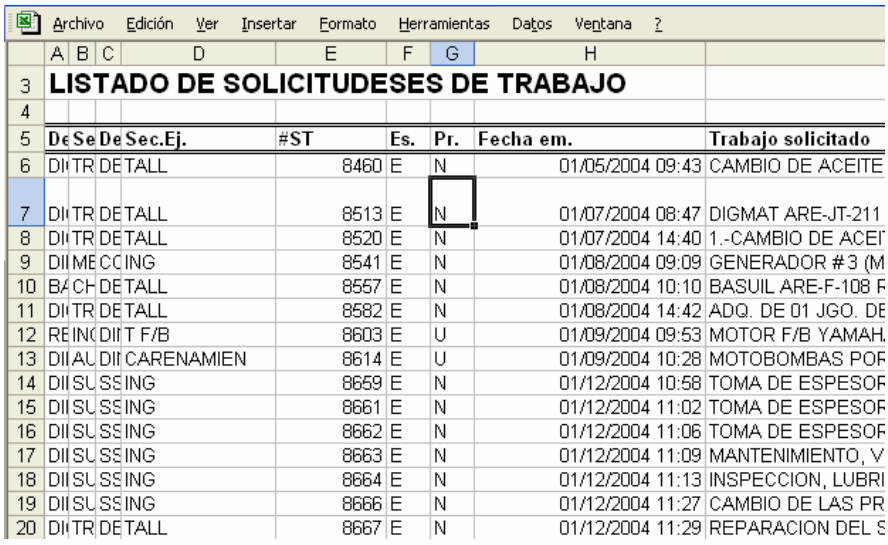
Las figuras 4.21 y 4.22 nos muestran la conciliación y análisis del formato y secuencia lógica de los números de las O/Ts de las transacciones y pruebas realizadas



id_st	idst	nmtrb	id_mtrb	
297	297	SALA DE GIRO /PL-41-(CAMBIO DEL PISO DE	10	EL CAUCHO DE
298	298	SISTEMA DE COMANDO Y CONTROL/IPN-10 (	10	TARJETA DAÑA
299	299	(SPECTRUM 2000) CHEQUEO Y REPARACIC	10	MODULO RS N
300	300	(SIST.GENERACION ELECTRICA #1) RECUBR	10	RECUBRIMIENT
301	301	CONFECCION DE 03 RESISTENCIAS PARA LA	10	REQUERIMOS
302	302	(SIST.DE AIRE DE MEDIA PRESION (40 KG/CI	2	SE REQUIERE
303	303	REPARACION DE TARJETAS ELECTRONICAS	8	FALLA DE ELE
304	304	CHEQUEO DE CAMARA DE VIDEO DE VIGILA	8	IMAGEN DE VI
305	305	INSTALACION DE 02 CAMARAS DE VIDEO	7	SE REQUIERE
306	306	(EVAPORADORA No1) CHEQUEO Y/O REPAI	8	CORTOCIRCUIT
307	307	(IPN-10) CHEQUEO DE LA CONSOLA HORIZ	8	PRESENTA FA
308	308	(SISTEMA DE ARMAS DE PROA) CAMBIO D	10	DATOS ERRON
309	309	(SISTEMA DE ARMAS DE POPA) CAMBIO D	10	DATOS ERRON
310	310	(ALEX II) CAMBIO DE TERMOMETRO E HIDR	10	DATOS ERRON

FIGURA 4.23 Prueba de Auditoría –Consulta en la base la tabla Solicitud de trabajo

La Figura 4.23 nos indica que se procedió al ingreso de la tabla m_Sts donde se encuentra la numeración de las solicitudes de trabajo.



Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

LISTADO DE SOLICITUDESES DE TRABAJO

De	Se	De	Sec.Ej.	#ST	Es.	Pr.	Fecha em.	Trabajo solicitado
DI	TR	DE	TALL	8460	E	N	01/05/2004 09:43	CAMBIO DE ACEITE
DI	TR	DE	TALL	8513	E	N	01/07/2004 08:47	DIGMAT ARE-JT-211
DI	TR	DE	TALL	8520	E	N	01/07/2004 14:40	1.-CAMBIO DE ACEI
DI	ME	CC	ING	8541	E	N	01/08/2004 09:09	GENERADOR #3 (M
BA	CH	DE	TALL	8557	E	N	01/08/2004 10:10	BASUIL ARE-F-108 F
DI	TR	DE	TALL	8582	E	N	01/08/2004 14:42	ADQ. DE 01 JGO. DE
RE	IN	DI	T F/B	8603	E	U	01/09/2004 09:53	MOTOR F/B YAMAH.
DI	AU	DI	CARENAMIEN	8614	E	U	01/09/2004 10:28	MOTOBOMBAS POR
DI	SU	SS	ING	8659	E	N	01/12/2004 10:58	TOMA DE ESPESOR
DI	SU	SS	ING	8661	E	N	01/12/2004 11:02	TOMA DE ESPESOR
DI	SU	SS	ING	8662	E	N	01/12/2004 11:06	TOMA DE ESPESOR
DI	SU	SS	ING	8663	E	N	01/12/2004 11:09	MANTENIMIENTO, V
DI	SU	SS	ING	8664	E	N	01/12/2004 11:13	INSPECCION, LUBRI
DI	SU	SS	ING	8666	E	N	01/12/2004 11:27	CAMBIO DE LAS PR
DI	TR	DE	TALL	8667	E	N	01/12/2004 11:29	REPARACION DEL S

FIGURA 4.24 Prueba de Auditoría-Evaluación de las Solicitudes de trabajo

Las figuras 4.23 y 4.24 nos muestran la conciliación y análisis del formato y secuencia lógica de las S/Ts de las transacciones y pruebas realizadas.

Campo Faltante

Este tipo de validación consiste en verificar que ciertos campos de un módulo o aplicativo no queden vacíos en virtud de que corresponde a un campo importante en el proceso de información.

Hemos detectado que el campo UBICACIÓN del equipo a reparar el campo DESTINO de la orden de trabajo y el campo PORCENTAJE DE EJECUCIÓN de la O/T que se encuentra en el módulo Orden de trabajo no son llenados y aún así se permite generar, aprobar y trabajar en las O/Ts. La falta de este tipo de dato evita que el sistema pueda poseer información íntegra y disponible para uso de informes y tomas de decisiones. Para tener mayor apreciación de las pruebas realizadas ver las (FIGURAS 4.25 y 4.26), adicionalmente ver los papeles de trabajos realizados con la ref. CP8 que se encuentra en el (ANEXO 2).

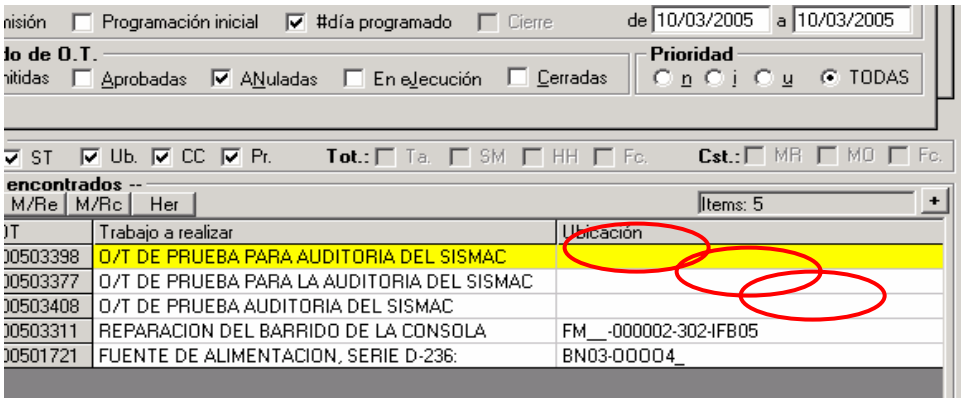


FIGURA 4.25 Prueba de Auditoría-Falta controles de validación

La figura 4.25 nos muestra la falta del control de validación en el campo UBICACIÓN del sistema o equipo a reparar del módulo orden de trabajo.

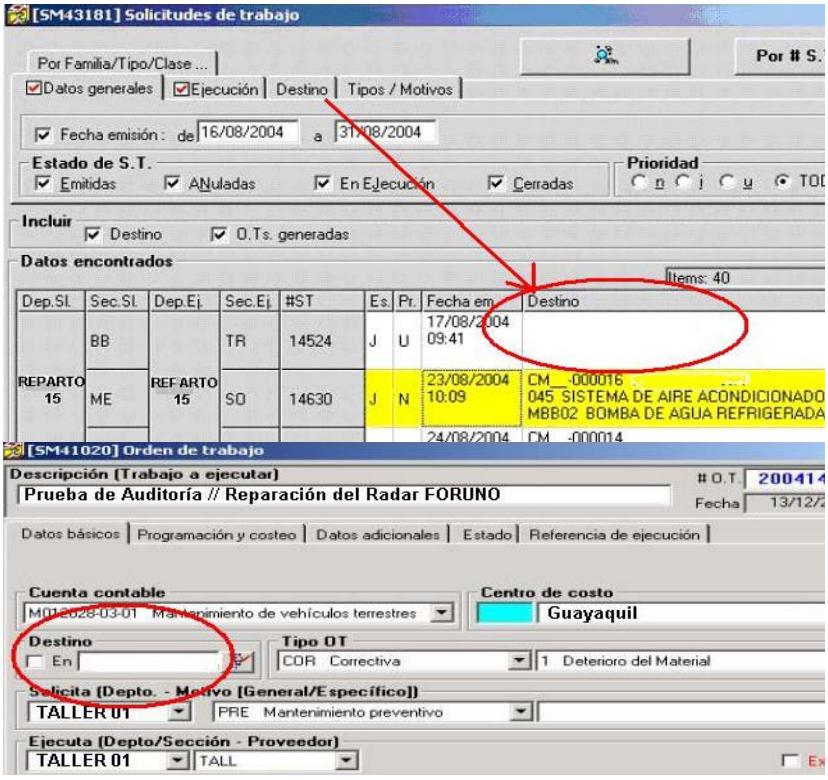


FIGURA 4.26 Prueba de Auditoría-Falta controles de validación

La figura 4.26 nos muestra la falta del control de validación en el campo DESTINO del sistema o equipo a reparar del módulo orden de trabajo y solicitud de trabajo.

Para efecto de obtención de pruebas hemos generado y emitido varias O/Ts con el concepto de prueba de auditoría las cuales nos indica que se puede generar y emitir O/Ts sin registrar la sección ejecutante, o sea sin indicar cual es la sección o laboratorio que realmente debería realizar el trabajo. No debería generarse una O/T sin colocar la sección ejecutante ya que este dato es fundamental para proceder a ejecutar el trabajo y porque existe un encargado administrativo en cada taller que debería saber el laboratorio, sección o técnico al cual deba ser asignado dicha O/T.

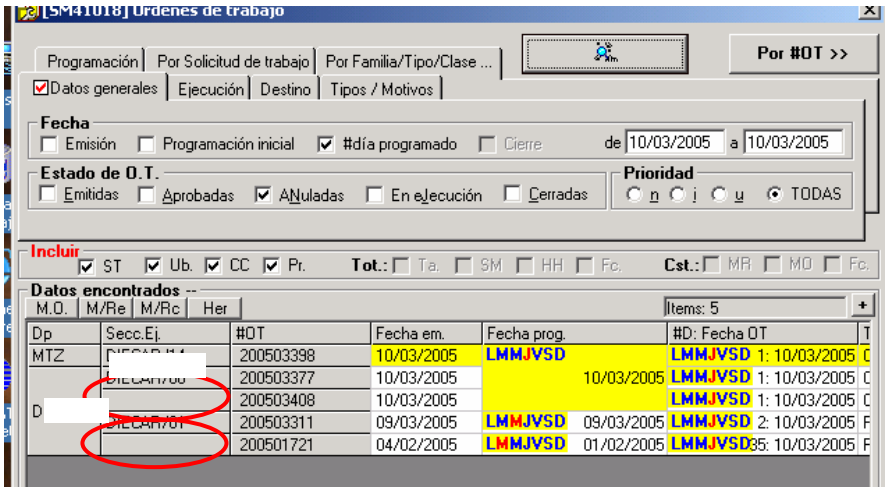


FIGURA 4.27 Prueba de Auditoría-Falta controles de validación

La figura 4.27 nos muestra que falta aplicar controles de validación en el campo donde se coloca la sección ejecutante (Indispensable).

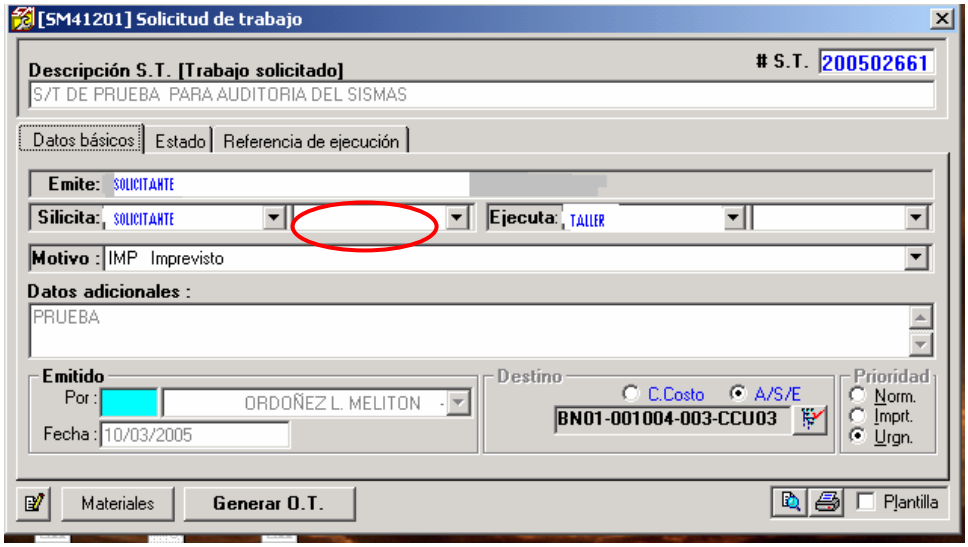


FIGURA 4.28 Prueba de Auditoría-Falta controles de validación.

La figura 4.28 nos indica la falta de controles de validación en la generación de una solicitud de trabajo ya que al momento de generarla se la puede emitir sin la sección que solicita el trabajo.

Razonabilidad

Este tipo de validación busca verificar que los datos no excedan de su valor razonable.

Por efecto del análisis hemos identificado que la opción Horas Hombres en el módulo de O/T donde se asigna al personal adecuado para dar mantenimiento y las horas Hombres empleadas puede ingresarse cualquier valor numérico, es decir que en la asignación de horas se puede colocar cualquier valor en tiempo desde minutos hasta miles de horas de trabajo por día. Si un técnico se equivoca colocando más de 10 horas, el sistema lo registrará.

Ver (FIGURA 4.29)

Todos sabemos que el día tiene 24 horas, y que una persona generalmente no puede trabajar más de 12 horas al día, peor aún si el trabajo demanda esfuerzo físico. Por dicha razón debe existir una adecuada y razonable asignación de valores en este campo para garantizar información efectiva y valedera.

FIGURA 4.29 Prueba de Auditoría-Falta controles de validación.

La figura 4.29 nos muestra la falta de controles de validación en los campos de asignación de Horas Hombres (HH). Si nos fijamos bien en el campo superior derecho encontramos la fecha "martes 18/1/2005" la cual corresponde a un solo día de trabajo, pero en la asignación de HH trabajadas el señor "Lema T. Carlos" tiene asignado 150 horas en un solo día, lo cual no guarda un valor lógico.

También pudimos chequear que la fecha de programación y la fecha de recepción de un O/T que es generada partiendo de una S/T pueden manipularse fácilmente. Se puede colocar fechas de años y siglos pasados. Esta falla impide que la información sea íntegra. Ver (FIGURA 4.30). Ver papeles de trabajo ref. CP8 que se encuentra en (ANEXO 2).

Para efecto de elaboración de pruebas hemos generado una orden de trabajo, con fecha de hoy 10/04/2005; la prueba consiste en tratar de modificar la fecha de programación de cada día laboral, dando como resultado la fecha 01/01/1992, esto demuestra que no existe una adecuada validación del campo Programación de la O/T.

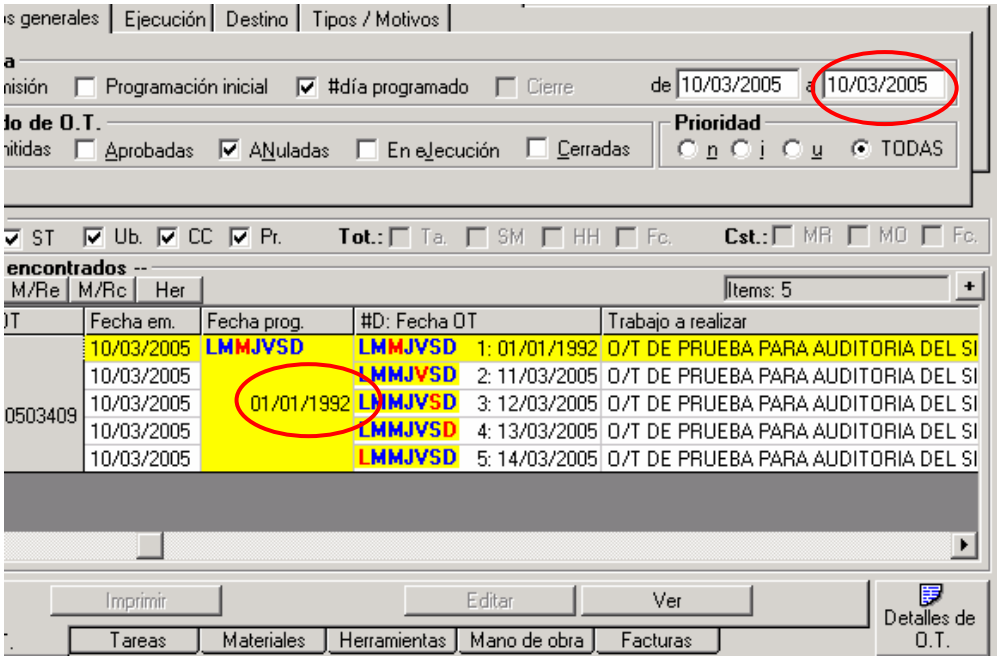


FIGURA 4.30 Prueba de Auditoría - Falta controles de validación

La figura 4.30 nos muestra que existe libre manipulación de las Fechas de Programación de las O/Ts.

4.4. Informe Final

4.4.1. Información General

4.4.1.1. Elaboración del informe

El informe de la auditoría es un documento que indica formalmente la culminación de una auditoría, el cual es de suma importancia ya que en esta realiza su manifestación fehaciente, tangible y visible ante los interesados y a terceros. Este documento indica el alcance del trabajo realizado y la responsabilidad de los criterios emitidos de la razonabilidad de los sistemas.

Para realizar este informe previamente se deben reunir y depurar todas las evidencias encontradas.

El informe de ser resumido en forma gerencial y debe constar mínimo de la siguiente estructura:

- Antecedentes
- Objetivos de la Auditoría

- Resultados de la Evaluación

  Situación actual

  Efectos

  Recomendaciones

4.4.1.2. Documentación de respaldo.

La documentación de auditoría debe estar debidamente realizada y ordenada de acuerdo a la importancia y prioridad.

Se considera que al momento de entregar el informe de auditoría se debe anexar todas las pruebas o documentos de soporte que utilizamos para emitir los criterios. Estos anexos muestran cuestionarios, formularios y documentación emitida por el sistema.

4.4.1.3. Fase de Cierre.

En esta fase el auditor da por terminado la auditoría, corrigiendo previamente el informe de auditoría, realizando una presentación del trabajo realizado y enviando e indicando

mediante una carta, oficio o memorando la finalización formal de los trabajos realizados.

Comentarios:

1. De lo evaluado.

Durante el transcurso de la evaluación realizada a este sistema llamado SMAC, hemos podido recolectado una serie de información las cuales nos ha incitado a la comprobación de las mismas mediante la realización de pruebas de control en transacciones y datos en general.

Ahora que ya hemos culminado nos gustaría dar a conocer y a la vez demostrar todas las observaciones y debilidades encontradas las cuales estarán acompañadas de su debida recomendación o sugerencia que ayudará y estimulará a la puesta en marcha de cambios y mejoras del sistema para una efectiva y eficiente en lo que respecta a la integridad, confiabilidad y disponibilidad de la información.

2. Del Informe Final.

Esta información final reflejada en el informe de auditoría guarda el modelo exacto del cual hemos hablado anteriormente, este

documento llamado informe final lo podemos encontrar y aprecia en la sección de anexo. Hemos pensado en colocarlo en la sección de anexo ya que deseamos presentar un documento de tipo real como las que se entrega o se presenta en un proceso de auditoría o evaluación y además porque este Informe guarda otro tipo de formato que no está permitido dentro de los capítulos de la tesis. Ver (ANEXO 4) donde se encuentra el informe de auditoría.

3. Para el lector.

De todo corazón quedo de ustedes agradecido por haber invertido buena parte de su tiempo en leer este documento y a la vez deseo que le haya servido de gran ayuda y permitido satisfacer sus necesidades mediante el ejercicio práctico donde aclaro y ejemplarizo todo la teoría expuesta en los capítulos anteriores. Su siempre servidor David Carrión Miranda.

CONCLUSIONES

Dirigido al tema de tesis

1. La elaboración y resolución de esta tesis contribuirá de manera positiva a todos los estudiantes y profesionales que deseen tomar como guía de consulta para orientar o ampliar los conocimientos y así elaborar y mejorar las ejecuciones y modelos de auditorías de sistemas de información.

2. Esta evaluación al sistema ha despertado una serie de expectativas a la empresa evaluada, ya que es la primera vez que analizan y detectan una serie de debilidades que en cierto grado puede afectar totalmente la integridad y confiabilidad de la información

3. Esta evaluación nos revela una serie de debilidades en la administración de claves de acceso, procedimientos de acción de la administración del sistema y falta de controles de validación en módulos importantes.

Dirigido a las empresa en general

4. El establecimiento de recursos Informáticos es un factor fundamental en el desarrollo organizacional, por medio de estos se puede encontrar la rapidez, eficiencia y eficacia de las operaciones de la organización.

5. Se considera pieza esencial, el establecimiento de sistemas de información que mediante el almacenamiento de los datos en una base, provea de información necesaria y oportuna a la alta gerencia en un momento dado.

6. Las medidas de control dentro de los procesos de registros de información en la organización son de gran relevancia para la reducción y disminución de riesgo que afectan considerablemente la desviación, integridad y disponibilidad de la información.

7. Los controles generales y específicos de la aplicación manejados en forma eficiente y efectiva son una garantía a la integridad y calidad de la información.

8. La ejecución de auditorías de sistemas de Información comprende un elemento importante para el desarrollo, mejoramiento y actualización a las nuevas exigencias sociales, culturales y tecnológicas.

9. La información es fuente principal para toda acción y actividad, sea mecánica, automática, personal u organizacional. Más aún las grandes organizaciones que dependen totalmente de una adecuada, oportuna y acertada información, por dichas razones se debe invertir en sólidas bases y sistemas de aplicación, hardware y software y sobre todo el establecimiento de controles adecuados y efectivos que garanticen el procesamiento de información, la veracidad y su disponibilidad.

10. Gran parte de las organizaciones no poseen medidas y sistemas de control, lo cual permite la alta vulnerabilidad y creciente riesgo de actos delictivos de fuerzas internas o externas de la organización.

Dirigido a estudiantes

11. El desarrollo de este ejercicio evaluativo nos ha permitido adquirir una mejor y mayor percepción de los problemas típicos que se presenta

por la falta de control en los sistemas de información de las organizaciones.

12. Nosotros los estudiantes estamos es capacidad de iniciar un proceso evaluativo de tecnología de información y en la capacidad de desarrollar nuevas estrategias de control para las organizaciones en general.

13. Después de haber experimentado la realización de este trabajo puedo concluir que nosotros los jóvenes tenemos un futuro inmenso y extenso en el manejo y control de recursos informáticos ya que estamos en el comienzo nueva era tecnológica inimaginable que traerá consigo una vida llena de sorpresas, facilidades pero así mismo mayores riesgos y desafíos para lo cual debemos estar preparados.

RECOMENDACIONES

Dirigido al tema de tesis

Entre las recomendaciones más importantes de la ejecución de esta evaluación de sistema de aplicación podemos mencionar las siguientes:

1. Documentar los planes y procedimientos de desarrollo, mantenimiento y mejoras del sistema.

2. Actualizar el manual del administrador a las últimas modificaciones.

3. Redactar, legalizar, presentar y publicar una política que justifique y defina parámetros en el diseño, asignación, actualización y eliminación de claves de accesos.

4. Definir de mejor manera los perfiles de acceso de cada usuario de acuerdo a sus necesidades y acciones.

5. Definir y documentar un procedimiento donde establezcan una efectiva periodicidad de cambio o actualización de claves de acceso al sistema.

6. Aplicar algún tipo de identificador de claves a nivel de tablas que evite el registro de contraseñas iguales.

7. Cambiar, redefinir y estandarizar las claves existentes las cuales tengan como mínimo seis a ocho caracteres.

8. Crear una clave de acceso para cada usuario, para que a su vez se pueda supervisar las acciones de cada uno, y en el caso que se presente alguna anomalía se proceda a la sanción o a la observación de dicho usuario.

9. Elaborar un plan de contingencia documentado y adecuado a las situaciones del departamento para atender y resolver fallas del sistema.

Dirigido a las empresa en general

10. Capacitar continuamente a todo el personal de la organización para fomentar y mejorar la cultura organizativa con el propósito de establecer ideales y objetivos de control para que a su vez contribuya a la obtención y el cumplimiento de metas y objetivos institucionales.

11. Fortalecer los controles de accesos a los sistemas de información, mejorar los procesos de registro de información e implantar controles adecuados a las mismas.

12. Fomentar a todo el personal de la organización la importancia de poseer y trabajar con información efectiva, oportuna y valedera para adecuadas y acertadas tomas de decisiones.

13. Evaluar continuamente los procesos manuales, procesos automáticos, controles generales, controles específicos y los aspectos físicos al sistema de aplicación.

14. Las organizaciones deben implantar sistemas y estándares de control interno y de tecnología de información tales como COBIT, COSO, ISO,

etc. para tener mayor control y efectividad en las operaciones y administraciones de recursos.

Dirigido a estudiantes

15. Como ya sabemos, los cambios tecnológicos y procesos globalizados demandan mayor rapidez, eficacia y efectividad de las actividades organizacionales, por dicha razón los profesores y estudiantes debemos profundizar el estudio acerca de la gran importancia de estándares internacionales y la necesidad de aplicarse o regirse bajo parámetros o estándares de control.

16. Fomentar y colocar mayor énfasis a la educación de sistemas tecnológicos para que en un futuro no muy lejano se pueda realizar y definir rápidamente diferentes tipos de métodos y técnicas de evaluación y desarrollo de aplicaciones; así mismo ampliar los conocimientos de controles tecnológicos de todas las áreas informáticas.

ANEXOS

CARTA DE COMUNICACION

Guayaquil, Febrero 09 de 2005

Distinguido Señor:

Cumplimos en comunicarle que el equipo de auditoría dirigido y guiado por el ACG. David Carrión de la empresa DConsulting S.A., ha dado inicio a la evaluación del Sistema de información SMAC; Sistema de Mantenimiento asistido por computadora. Cuyo alcance está enfocado a las opciones orden de trabajo y solicitud de trabajo del módulo de mantenimiento.

Con ésta oportunidad agradecemos nos facilite el acceso total al software SMAC para realizar las pruebas necesarias así como a la documentación que tenga relación con la evaluación mencionada.

Agradecemos de antemano por toda la ayuda que nos brinde sus colaboradores para la culminación a fin de alcanzar los objetivos del presente trabajo.

Atentamente;

ACG. David Carrión M.
Presidente
DConsulting S.A.

ANEXO 1

AUDITORIA DE SISTEMAS DE INFORMACIÓN

PROGRAMA DE TRABAJO GENERAL

A. Familiarización y Documentación del sistema y las funciones o prácticas que realiza.
Conocer la Situación Actual del Sistema de Información y de las áreas relacionadas
B. Revisar los procedimientos y los controles del acceso
Evaluar la administración de las claves de accesos a los módulos del sistema.
C. Evaluación de los controles al momento de hacer cambios en la aplicación.
Evaluar los procesos y procedimientos de la administración del Servidor de aplicaciones al momento de hacer cambios.
D. Obtener conocimiento sobre los aspectos Técnicos complementarios del entorno de procesamientos.
Determinar el ambiente del hardware y software del servidor de aplicaciones, del servidor de datos y equipos de ciertos usuarios, en términos de disponibilidad y requisitos técnicos.
E. Evaluar la integridad de transacción y los controles de entrada o ingreso de datos.
Evaluar la integridad y validez de los datos de entrada a los módulos del sistema
F. Revisar los planes de Contingencia
Evaluar el plan de contingencia de la aplicación en caso de fallas del sistema
G. Evaluar los controles Físicos
Evaluar las medidas de seguridad física considerando los aspectos de integridad, confiabilidad y disponibilidad de la información

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

A

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	A. Familiarización y Documentación del sistema y las funciones o prácticas que realiza.	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Conocer la Situación Actual del Sistema de Información y de las áreas relacionadas			
	PROCEDIMIENTOS			
1	Conducir una entrevista con personal apropiado para determinar quién es el responsable de la administración y mantenimiento del sistema. Obtener el mapa Orgánico actual	**CVP**	**DCM**	**01/03/2005**
2	Obtener Información de Auditorías anteriores relacionado con el área a evaluar	**CCG**	**DCM**	**01/03/2005**
3	Obtener el mapa o flujo del proceso de información	**CCG**	**DCM**	**01/03/2005**
4	Obtener manual de Usuario	**CCG**	**DCM**	**01/03/2005**
5	Obtener el Diagrama de entidad Relación de la Base de Datos del SISMAC	**CCG**	**DCM**	**01/03/2005**
6	Revisar cualquier plan para el desarrollo, mejora/modificación, y la actividad del mantenimiento concerniente a los sistemas bajo revisión.	**CCG**	**DCM**	**01/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

B

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	B. Revisar los procedimientos y los controles del acceso	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Evaluar la administración de las claves de accesos a los módulos del sistema.			
	PROCEDIMIENTOS			
1	Conducir una entrevista con personal apropiado para ganar comprensión de los procedimientos para crear y quitar el acceso de la utilización de las bases de datos y a los sistemas.	**CCG**	**DCM**	**03/03/2005**
2	Obtener una lista de todos los usuarios con el respectivo perfil, clave, permiso de acceso (creación, modif.emisión, consulta, accesos, no accesos) y revisarla para la autorización.	**CP6**	**DCM**	**03/03/2005**
3	Determinar el procedimiento para evaluar, asignar y entregar las claves de acceso al sistema hacia los usuarios	**CCG**	**DCM**	**03/03/2005**
4	Revisar las políticas de las aplicaciones de Contraseñas	**CP7**	**DCM**	**03/03/2005**
	a. Revisar las reglas de las contraseñas para la longitud y composición , Revisar su cumplimiento		**DCM**	**03/03/2005**
	b. Revisar la periodicidad de los cambios de la contraseña para la frecuencia y la conformidad.		**DCM**	**03/03/2005**
	c. Determinar si las claves de accesos son encriptadas		**DCM**	**03/03/2005**
	d. Determinar si los intentos de claves de acceso invalidas son detectadas, registradas y bloqueadas.		**DCM**	**03/03/2005**
5	Examinar los procedimientos para quitar el acceso cuando un empleado deja una posición laboral.	**CCG**	**DCM**	**03/03/2005**
6	Determinar si se suprimen las cuentas sin usar		**DCM**	**03/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

C

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	C. Evaluación de los controles al momento de hacer cambios en la aplicación.	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones al momento de hacer cambios.			
	PROCEDIMIENTOS			
1	Existe una política de autorización y aprobación de cambios en el sistema.	**CCG**	**DCM**	**01/03/2005**
2	Revisar el proceso de pruebas para los cambios	**CCG**	**DCM**	**01/03/2005**
3	Revisar el procedimiento de autorización y aprobación de cambios	**CCG**	**DCM**	**01/03/2005**
4	Revisar las autorizaciones y aprobaciones de cambios (documentos)	**CCG**	**DCM**	**01/03/2005**
5	Verificar si aplicaciones en estudio han sufrido cambios recientemente, y si éstos están en conocimiento formal y documentado por la gerencia.	**CCG**	**DCM**	**01/03/2005**
6	Verificar la existencia de adecuados registros u hojas donde conste las modificaciones y/o mantención.	**CCG**	**DCM**	**01/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

D

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	D. Obtener conocimiento sobre los aspectos Técnicos complementarios del entorno de procesamientos.	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Determinar el ambiente del hardware y software del servidor de aplicaciones, del servidor de datos y equipos de ciertos usuarios, en términos de disponibilidad y requisitos técnicos.			
	PROCEDIMIENTOS			
1	Obtener conocimiento del diseño de la Organización estructural del servicio computacional e informático donde se encuentre instalado el sistema (Redes, topología, # computadoras, conexiones, capacidad)	**CCG**	**DCM**	**01/03/2005**
2	Obtener un inventario de todos los servidores críticos, incluyendo los detalles en configuraciones de hardware, los periférico, los sistemas operativos, el propósito del servidor, los usos permitidos o que funcionan dentro de estos.	**CCG**	**DCM**	**01/03/2005**
3	Determinar Quién tiene acceso de administrador.	**CCG**	**DCM**	**01/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

E

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	E. Evaluar la integridad de transacción y los controles de entrada o ingreso de datos.	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Evaluar la integridad y validez de los datos de entrada a los módulos del sistema			
	PROCEDIMIENTOS			
1	Verificar y evaluar validaciones de campos (cálculo) validaciones de fechas, operabilidad, autodocumentación, manejo de pantalla vs. documento de estrada si existe	**CP8**	**DCM**	**04/03/2005**
2	Verificar y evaluar que exista Razonabilidad y consistencia de los números generados de las O/t de la pantalla ,impresa y en la bases de datos.	**CP8**	**DCM**	**04/03/2005**
3	Verificar y evaluar los datos y valores ingresados en los opciones de la S/T y O/T contra los valores almacendos en la base de datos del sistema. (verificar la integridad y exactitud de datos).	**CP1**	**DCM**	**04/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

F

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	F. Revisar los planes de Contingencia	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Evaluar el plan de contingencia de la aplicación en caso de fallas del sistema			
	PROCEDIMIENTOS			
1	Verificar la existencia de políticas o planes de contingencia con los servidores de aplicaciones y de datos	**CF**	**DCM**	**02/03/2005**
2	Verificar políticas de respaldo de información.	**CF**	**DCM**	**02/03/2005**
3	Verificar los procedimientos de respaldo de información magnética	**CF**	**DCM**	**02/03/2005**
4	Determinar que los archivos de respaldo se los almacena o guarda en un lugar seguro	**CF**	**DCM**	**02/03/2005**
5	Revisar los siguientes planes y los procedimientos de recuperación en caso de desastres :	**CF**	**DCM**	**02/03/2005**
	a. offsite storage of data // Almacenamiento y custodia de datos en un lugar seguro	**CF**	**DCM**	**02/03/2005**
	b. hot/cold site; // El lugar temperado (fuera del frío y el calor);	**CF**	**DCM**	**02/03/2005**
	c. redundant data center; // respaldo de información	**CF**	**DCM**	**02/03/2005**
	d. periodic review; and // revisiones periódicas	**CF**	**DCM**	**02/03/2005**

AUDITORIA DE SISTEMAS DE INFORMACIÓN
PROGRAMA DE TRABAJO

G

ENTIDAD: Talleres Integrados
FECHA. Marzo del 2005
TIEMPO PREVISTO: 2 días **TIEMPO DE INICIO:** 01 de marzo
AUDITOR RESPONSABLE: David Carrión M

PASOS	G. Evaluar los controles Físicos	REF. P/T	EJECUTADO POR	FECHA DE EVALUACIÓN
	OBJETIVO			
	Evaluar las medidas de seguridad física considerando los aspectos de integridad, confiabilidad y disponibilidad de la información			
	PROCEDIMIENTOS			
1	Determinar la existencia de políticas de seguridad Física			
2	Determinar si todo el hardware está situado en áreas físicamente seguras	**CG**	**DCM**	**02/03/2005**
3	Revisar la seguridad de la sala de ordenadores y los controles de acceso físicos	**CG**	**DCM**	**02/03/2005**
4	Determinar si el equipo está protegido contra factores ambientales tales como apagones, inundaciones, calor, y humedad	**CG**	**DCM**	**02/03/2005**
5	Realizar las inspecciones en sitio para evaluar controles	**CG**	**DCM**	**02/03/2005**

ANEXO 2
PAPELES DE TRABAJO

AUDITORIA DE SISTEMAS DE INFORMACIÓN
GUIA DE VISITA PREVIA

CVP

Fecha:	01 de marzo del 2005
Departamento :	División de Mantenimiento y Planificación
Nombre del Entrevistado:	Ing. Cindy Encalada Moreno
Auditor Responsable:	David Carrión Miranda

¿CUÁL ES NOMBRE DEL SISTEMA ?

SMAC , Sistema de Mantenimiento Asistido por Computadora

¿ CUÁL ES EL ENCARGADO O ADMINISTRADOR DEL SISTEMA ?

Para el servidor de Aplicaciones es la Analista de Sistema Cindy Encalada Moreno

Para el servidor de Base de Datos es el Ing. Xavier Mancero Ordoñez

¿ CUÁNDO SE ADQUIRIÓ EL SISTEMA ?

En el 2001

¿CUANTOS MÓDULOS TIENE EL SISTEMA?

El SMAC posee 8 módulos y tres utilitarios, de los cuales solo se compro 5 módulos y los tres utilitarios.

Inventario	Mantenimiento	Utilitarios	Global
Ficha Técnica	Lista base de Recambio		Informes
Personal			Gráficos

¿QUÉ ACTIVIDADES REALIZA EL SISTEMA ?

Controla el costo y mantenimiento de las Unidades Navales y repartos

¿CUÁNTAS PERSONAS TRABAJAN EN ESTE DEPARTAMENTO?

5 personas

Sr. Cristian Aguirre y Sr. Dario Mendoza Soporte al Usuario y asesor técnico

Sr. Miguel Flores Estadístico

Srta. Cindy Encalda Moreno Administradora

Sr. Augusto Tacle Secretario

¿CUÁL ES EL JEFE SUPERIOR DE ESTE DEPARTAMENTO?

Señor Victor Aviles Pérez

¿QUIÉNES SON USUARIOS DEL SMAC?

Todas las unidades Navales, repartos y Talleres-Laboratorios

Existen 3 tipos de Grandes Talleres, 1 especializado en Motores, 2 especializado en sistemas electrónicos y 3 en Vehículos

Firma entrevistado

AUDITORIA DE SISTEMAS DE INFORMACIÓN
DESCRIPCIÓN BREVE DEL SISTEMA

CVP

SERVIDOR DE APLICACIONES	SOFT BLOCK	Controla a los usuarios que están conectados Controla la Ruta de la aplicación
	SMAC SERVER	Actualización de los Datos Mano de Obra Ejecución de mantenimiento Fecha Próximas Actividades Costos de O/Ts
	SMAC INTERFAZ	Ejecuta Interfase con el Sistema Canopus Con las tablas de Personal, Costos; ubicación , Stock

Existe el Proceso Batch

Este consiste en Consolidar la Información, este proceso se lo realiza cada vez que las unidades navales regresan de navegar

Previamente se instala una base local de datos y de aplicación, esto permite que cada unidad puede solicitar mantenimiento mediante el SMAC.

Al momento de llegar a puerto se procede a ejecutar el proceso Batch; es proceso se lo realiza mediante conexión Vía red o movilizando el computador hacia el servidor de aplicaciones. No se lo realiza automáticamente.

El encargado de los respaldo de Datos o Backups es el Sr. Ing Xavier Mancero Ordoñez

El servidor de aplicación permanece en una oficina sin seguridad al acceso de personas

Firma entrevistado

AUDITORIA DE SISTEMAS DE INFORMACIÓN

PRIORIDAD DE AUDITAJE
(SISTEMA DE PUNTAJE)

PA

NOMBRE DE LA APLICACIÓN: SISMAC

PUNTAJE / FACTORES	1	2	3	TOTAL
1 INVENTARIOS	**3**	**5**	**3**	**11**
2 FICHA TÉCNICA	**3**	**5**	**3**	**11**
3 LISTA BASE DE RECAMBIO	**3**	**5**	**3**	**11**
4 PERSONAL	**5**	**5**	**5**	**15**
5 MANTENIMIENTO	**10**	**10**	**10**	**30**
PUNTAJE TOTAL	**24**	**30**	**24**	**78**

1 Emiteny registra la información de las ordenes de mantenimiento
2 Mayor riesgo de manipulación de datos
3 Permite controlar las acciones de mantenimiento

Escala

1-3 Básico
4-6 Importante
7-10 Fundamental

Comentario

Para determinar la prioridad e importancia de los módulos a evaluar hemos tomado la técnica SCORING sistema de Puntaje, el cual nos indica que mediante una valoración de las carácteristicas de los módulos podemos determinar el módulo de

AUDITORIA DE SISTEMAS DE INFORMACIÓN

Familiarización y Documentación del sistema

Fecha: 01 de Marzo del 2005
Departamento : División de Mantenimiento y Planificación
Nombre del Entrevistado: Ing. Cindy Encalada Moreno
Auditor Responsable: David Carrión M.

CCG

#	Área	Existe		Papel de Trabajo	Comentarios
		Si	No		
1	Mapa orgánico de los puestos y funciones del departamento que administra al sistema	x		manual orgánico y de funciones	
2	Proceso y flujo de información de las actividades de mantenimiento de la empresa (documentada y legalizada)	x		flujograma	Ver la FIGURA 4.6 donde se encuentra el proceso de las solicitudes y órdenes de trabajo atendidas por los talleres
3	Manual de usuario del sistema	x		manual /usuario	
4	Auditorias anteriores del sistema.		x		anteriormente no se han realizado auditorías a este sistema
5	Procedimientos adecuados para la configuración del sistema (Documentado y legalizado)	x			Existe un manual de configuración pero desactualizado.

6	El diagrama de entidad y relación esta debidamente actualizada y documentada		**x**		**se han realizado un serie de modificaciones pero no está actualizada el diagrama de entidad y relación.**
7	Diccionario de datos del sistema (Documentado y legalizado)		**x**		**No porque el sistema es comprado**
8	Secuencia crítica del proceso de información del sistema (ELABORAR recibir solicitud/t O/t- reenviar solicitud/t)	**x**			**Existen cuellos de botellas dentro del proceso de información, pero a nivel administrativo, no del sistema**
9	Plan de desarrollo de mejora/modificación (Documentado y legalizado)		**x**		
10	Procedimientos adecuados para realizar los cambios en las aplicaciones y generación de reportes. (Documentado y legalizado)	**x**		**Contrato de servicio**	**El proveedor hace los cambios previa llamada y análisis del problema. Existe un contrato , el cual hemos podido verificar y determinar su veracidad**
11	Procedimiento para autorización y aprobación cambios en el sistema	**x**			**Los cambios en el sistema son autorizado por el jefe del pricipal del departamento previo análisis e informe de los administradores de BD**
12	Existencia de adecuados registros u hojas donde conste las modificaciones y/o mantención.		**x**		
13	Aplicaciones en estudio han sufrido cambios recientemente, y si éstos están en conocimiento formal y documentado por la gerencia.	**x**		**Oficio**	**oficio enviado al jefe principal de departamento**

Debido al acuerdo realizado con la empresa que nos facilitó la información NO podemos mostrar la documentación recolectada, ya que en estás se encuentra el nombre e información confidencial.

AUDITORIA DE SISTEMAS DE INFORMACIÓN

COMPROBACIÓN DE LA LÓGICA E INTEGRIDAD DE DATOS ENTRE LAS TABLAS DE LA BD CONTRA LAS CONSULTAS

Fecha: 04 de marzo del 2005

Auditor Responsable: David Carrión

Módulo Mantenimiento

CP1

SOLICITUD DE TRABAJO

NOMBRE DE LAS TABLAS	NATURALEZA DEL CAMPO	DATOS //VALORES INGRESADOS EN SISTEMA	VERIFICACIÓN POR MUESTREO DE LOS DATOS EN LAS TABLAS BD	CUMPLE CON EL FORMATO		COMENTARIO
				SI	NO	
Solicitud de Trabajo	Autonumérico	8460	8460	X		OK
Solicitud de Trabajo	Autonumérico	8513	8513	X		OK
Solicitud de Trabajo	Autonumérico	8520	8520	X		OK
Solicitud de Trabajo	Autonumérico	8541	8541	X		OK
Solicitud de Trabajo	Autonumérico	8557	8557	X		OK
Solicitud de Trabajo	Autonumérico	8582	8582	X		OK
Solicitud de Trabajo	Autonumérico	8603	8603	X		OK
Solicitud de Trabajo	Autonumérico	8614	8614	X		OK
Solicitud de Trabajo	Autonumérico	8659	8659	X		OK
Solicitud de Trabajo	Autonumérico	8661	8661	X		OK
Solicitud de Trabajo	Autonumérico	8662	8662	X		OK
Solicitud de Trabajo	Autonumérico	8663	8663	X		OK
Solicitud de Trabajo	Autonumérico	8664	8664	X		OK
Solicitud de Trabajo	Autonumérico	8666	8666	X		OK
Solicitud de Trabajo	Autonumérico	8667	8667	X		OK
Solicitud de Trabajo	Autonumérico	8668	8668	X		OK
Solicitud de Trabajo	Autonumérico	8669	8669	X		OK
Solicitud de Trabajo	Autonumérico	8670	8670	X		OK
Solicitud de Trabajo	Autonumérico	8671	8671	X		OK
Solicitud de Trabajo	Autonumérico	8672	8672	X		OK
Solicitud de Trabajo	Autonumérico	8673	8673	X		OK
Solicitud de Trabajo	Autonumérico	8674	8674	X		OK
Solicitud de Trabajo	Autonumérico	8691	8691	X		OK
Solicitud de Trabajo	Autonumérico	8725	8725	X		OK
Solicitud de Trabajo	Autonumérico	8734	8734	X		OK
Solicitud de Trabajo	Autonumérico	8739	8739	X		OK
Solicitud de Trabajo	Autonumérico	8781	8781	X		OK
Solicitud de Trabajo	Autonumérico	8782	8782	X		OK

Solicitud de Trabajo	Autonumérico	8788	8788	X		OK
Solicitud de Trabajo	Autonumérico	8790	8790	X		OK
Solicitud de Trabajo	Autonumérico	8791	8791	X		OK
Solicitud de Trabajo	Autonumérico	8864	8864	X		OK
Solicitud de Trabajo	Autonumérico	8883	8883	X		OK
Solicitud de Trabajo	Autonumérico	8916	8916	X		OK
Solicitud de Trabajo	Autonumérico	8965	8965	X		OK
Solicitud de Trabajo	Autonumérico	8997	8997	X		OK
Solicitud de Trabajo	Autonumérico	9004	9004	X		OK
Solicitud de Trabajo	Autonumérico	9014	9014	X		OK
Solicitud de Trabajo	Autonumérico	9028	9028	X		OK
Solicitud de Trabajo	Autonumérico	9032	9032	X		OK
Solicitud de Trabajo	Autonumérico	9042	9042	X		OK
Solicitud de Trabajo	Autonumérico	9080	9080	X		OK
Solicitud de Trabajo	Autonumérico	9081	9081	X		OK
Solicitud de Trabajo	Autonumérico	9082	9082	X		OK
Solicitud de Trabajo	Autonumérico	9083	9083	X		OK
Solicitud de Trabajo	Autonumérico	9126	9126	X		OK
Solicitud de Trabajo	Autonumérico	9127	9127	X		OK
Solicitud de Trabajo	Autonumérico	9151	9151	X		OK
Solicitud de Trabajo	Autonumérico	9173	9173	X		OK
Solicitud de Trabajo	Autonumérico	9209	9209	X		OK
Solicitud de Trabajo	Autonumérico	9407	9407	X		OK
Solicitud de Trabajo	Autonumérico	9409	9409	X		OK
Solicitud de Trabajo	Autonumérico	9412	9412	X		OK

Los valores generados en producción y en pruebas coincide exactamente con los almacenados en la Tabla mi_sts de la base de datos.

COMENTARIO

Según la prueba realizada en el Software de auditoría llamada IDEA, SI cumple con el control de validación de FORMATO, lo cual se refleja en este documento de prueba

AUDITORIA DE SISTEMAS DE INFORMACIÓN

COMPROBACIÓN DE LA LÓGICA E INTEGRIDAD DE DATOS ENTRE LAS TABLAS DE LA BD CONTRA LAS CONSULTAS

Fecha: 04 de marzo del 2005

Auditor Responsable: David Carrión

Módulo Mantenimiento

CP1

ORDEN DE TRABAJO

				CUMPLE CON EL FORMATO		
NOMBRE DE LAS TABLAS	**NATURALEZA DEL CAMPO**	**DATOS //VALORES INGRESADOS EN SISTEMA**	**VERIFICACIÓN POR MUESTREO DE LOS DATOS EN LAS TABLAS BD**	**SI**	**NO**	**COMENTARIO**
Ordenes de Trabajo	Autonumérico	200401415	200401415	X		OK
Ordenes de Trabajo	Autonumérico	200401418	200401418	X		OK
Ordenes de Trabajo	Autonumérico	200401420	200401420	X		OK
Ordenes de Trabajo	Autonumérico	200401421	200401421	X		OK
Ordenes de Trabajo	Autonumérico	200401422	200401422	X		OK
Ordenes de Trabajo	Autonumérico	200401426	200401426	X		OK
Ordenes de Trabajo	Autonumérico	200401427	200401427	X		OK
Ordenes de Trabajo	Autonumérico	200401429	200401429	X		OK
Ordenes de Trabajo	Autonumérico	200401431	200401431	X		OK
Ordenes de Trabajo	Autonumérico	200401433	200401433	X		OK
Ordenes de Trabajo	Autonumérico	200401434	200401434	X		OK
Ordenes de Trabajo	Autonumérico	200401436	200401436	X		OK
Ordenes de Trabajo	Autonumérico	200401437	200401437	X		OK
Ordenes de Trabajo	Autonumérico	200401438	200401438	X		OK
Ordenes de Trabajo	Autonumérico	200401439	200401439	X		OK
Ordenes de Trabajo	Autonumérico	200401440	200401440	X		OK
Ordenes de Trabajo	Autonumérico	200401445	200401445	X		OK
Ordenes de Trabajo	Autonumérico	200401448	200401448	X		OK
Ordenes de Trabajo	Autonumérico	200401456	200401456	X		OK
Ordenes de Trabajo	Autonumérico	200401459	200401459	X		OK
Ordenes de Trabajo	Autonumérico	200401474	200401474	X		OK
Ordenes de Trabajo	Autonumérico	200401477	200401477	X		OK
Ordenes de Trabajo	Autonumérico	200401479	200401479	X		OK
Ordenes de Trabajo	Autonumérico	200401484	200401484	X		OK
Ordenes de Trabajo	Autonumérico	200401487	200401487	X		OK
Ordenes de Trabajo	Autonumérico	200401490	200401490	X		OK
Ordenes de Trabajo	Autonumérico	200401491	200401491	X		OK
Ordenes de Trabajo	Autonumérico	200401493	200401493	X		OK

Ordenes de Trabajo	Autonumérico	200401494	200401494	X		OK
Ordenes de Trabajo	Autonumérico	200401495	200401495	X		OK
Ordenes de Trabajo	Autonumérico	200401496	200401496	X		OK
Ordenes de Trabajo	Autonumérico	200401497	200401497	X		OK
Ordenes de Trabajo	Autonumérico	200401498	200401498	X		OK
Ordenes de Trabajo	Autonumérico	200401500	200401500	X		OK
Ordenes de Trabajo	Autonumérico	200401499	200401499	X		OK
Ordenes de Trabajo	Autonumérico	200401550	200401550	X		OK
Ordenes de Trabajo	Autonumérico	200401559	200401559	X		OK
Ordenes de Trabajo	Autonumérico	200401566	200401566	X		OK
Ordenes de Trabajo	Autonumérico	200401567	200401567	X		OK
Ordenes de Trabajo	Autonumérico	200401581	200401581	X		OK
Ordenes de Trabajo	Autonumérico	200401586	200401586	X		OK
Ordenes de Trabajo	Autonumérico	200401591	200401591	X		OK
Ordenes de Trabajo	Autonumérico	200401595	200401595	X		OK
Ordenes de Trabajo	Autonumérico	200401694	200401694	X		OK
Ordenes de Trabajo	Autonumérico	200401687	200401687	X		OK
Ordenes de Trabajo	# del Proceso Batch	230001016	230001016	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	230001018	230001018	X		OK
Ordenes de Trabajo	Autonumérico	200401731	200401731	X		OK
Ordenes de Trabajo	Autonumérico	200401774	200401774	X		OK
Ordenes de Trabajo	Autonumérico	200401784	200401784	X		OK
Ordenes de Trabajo	Autonumérico	200401785	200401785	X		OK
Ordenes de Trabajo	# del Proceso Batch	230001053	230001053	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	# del Proceso Batch	2300010	2300010	X		OK
Ordenes de Trabajo	Autonumérico	200401954	200401954	X		OK

los números del proceso Batch son distinto formato

COMENTARIO

Según la prueba realizada en el Software de auditoría llamada IDEA, SI cumple con el control de validación de FORMATO, lo cual se refleja en este documento de prueba

AUDITORIA DE SISTEMAS DE INFORMACIÓN

COMPROBACIÓN DE LA LÓGICA E INTEGRIDAD DE DATOS ENTRE LAS TABLAS DE LA BD CONTRA LAS CONSULTAS

FECHA: 03 de marzo del 2005

NOMBRE DE TABLA: m_ots

CONSULTA **Orden de Trabajo**

CP1

DATOS INGRESADOS	DATOS DE LA TABLA	CUMPLE CON EL FORMATO	
		SI	NO
CONGELADOR#2 COMPRESOR.ADQUISICION DE 01 COMPRESOR PARA MEDIA REFRIGERADO POR AIRE 1/3HP 110VAC	CONGELADOR#2 COMPRESOR.ADQUISICION DE 01 COMPRESOR PARA MEDIA REFRIGERADO POR AIRE 1/3HP 110VAC	X	
RAN-10S. UNIDAD SERVO AMPLIFICADORA	RAN-10S. UNIDAD SERVO AMPLIFICADORA	X	
MANTENIMIENTO DEL FLAP DEL SILENCIADOR DE LA MAQUINA No 2 (MAQUINA DIESEL)	MANTENIMIENTO DEL FLAP DEL SILENCIADOR DE LA MAQUINA No 2 (MAQUINA DIESEL)	X	
REPARACION COMPRESOR INGERSOLL RAND 15T2	REPARACION COMPRESOR INGERSOLL RAND 15T2	X	
BASUIL ARE-T-055 CAMBIO DE ACEITS I FILTROS/COMBUSTIBLE/ACEITE /LAVADADO ENGRASADO Y PULVERIZADO	BASUIL ARE-T-055 CAMBIO DE ACEITS I FILTROS/COMBUSTIBLE/ACEITE /LAVADADO ENGRASADO Y PULVERIZADO	X	
CHEQUEO Y MANTENIMIENTO DEL SISTEMA HIDRAULICO DE LA PLUMA DE LA GRUA HIDRAULICA.	CHEQUEO Y MANTENIMIENTO DEL SISTEMA HIDRAULICO DE LA PLUMA DE LA GRUA HIDRAULICA.	X	
TOMA DE DEFLEXION, BALANCEO DEL ROTOR Y CAMBIO DE RODAMIENTOS DEL MOTOR DE EXTRACCION EB DE CALDERAS	TOMA DE DEFLEXION, BALANCEO DEL ROTOR Y CAMBIO DE RODAMIENTOS DEL MOTOR DE EXTRACCION EB DE CALDERAS	X	
CAMBIO DE FUSIBLES EN LA UNIDAD	CAMBIO DE FUSIBLES EN LA UNIDAD	X	
MANTENIMIENTO DEL COMPRESOR EB. (PLANTA AIRE ACONDICIONADO)	MANTENIMIENTO DEL COMPRESOR EB. (PLANTA AIRE ACONDICIONADO)	X	
RAN-10S. UNIDAD SERVO AMPLIFICADORA	RAN-10S. UNIDAD SERVO AMPLIFICADORA	X	
PL-41. SINCRONIZADOR DE RUMBO	PL-41. SINCRONIZADOR DE RUMBO	X	
CAMBIO DE PLANCHAJE EN LA CUBIERTA PRINCIPAL EN AREA ESCOTILLA DE PROA	CAMBIO DE PLANCHAJE EN LA CUBIERTA PRINCIPAL EN AREA ESCOTILLA DE PROA	X	
SISTEMA DE COMBUSTIBLE -ACEITE(ADQUISICIÒN DE BOMBA MANUAL)	SISTEMA DE COMBUSTIBLE -ACEITE(ADQUISICIÒN DE BOMBA MANUAL)	X	
OT programada	OT programada	X	
MQS. PRINCIPALES, GENERADORES Y PLANTA DE A/A (CONFECCION DE ZINES DE SACRIFICIO)	MQS. PRINCIPALES, GENERADORES Y PLANTA DE A/A (CONFECCION DE ZINES DE SACRIFICIO)	X	
ADQUISICION DE CABLE DE PODER DE TIERRA SOLICITADO MEDIANTE OFICIO FRAMOR-PER-079-O; 11/MAR/03	ADQUISICIÓN DE CABLE DE PODER DE TIERRA SOLICITADO MEDIANTE OFICIO FRAMOR-PER-079-O; 11/MAR/03	X	
ADQUISICION DE 04 RESISTENCIAS PARA LA COCINA SEGUN MUESTRA	ADQUISICION DE 04 RESISTENCIAS PARA LA COCINA SEGUN MUESTRA	X	
ADQUISICION DE RODAMIENTOS PARA EL MOTOR DE VENTILACIÓN 02J13	ADQUISICION DE RODAMIENTOS PARA EL MOTOR DE VENTILACIÓN 02J13	X	
CONFECCION DE LAPICES DE ZINC PARA PROTECCION DEL INTERCAMBIADOR AGUA DULCE- AGUA SALADA DE LAS MAQUINAS PRINCIPALES	CONFECCION DE LAPICES DE ZINC PARA PROTECCION DEL INTERCAMBIADOR AGUA DULCE- AGUA SALADA DE LAS MAQUINAS PRINCIPALES	X	
CHEQUEO Y REVISION DEL MANIFOLD No V . DEL SISTEMA DE ACHIQUE	CHEQUEO Y REVISION DEL MANIFOLD No V . DEL SISTEMA DE ACHIQUE	X	
TRANSRECEPTOR VHF 618M-3A	TRANSRECEPTOR VHF 618M-3A	X	
TRANSRECEPTOR VHF AEREO 618-3A UNIDAD DE CONTROL REMOTO	TRANSRECEPTOR VHF AEREO 618-3A UNIDAD DE CONTROL REMOTO	X	
LIMPIEZA DEL CARBURADOR Y CHEQUEO DEL SISTEMA DE ARRANQUE	LIMPIEZA DEL CARBURADOR Y CHEQUEO DEL SISTEMA DE ARRANQUE	X	

CAMBIO DE PORTAFUSIBLE, ADQUISICION DE FUSIBLES Y DIODOS, MANTENIMIENTO ELECTRICO DE RECTIFICADOR DE CORRIENTE 440 VOLT AC a 220 VOLT DC	CAMBIO DE PORTAFUSIBLE, ADQUISICION DE FUSIBLES Y DIODOS, MANTENIMIENTO ELECTRICO DE RECTIFICADOR DE CORRIENTE 440 VOLT AC a 220 VOLT DC	X	
CAMBIO DE RODAMIENTOS POR RUIDO ECCESVO	CAMBIO DE RODAMIENTOS POR RUIDO ECCESVO	X	
ESTUDIO PARA EL CAMBIO DEL SISTEMA DE CONTROL	ESTUDIO PARA EL CAMBIO DEL SISTEMA DE CONTROL	X	
MANTENIMIENTO DEL FLAP DEL SILENCIADOR DE LA MAQUINA No 2 (MAQUINA DIESEL)	MANTENIMIENTO DEL FLAP DEL SILENCIADOR DE LA MAQUINA No 2 (MAQUINA DIESEL)	X	

Los Datos ingresados al sistema y extraído medio consulta, cumplen exactamente la igualdad con los datos de la tabla mi_ots del SISMAC

DAVID CARRIÓN
Auditor Responsable

AUDITORIA DE SISTEMAS DE INFORMACIÓN

COMPROBACIÓN DE LA LÓGICA E INTEGRIDAD DE DATOS ENTRE LAS TABLAS DE LA BD CONTRA LAS CONSULTAS

FECHA: 03 de marzo del 2005

NOMBRE DE TABLA: m_ots

CONSULTA **Solicitud de Trabajo**

CP1

DATOS INGRESADOS	DATOS DE LA TABLA	CUMPLE CON EL FORMATO	
		SI	NO
MOTOR F/B YAMAHA 48 HP	MOTOR F/B YAMAHA 48 HP	X	
REPARACION DE FUGA HIDRAULICA EN EL CILINDRO DE OPERACION DEL PLANO DE POPA	REPARACION DE FUGA HIDRAULICA EN EL CILINDRO DE OPERACION DEL PLANO DE POPA	X	
CAMBIO DE ELEMENTOS FILTRANTES	CAMBIO DE ELEMENTOS FILTRANTES	X	
CONFECCION DE TAPONES Y CUNAS MADERA EN VARIAS MEDIDAS PARA COMPLETAR PARTIDAS DE CONTROL AVERIAS	CONFECCION DE TAPONES Y CUNAS MADERA EN VARIAS MEDIDAS PARA COMPLETAR PARTIDAS DE CONTROL AVERIAS	X	
CAMBIO DE CIRCUITOS Y CONFECCION DE 0 TAPAS REGISTRO DE TANQUES DE COMBUSTIBLE	CAMBIO DE CIRCUITOS Y CONFECCION DE 0 TAPAS REGISTRO DE TANQUES DE COMBUSTIBLE	X	
CHEQUEO Y REPARACION DE 04 BOMBAS SUMERGIBLES	CHEQUEO Y REPARACION DE 04 BOMBAS SUMERGIBLES	X	
RECUBRIMIENTO TERMICO-ACUSTICO CON POLIURETANO EN EL INTERIOR DEL CASCO DE PRESION, COMPARTIMENTO DE TORPEDOS, RECUBRIMIENTO CON	RECUBRIMIENTO TERMICO-ACUSTICO CON POLIURETANO EN EL INTERIOR DEL CASCO DE PRESION, COMPARTIMENTO DE TORPEDOS, RECUBRIMIENTO CON	X	
PRUEBA DE PRESION DE CAÑERIAS DE AIRE DEL COMPARTIMENTO DE TORPEDOS (AIRE DE ALTA PRESION)	PRUEBA DE PRESION DE CAÑERIAS DE AIRE DEL COMPARTIMENTO DE TORPEDOS (AIRE DE ALTA PRESION)	X	
PRUEBA DE PRESION DE CAÑERIAS DE HIDRAULICA DEPL COMPARTIMENTO DE TORPEDOS (SISTEMA HIDRAULICO)	PRUEBA DE PRESION DE CAÑERIAS DE HIDRAULICA DEPL COMPARTIMENTO DE TORPEDOS (SISTEMA HIDRAULICO)	X	
RECUBRIMIENTO TERMICO DE LOS DUCTOS DE VENTILACION DEL COMPARTIMENTO DE TORPEDOS	RECUBRIMIENTO TERMICO DE LOS DUCTOS DE VENTILACION DEL COMPARTIMENTO DE TORPEDOS	X	
Adquisicion de un purificador de combustible	Adquisicion de un purificador de combustible	X	
ADQUISICION DE BOMBA DE ACHIQUE PORTATIL DE 1,5HP O 1 HP, 220V O 110V	ADQUISICION DE BOMBA DE ACHIQUE PORTATIL DE 1,5HP O 1 HP, 220V O 110V	X	
CABRESTANTE / CAMBIO DE PLANCHAJE DONDE DESCANZA EL CABRESTANTE	CABRESTANTE / CAMBIO DE PLANCHAJE DONDE DESCANZA EL CABRESTANTE	X	
MOTOR F/B YAMAHA 48 (LIMPIEZA GENERAL Y CAMBIO DE SOPORTE DE LA TIRA DE ARRANQUE. INGRESO DE AGUA DE MAR A LAS CAMARAS DE COMBUSTION)	MOTOR F/B YAMAHA 48 (LIMPIEZA GENERAL Y CAMBIO DE SOPORTE DE LA TIRA DE ARRANQUE. INGRESO DE AGUA DE MAR A LAS CAMARAS DE COMBUSTION)	X	
MANTENIMIENTO DE 06 BALSAS SALVAVIDA E INSTALACION DE 06 CANDADOS HIDROSTATICOS	MANTENIMIENTO DE 06 BALSAS SALVAVIDA E INSTALACION DE 06 CANDADOS HIDROSTATICOS	X	
INSPECCION, MANTENIMIENTO Y / O CAMBIO DE BANDEJA CONTENEDORA DE CABLES DE C.H.A. (SONAR CSU3-2)	INSPECCION, MANTENIMIENTO Y / O CAMBIO DE BANDEJA CONTENEDORA DE CABLES DE C.H.A. (SONAR CSU3-2)	X	
ADQUISICION DE TALADRO INDUSTRIAL DE 220V O 110 V	ADQUISICION DE TALADRO INDUSTRIAL DE 220V O 110 V	X	
ADQUISICION DE FILTROS DE TELA PARA EL CLARIFICADOR DE ACEITE DE LA M.M.P.P.	ADQUISICION DE FILTROS DE TELA PARA EL CLARIFICADOR DE ACEITE DE LA M.M.P.P.	X	
CAMBIO DE 04 LLANTAS	CAMBIO DE 04 LLANTAS	X	
CAMBIO DE CHAPA EN LA PUERTA DE LA SALA DE RADIO	CAMBIO DE CHAPA EN LA PUERTA DE LA SALA DE RADIO	X	
BASUIL ARE-A-195 ADQ DE UNA ALARMA	BASUIL ARE-A-195 ADQ DE UNA ALARMA	X	
ALUMBRADO 115 V (CAMBIO DE 06 LAMPARAS)	ALUMBRADO 115 V (CAMBIO DE 06 LAMPARAS)	X	
RECORRIDO E INTEGRACION DEL SISTEMA FRIGORIFICO (FRIGORIFICOS)	RECORRIDO E INTEGRACION DEL SISTEMA FRIGORIFICO (FRIGORIFICOS)	X	
MODERNIZACION DEL SISTEMA DE LIQUIDOMETROS	MODERNIZACION DEL SISTEMA DE LIQUIDOMETROS	X	
CONFECCION DE 09 SONDAS DE LOS DISTINTOS TANQUES DE ABORDO (TANQUES)	CONFECCION DE 09 SONDAS DE LOS DISTINTOS TANQUES DE ABORDO (TANQUES)	X	

ADQUISICION DE PANTALLA PLC Y MODULO DE TERMOCUPLAS (SISTEMA DE CONTROL DE BATERIAS)	ADQUISICION DE PANTALLA PLC Y MODULO DE TERMOCUPLAS (SISTEMA DE CONTROL DE BATERIAS)	X	
ELABORACION DE LAS LISTAS DE CHEQUEO DE LA UNIDAD (COMPARTIMENTAJE)	ELABORACION DE LAS LISTAS DE CHEQUEO DE LA UNIDAD (COMPARTIMENTAJE)	X	

Los Datos ingresados al sistema y extraído medio consulta, cumplen exactamente la igualdad con los datos de la tabla mi:sts del SISMAC

DAVID CARRIÓN
Auditor Responsable

AUDITORIA DE SISTEMAS DE INFORMACIÓN

listado de todo los usuarios con sus respectivo perfil de acceso

CP6

Fecha: 03 de marzo del 2005
Nombre del Entrevistado: Cindy Encalada Moreno
Auditor Responsable: David Carrión
Nombre Modulo : Autorización de acceso

USUARIO	PASSWORD	ENCRIPTADO EN EL SISTMA	SUB-MODULO	INGRESO DE INFORMACIÓN			CONSULTAR	INFORMES
				EMITIR	APROBAR	CERRAR		
ARIAS	TISAR	NO	Mantenimiento	X			X	X
	TI3071	NO	Mantenimiento		X	X		
KBalarezo	andrea	NO	Mantenimiento	X			X	X
EDUARDO	EDU	NO	Mantenimiento	X			X	X
SANTANA	DFRA	NO	Mantenimiento	X			X	X
	D0821	NO	Mantenimiento		X	X		
COLOMA	ELT	NO	Mantenimiento	X			X	X
	ELT	NO	Mantenimiento		X	X		
MALDONADO	besing	NO	Mantenimiento	X			X	X
	besing	NO	Mantenimiento		X	X		
ALFG SANTIN	tr64art	NO	Mantenimiento	X			X	X
	tr64art	NO	Mantenimiento		X	X		
TN CORAL	LANGEL	NO	Mantenimiento	X			X	X
	LANGEL	NO	Mantenimiento		X	X		
Anabell	abi	NO	Mantenimiento	X			X	X
	abi	NO	Mantenimiento		X	X		
RODAS	hugo	NO	Mantenimiento	X			X	X
	hugo	NO	Mantenimiento		X	X		
TI GElectronica	elt	NO	Mantenimiento	X			X	X
sismac	tecnico	NO	Mantenimiento	X			X	
Flores	elt	NO	Mantenimiento	X			X	
Giler	elt	NO	Mantenimiento	X			X	
Geletrónica	elt	NO	Mantenimiento	X			X	
Sarango	TRABAJADOR	NO	Mantenimiento	X			X	
Aviles	123	NO	Mantenimiento	X			X	
TN IARIAS	CM14ING	NO	Mantenimiento	X			X	X
	C1520	NO	Mantenimiento		X	X		
TN ROBELLY	CM12SAR	NO	Mantenimiento	X			X	X
	C4337	NO	Mantenimiento		X	X		

COMENTARIO

Esta cédula de prueba nos muestra la variedad de tipos de claves en formato, perfiles, acceso. La cual nos indica que no guardan un solo estandar en la generación y creación de claves, adicionalmente hemos detectado claves de acceso y autorización repetidas y faciles de deducirlas.

AUDITORIA DE SISTEMAS DE INFORMACION

CP7

Cuestionario aplicado a la administración de claves y control de acceso

Fecha: 02 de marzo del 2005

Departamento : División de Mantenimiento y Planificación

Nombre del Entrevistado: Ing. Cindy Encalada Moreno

Auditor Responsable: David Carrión

Controles de acceso

¿Se asignan claves de acceso para los usuarios en los módulos?
Si, se tiene asignado claves de acceso. Solo existe una clave de acceso pero los permisos son designado de acuerdo a los perfiles de cada persona.

¿Tiene habilitados los mecanismos de contabilidad de las acciones de los usuarios? SI/NO
El SISMAC posee un mecanismo de control de las acciones que indican la Hora Ingreso y Salida, identifica el usuario conectado, las máquinas conectadas y la fecha.
Ver referencia FIGURA 4.12

¿Se registran las acciones que hacen los usuarios sobre las transacciones? SI O NO
Si existe el registro de las acciones de los Usuarios mediante el Log de transacciones.
Ver referencia FIGURA 4.13

¿Sabe la cantidad de usuarios que están conectados?
SI, mediante el módulo SOTFLOCK **Ver referencia FIGURA 4.12**

¿Tiene definido los perfiles de acceso para cada password?
SI tiene definido los perfiles de acceso, la asignación de acceso lo define mediante los niveles de permisos, los cuales son: Acceso por Unidad naval, Equipo y Departamento.

¿Cuál es la política implementada para la gestión de las claves de acceso?
NO existe una política documentada y debidamente legalizada para el establecimiento de claves.

Las claves de acceso utilizan los mecanismos de:

	SI	NO	observación
Asignación	X		No documentada
Confección	X		Generación de claves mediante Soft en Excel **Ver referencia FIGURA 4.11**
Control de Claves	X		Automáticamente mediante el sistema

Las claves de acceso son escogida por:

El Usuario	No
El Administrador	Las claves de acceso son definidas por el Administrador del Sistema de Aplicación.

¿Qué longitud tienen las claves?
Las claves son de 5 dígitos

¿Cómo están conformadas las claves? (composición)
1 dígito tipo Chart y 4 dígitos numéricos aleatorios

¿Existe una periodicidad de actualización de claves (documentadas)?
Si existe, pero no la tenemos documentada .

¿Quièn actualiza las claves ?
La administradora del Sistema de Aplicaciones

¿Con qué peridicidad actualizan las claves?
Cada Año , o cada vez que lo solicitan, o cuando hay movilización de personal

¿Las cuentas sin usar son suprimidas?
Si, pero no existe un procedimiento establecido para suprimirlas. Esto se hace cuando lo solicita algún taller o reparto.

¿Las claves de acceso son encriptadas?
No, el archivo de autorizaciones no tiene enciptado las claves de acceso.

¿Los intentos de claves de acceso inválidas son detectadas, resgistrada y bloqueadas?
Si son bloqueadas, es decir que si la clave no es exacta no podrá ingresar al sistema.

¿Estàn definidos los usuarios y claves en forma independiente?(una clave para cada usuario)
No, debido a que no existe una cantidad adecuada de licencias que satisfaga la cantidad de empleados y usuarios del sistema.

¿Quién tiene asignado cuentas de supervisor y quién autoriza la asignación de estás cuentas?
Los señores que brindan asistencia y soporte al usuario que trabajan en el departamento de administración del sistema, la clave es asignada por el Administrador del Sistema.

¿Quién conoce las claves de supervisor?
El admistrador y supervisor.

¿Existe algún manual donde se registren los erroes y Fallas del sistema?
No existe un manual donde se registren los errores y fallas, pero si existen los Logs de errores y transacciones del Sistema. **Ver referencia FIGURA 4.13**

AUDITORIA DE SISTEMAS DE INFORMACIÓN

PARA EVALUAR LOS CONTROLES DE VALIDACIONES DE LOS MÓDULOS DEL SISTEMA MEDIANTE LA EJECUCIÓN DE TRANSACCIONES DE PRUEBAS

CP8

Fecha: 04 de marzo del 2005

Auditor Responsable: David Carrión M.

Aplicación: Mantenimiento

OPCIONES DE MENÚ		Nombre del CAMPO	NATURALEZA DEL CAMPO	DATOS //VALORES INGRESADOS	Cumple con el tipo de CONTROL DE VALIDACION			COMENTARIO
					Formato	Faltante	Razonabilidad	
O/T	Datos Básicos	Cuenta Contable	Combo de selección de datos	Selección/Asignación	OK	OK	OK	OK
O/T	Datos Básicos	Centro de Costo	Combo de selección de datos	Selección/Asignación	OK	OK	OK	OK
O/T	Datos Básicos	Destino de la O/T	Combo de selección de datos	Selección/Asignación	OK	FALTA	OK	El sistema acepta emitir una O/T sin definir el Destino (este dato es indispensable para el proceso de mantenimiento)
O/T	Datos Básicos	sección que ejecuta el trabajo	Combo de selección de datos	Selección/Asignación	OK	OK	OK	OK
O/T	Programación	Programación #de días	Numérico	2,3,16,18,…….20	OK	OK	OK	OK
O/T	Programación	Días programados	Numérico	Automáticamente	OK	OK	OK	OK
O/T	Programación	Fecha de Programación de la O/T	Combo de selección de Fecha	Selección o asignación de la fecha	OK	OK	FALTA	La Fecha es Manipulable, se puede cambiar la fecha a conveniencia, puede colocar años, meses y días anteriores
O/T	Costeo, Datos Adicionales	Porcentaje de Ejecución de la O/T	Registro del valor Porcentual (numérico)	4,6,8,19,20,35….100%	OK	FALTA	OK	Carece de validación ya que falta el valor porcentual de una O/T la cual es muy importante.

O/T	Estado	# de O/T	Autonumérico secuencial	Transacciones de Pruebas	OK	OK	OK	OK
O/T	Estado	Fecha de O/T	Fecha	Transacciones de Pruebas	OK	OK	OK	OK
O/T	Movimiento de Envío	Fecha de Recepción	Fecha	Transacciones de Pruebas	OK	OK	FALTA	La Fecha es Manipulable, se puede cambiar la fecha a conveniencia, puede colocar años, meses y días anteriores
S/T	Datos Básicos	Sección Solicitante	Combo de selección de datos	Transacciones de Pruebas	OK	FALTA	OK	Al momento de generar una S/T el sistema permite no llenar este dato (este dato es fundamental para el sistema)
S/T	Estado	# de S/T	Autonumérico secuencial	Transacciones de Pruebas	OK	OK	OK	

AUDITORIA DE SISTEMAS DE INFORMACIÓN

RESPALDO DE INFORMACIÓN

CP9

Fecha: 02 de marzo del 2005

Departamento : División de Mantenimiento y Planificación

Nombre del Entrevistado: Ing. Xavier Mancero Ordoñez

Auditor Responsable: David Carrión

SISTEMA DE BACKUPS

Poseen una política de respaldos de información ?

Si, existe.

Por efecto de prueba solo tuvimos acceso a chequear, revisarla,pero sin tener el acceso a sacarle copia para pruebas de auditoría

¿Qué mecanismos de Backups se han implementado?

Mediante una ejecución programada para respaldar automáticamente a un hora y día determinado

¿Con qué periodicidad se realizan los mismos?

Diariamente de 12:00 a 13:00

¿En qué soportes se realiza?

En una Base de Datos: Informix Server V.7.22

¿Cuántos Backups se realizan?

Una sola por día

¿Dónde se guardan los Backups?

En un servidor de respaldos

¿Quién controla el funcionamiento de los mismos?

El administrador del servidor de Datos

¿Quién se responsabiliza de la información guardada?

El administrador del servidor de Datos

AUDITORIA DE SISTEMAS DE INFORMACIÓN

CHEQUEO Y EVALUACIÓN DE LOS PLANES DE CONTINGENCIA

CF

Fecha: 02 de marzo del 2005
Departamento : División de Mantenimiento y Planificación
Nombre del Entrevistado: ING. Xavier Mancero Ordoñez
Auditor Responsable: David Carrión

#	Planes de Contingencia en caso de fallas del sistema	Si	No	N/A	Constatación Física	Comentarios
2	Políticas y Procedimientos para actuar y resolver problemas de fallas del sistema.		x			
3	Existen procedimientos de respaldos de datos (backups)	x			CP9	diariamente de 12:00 a 13:00
4	Se cuentan con registro de control de respaldos realizados	x			Indagación	mediante log de respaldo
5	Se mantienen copias de respaldo en una localidad segura	x			visual	Se cuenta con otro servidor, en un lugar de acceso restringido y adicionalmente una biblioteca de respaldos de
6	Baterias de respaldo energético	x			visual	Exista un UPS y una planta generadora
7	Almacenamiento y custodia de datos en un lugar seguro	x			visual	Área restringida, acceso con tarjetas magnéticas
8	El lugar temperado (fuera del frío y el calor);	x			visual	un correcto clima que evita que las computadoras sufran recalentamiento y por lo consiguientes daños.

Del área del Administrador del servidor de Datos no nos permitieron sacar pruebas , ni copias a documentos. La revisión es visual y en base a preguntas.

AUDITORIA DE SISTEMAS DE INFORMACIÓN

CHEQUEO Y EVALUACIÓN DE LA SEGURIDAD FÍSICA

CG

Fecha: 02 de marzo del 2005

Departamento : División de Mantenimiento y Planificación

Nombre del Entrevistado: XXXXXXX

Auditor Responsable: David Carrión

#	Seguridad Física y Ambiental	Si	No	N/A	Constatación Física	Comentarios
1	Cuenta con una política documentada donde se considere todos los aspectos de seguridad física de los servidores y	x			si	Chequeo ocular
2	Cuentan con extintores de fuego.	x			si	Chequeo ocular
3	Están localizados en puntos claves del área de tecnología?	x			si	Chequeo ocular
4	Existen detectores de humo.	x			si	Chequeo ocular
5	Disponen de protección de cables de red.	x			si	Chequeo ocular
6	Existe un regulador de poder instalado y adecuadamente protegidos contra fallos eléctricos?	x			si	Chequeo ocular
7	Cada que tiempo se prueban las condiciones de la fuente de poder o UPS?	x			si	Una vez cada semana revisan la Bateria y el regulador
9	Existe un nivel de autoridad requerido para retirar equipo de las instalaciones	x			si	una orden documentada del jefe prinipcal
10	Existe medidas de seguridad en caso de robo o sabotaje del sistema o componente físico	x			si	cámas activas, guardias, puertas elctricas mediante identificador
11	Existe un adecuado ambiente- Entorno (temperatura, humedad, ventilación).	x			si	Chequeo ocular
12	Cuentan con señalización adecuada de los lugares restringidos .		x			Deberían colocar.

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
1. Conocer la situación actual del sistema de información y de las áreas relacionadas.	1.1. Segregación de Funciones.	1.1.1.Cuestionario de entrevistas	1.1.1.1. Se laboró y se aplicó un cuestionario de visita Previa donde se entrevistó al personal encargado del SMAC ref. CVP	1.1.1.1.1. Existe una ordena y adecuada designación de funciones y actividades dentro del departamento que administra el sistema.	1.1.1.1.1.1.---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	1.1.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
	1.2. Documentación y manuales de Operaciones.	1.2.1. Cuestionario de entrevistas	1.2.1.1. Se elaboró y se aplicó un cuestionario donde se preguntó la existencia de, Flujo de proceso de Información, manual del administrador (Diagrama de entidad y relación del sistema, tablas, configuración y aspectos técnicos básicos), Planes de desarrollo, mantenimiento y mejoras del sistema. Y el	1.2.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	1.2.1.1.1.1. No existe un plan documentado de desarrollo, mantenimiento y mejoras del sistema	1.2.1.1.1.1.1. Documentar los planes y procedimientos de desarrollo, mantenimiento y mejoras del sistema.

			manual de usuario			
		1.2.2.Confirmación y observación	1.2.2.1. Se confirmó la existencia de la documentación consultada.	1.2.2.1.1. El manual de Usuario está actualizado hasta los últimos cambios, además es muy explicativo y entendible para los usuarios.	1.2.2.1.1.1. No existe manual de administrador actualizados a las últimas modificaciones del sistema.	1.2.2.1.1.1.1. Se debe actualizar el manual del administrador. a las últimas modificaciones.

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
2. Evaluar la administración de las claves de accesos a los módulos del sistema.	2.1. Políticas de diseños, asignación, actualización y eliminación de claves de accesos (contraseñas).	2.1.1. Cuestionario de entrevistas.	2.1.1.1. Se elaboró y se aplicó un cuestionario en el cual se preguntaba la existencia de alguna política documentada. Para el manejo y diseño de las claves de accesos.	2.1.1.1.1. ---	2.1.1.1.1.1. No existe una Política documentada y legalizada donde se establezcan normas y parámetros para el diseño, asignación y eliminación de claves de accesos.	2.1.1.1.1.1.1. Se debe redactar, legalizar, presentar y publicar una política que justifique y defina parámetros en el diseño, asignación, actualización y eliminación de claves de accesos.
	2.2. Administración de contraseñas y perfiles de acceso.	2.2.1. Cuestionario de entrevistas.	2.2.1.1. Se elaboró y se ejecutó un cuestionario en el cual se consultaba la forma de diseñar claves de acceso y la forma de asignarle e perfil de usuario. También se consultó los periodos de actualización y eliminación de claves.	2.2.1.1.1.---	2.2.1.1.1.1. El sistema carece de una adecuada asignación de perfiles de acceso y ejecución de acciones que permita autorizar o restringir la programación, asignación de tareas, horas hombres, aprobación, anulación y cierre de Ordenes de trabajos.	2.2.1.1.1.1.1. Definir de mejor manera los perfiles de acceso de cada usuario de acuerdo a sus necesidades y acciones. Además se deberá contactar al proveedor del sistema para que establezcan mejores sistemas de control y acceso en lo que respecta a la asignación de perfiles de acceso.

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

					2.2.1.1.1.2. No existe una adecuada periodicidad de Cambio o actualización de claves de acceso al sistema.	2.2.1.1.1.2.1. Definir y documentar un procedimiento donde establezcan una efectiva periodicidad de cambio o actualización de claves de acceso al sistema.
		2.2.2. Datos de Pruebas	2.2.2.1. Se ingresó a la BD y se procedió a la selección del archivo de autorizaciones.	2.2.2.1.1.---------- ---------- ---------- ----------	2.2.2.1.1.1. ---------- ---------- ---------- ----------	2.2.2.1.1.1.1.---------- ---------- ---------- ----------
			2.2.2.2. Se los importó a un software de auditoría llamado IDEA.	2.2.2.2.1.---------- ---------- ---------- ----------	2.2.2.2.1.1.---------- ---------- ---------- ----------	2.2.2.2.1.1.1. ---------- ---------- ---------- ----------
			2.2.2.3. Se evaluó los aspectos de diseño en términos de Independencia, Longitud, repetición y permisos de accesos. Ver ref.	2.2.2.3.1.---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	2.2.2.3.1.1. Existen claves de acceso al sistema que son idéntica a las claves de aprobación.	2.2.2.3.1.1.1. Se debe cambiar todas las claves de acceso iguales y aplicar algún tipo de identificador de claves a nivel de tablas que evite el registro de contraseñas iguales.

			CP6 y CP7.		2.2.2.3.1.2. Existen claves de acceso al sistema que se repiten.	2.2.2.3.1.2.1. Se debe cambiar, redefinir y estandarizar las claves existentes que no guarden el modelo y formato con lo establecido por el programa de generación de claves que ya poseen, además registrar y controlar que cada persona posea una contraseña distinta de las demás.
					2.2.2.3.1.3. Las claves de acceso y aprobación no son significativas, no guardan un solo diseño y estandarización en longitud y forma de elaborarse.	2.2.2.3.1.3.1. Se recomienda utilizar un solo estándar para generar o crear claves, las cuales tengan como mínimo seis a ocho caracteres.
					2.2.2.3.1.4. Existen varias claves de acceso que no son individuales. (Es elaborada para un grupo de personas)	2.2.2.3.1.4.1. Se debe crear una clave de acceso para cada usuario, para que a su vez se pueda supervisar las acciones

						de cada uno, y en el caso que se presente alguna anomalía se proceda a la sanción o a la observación de dicho usuario
	2.3. Control de acceso	2.3.1. Cuestionario de entrevistas	2.3.1.1. Se elaboró se ejecutó un cuestionario donde se consulta sobre la existencia de controles de accesos que identifique los usuarios conectados y el historial se sus acciones.	2.3.1.1.1. Existe una pequeña aplicación llamada SOFTLOCK el cual indica todos los usuarios que se encuentran conectados en tiempo, maquina y acción ejecutante. Adicionalmente existe un Log de transacciones, el cual indica todos los detalles de las transacciones realizadas por los usuarios.	2.3.1.1.1.1. ----------	2.3.1.1.1.1.1. ----------

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
3. Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones al momento de hacer cambios.	3.1. Políticas del autorización y aprobación de cambios	3.1.1. Cuestionario de entrevistas.	3.1.1.1. Se elaboró y se ejecutó un cuestionario donde se consultaba la existencia de una política de autorización y aprobación de cambios en el sistema.	3.1.1.1.1. ----------	3.1.1.1.1.1. ----------	3.1.1.1.1.1.1.----------
		3.1.2.Confirmación Observación	3.1.2.1. Se constató la existencia y vigencia de l contrato realizado con el proveedor del sistema.	3.1.2.1.1. Si existe una política la cual hace referencia a un contrato que se realizó con el proveedor donde se explica los procesos y procedimientos para hacer cambios a la aplicación.	3.1.2.1.1.1. ----------	3.1.2.1.1.1.1. ----------
	3.2. Firma Autorizada	3.2.1.Observación	3.2.1.1. Se procedió a verificar la existencia de autorizaciones documentadas y firmadas por el jefe superior del área.	3.2.1.1.1. Si existe la documentación previa donde se autoriza alguna ejecución de cambios o actualización	3.2.1.1.1.1. ----------	3.2.1.1.1.1. ----------

	3.3. Bitácora de registro	3.3.1. Cuestionario de entrevistas.	3.3.1.1.Se aplicó una serie de preguntas, en las cuales una de estas consultaba la existencia de hojas, bitácoras o libros donde se registraban los cambios realizados	3.3.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	3.3.1.1.1.1. No existe un documento donde se registre en forma ordenada y actualizada todos los cambios que haya recibido el sistema.	3.3.1.1.1.1.1. Realizar una bitácora de registros de modificaciones del sistema.

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
4. Determinar el ambiente del hardware y software del servidor de aplicaciones, del servidor de datos y equipos de ciertos usuarios, en términos de disponibilidad y requisitos técnicos.	4.1.Custodia de los servidores	4.1.1. Cuestionario de entrevista.	4.1.1.1. Mediante el cuestionario de visita previa se investigó quienes son los responsables y administradores del sistema.	4.1.1.1.1. Existen dos personas debidamente asignadas para la administración del sistema. Uno es el administrador del servidor de aplicaciones y el otro es el administrador del servidor de BD.	4.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	4.1.1.1.1.1.1 ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
	4.2.Identificación de equipos de cómputos	4.2.1. Verificación	4.2.1.1. Se solicitó al departamento un listado de la ubicación de los computadores destinados para la ejecución de sistema. y se procedió a la verificación	4.2.1.1.1. Existe una efectiva y actualizada base de datos donde se encuentra las características técnicas de las computadoras que trabajan con el sistema.	4.2.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- -	4.2.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
5. Evaluar la integridad y validez de los datos de entrada a los módulos del sistema	5.1.Control de validación	5.1.1.Transacciones de pruebas	5.1.1.1. Se procedió a la ejecución de transacciones de Prueba en las cuales tratábamos de registrar valores y datos reales, normales, ilógicos, imposibles y valores extremos.	5.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	5.1.1.1.1.1. Existen varios campos de la Orden de trabajo y Solicitud de trabajo que no se encuentran validados.	5.1.1.1.1.1. Contactar al proveedor del sistema y solicitarle mediante contrato la ejecución de validación de los campos identificados.

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
6. Evaluar el plan de contingencia de la aplicación en caso de fallas del sistema.	6.1. Políticas y procedimientos	6.1.1. Cuestionario de entrevista	6.1.1.1. Se elaboró y se ejecutó ciertas preguntas en las cuales consultaba la existencia de políticas o planes de contingencias para resolver fallas del sistema en caso que se presenten.	6.1.1.1.1.---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	6.1.1.1.1.1. No existe una política o plan de contingencia que eviten situaciones de riesgos y problemas al suscitarse una falla en el sistema.	6.1.1.1.1.1.1. Debe elaborarse un plan de contingencia documentado y adecuado a las situaciones del departamento para atender y resolver fallas del sistema.
	6.2.Procedimientos de respaldo de información (Backups)	6.2.1. Cuestionario de entrevista	6.2.1.1. Mediante un cuestionario pudimos tener conocimiento de la existencia de políticas y procedimientos de respaldo de información.	6.2.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- --	6.2.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----	6.2.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- -
		6.2.2.Confirmación y observación	6.2.2.1. hemos procedimos a comprobar la veracidad y vigencia de dicho documento	6.2.2.1.1. ---------- ---------- ---------- ---------- ----------	6.2.2.1.1.1. ---------- ---------- ---------- ---------- ---------- -	6.2.2.1.1.1.1. ---------- ---------- ---------- ---------- ----------

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
7. Evaluar las medidas de seguridad considerando los aspectos de confiabilidad y disponibilidad de la información.	7.1. Política de seguridad física	7.1.1. Cuestionario de entrevista	7.1.1.1. Se elaboró y se ejecutó un cuestionario donde se consultaba la existencia de una política documentada de seguridad física donde conste los aspectos de control.	7.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	7.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	7.1.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
		7.1.2. Confirmación y observación.	7.1.2.1. Se revisó y se confirmó la existencia de la política de seguridad física.	7.1.2.1.1. Existe una Política adecuada, actualizada y documenta donde consta todos los objetivos de control físico.	7.1.2.1.1. Hemos podido apreciar la falta de cumplimiento de la política de seguridad física ya que el servidor de aplicaciones se encuentra en un lugar de fácil acceso a las personas (Sabotajes, travesuras, daños y errores)	7.1.2.1.1.1. Es Importante que todo servidor, de datos o aplicaciones esté debidamente resguardado en un lugar seguro y restringido, ubicado de tal manera que no exista la posibilidad de accidentes personales contra el computador ni manipulación del equipo por cualquier persona

ANEXO 3
MATRIZ DE OBJETIVOS Y CONTROLES

Objetivo Específico	Controles	Técnicas Usada	Actividades	Fortaleza	Debilidades	Recomendaciones
8. Identificar el proceso y Flujo de Información del sistema.	8.1. Documentación	8.1.1. Cuestionario de entrevista.	8.1.1.1. Mediante cuestionario se consultó sobre el flujo de información del sistema. Para lo cual nos facilitaron una explicación y unas figuras. ref. FIGURA 4.4, 4.5, 4.6	8.1.1.1 Existe una documentación adecuada de los procesos de información, tanto del sistema como del proceso de mantenimiento.	8.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	8.1.1.1.1.1. ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------

ANEXO 4
INFORME FINAL DE LA EVALUACION

Guayaquil, Marzo 08 de 2005

Distinguido Señor:

En cumplimiento al acuerdo, realizado con la distinguida compañía que Ud. dirige en el Contrato de la prestación de servicio de asesoría administrativa en la evaluación de los controles y seguridades del Sistema de Mantenimiento asistido por computadora (SMAC); y en relación a las necesidades y problemas presentados por su compañía a través de objetivos elaborados conjuntamente me permito indicarle que el trabajo ha sido concluido de manera exitosa.

Entrego a usted el presente informe en el cual podrá encontrar todas las debilidades que han sido detectadas y las respectivas recomendaciones realizadas.

Atentamente;

ACG. David Carrión M.
Presidente
DConsulting S.A.

Evaluación de Controles y seguridades del Sistema de Mantenimiento asistido por computadora de una empresa del sector Naviero.

Antecedentes de la Empresa

Talleres Integrados es una empresa dedicada a dar mantenimiento preventivo, correctivo y de mejoras a las unidades navales las cuales son consideradas como parte del activo de una de las compañías de la misma corporación. Esta empresa es reconocida a nivel nacional, posee una gran cantidad de unidades navales tales como Veleros, Remolcadores y Fragatas entre otras, en todo el litoral Ecuatoriano.

La sede de esta empresa es en Guayaquil, posee un extenso territorio para ejecutar todas las operaciones de mantenimiento y cuenta con una gama de empleados en calidad de especialistas encargado de las diferentes tareas encomendadas.

Ante una serie de problemas suscitado en la compañía en relación al manejo del sistema, la Dirección General en acuerdo con varios miembros de la misma procedió a la contratación de una Auditoría externa con finalidad de efectuar la evaluación al Sistema de mantenimiento Asistido por computadora de una empresa del sector Naviero, por el período de 01- 31 de marzo del 2005.

Entre los motivos más relevantes que pudimos receptar son los siguientes:

1. Desconocimiento del sistema por parte de los directivos.
2. Desconocimiento de la existencia de adecuados procedimientos en la asignación, actualización y eliminación de claves de acceso.
3. Desconocimiento de la existencia de la documentación del sistema y los procedimientos y tareas de respaldo de información.
4. Desconocimiento de la existencia de controles generales y específicos que garanticen la veracidad e integridad de la información.
5. Desconocimiento de la existencia de un plan de contingencia donde se establezcan los procedimientos para resolver fallas.
6. Desconocimiento de políticas y objetivos de seguridad física y lógica.
7. Desconocimiento del proceso y flujo de información de las actividades de mantenimiento de la empresa por parte de los usuarios y directivos.

Estos problemas detectados nos ayudaron a delimitar nuestro trabajo para los siguientes objetivos:

Objetivos de la Auditoría.

1. Conocer la situación actual del sistema de información y de las áreas relacionadas
2. Evaluar la administración de las claves de accesos a los módulos del sistema.
3. Evaluar los procesos y procedimientos de la administración del servidor de aplicaciones al momento de hacer cambios.

4. Determinar el ambiente del hardware y software del servidor de aplicaciones, del servidor de datos y equipos de ciertos usuarios, en términos de disponibilidad y requisitos técnicos.
5. Evaluar la integridad y validez de los datos de entrada a los módulos del sistema
6. Evaluar el plan de contingencia de la aplicación en caso de fallas del sistema.
7. Evaluar las medidas de seguridad físicas considerando los aspectos de integridad, confiabilidad y disponibilidad de la información.
8. Identificar el proceso y Flujo de Información del sistema.

Resultados de la Evaluación.

De acuerdo a la evaluación realizada encontramos las siguientes debilidades en:

1. No existe un plan documentado de desarrollo, mantenimiento y mejoras del sistema.
2. No existe manual de administrador actualizados a las últimas modificaciones del sistema.
3. No Existe políticas ni procedimientos documentados y aprobados donde se establezcan los criterios estándares para la creación, asignación y eliminación de claves de acceso.
4. El sistema carece de una adecuada asignación de perfiles de acceso y ejecución de acciones que permita autorizar o restringir la programación, asignación de tareas, horas hombres, aprobación, anulación y cierre de órdenes de trabajos.
5. No existe una adecuada periodicidad de cambio de las claves de acceso.

6. Existen claves de acceso al sistema que son idéntica a las claves de aprobación.
7. Existen claves de acceso al sistema que se repiten.
8. Las claves de acceso y aprobación son significativas, no guardan un solo diseño y estandarización en longitud y forma de elaborarse.
9. Existen varias claves de acceso que no son individuales. (Son usadas por un grupo de personas).
10. No existe un documento donde se registre en forma ordenada y actualizada todos los cambios que se hacen al sistema.
11. Existen varios campos de la Orden de trabajo y Solicitud de trabajo que no son validados.
12. No existe un plan de contingencia que delinee las acciones a ejecutar ante fallas en el sistema.
13. El servidor de aplicaciones se encuentra en un lugar de fácil acceso a las personas. (Sabotajes, travesuras, daños, errores).

Resultados de la Evaluación.

A continuación se presenta un análisis detallado de las debilidades encontradas, los efectos y una serie de recomendaciones orientadas a eliminar dichas falencias detectadas en el manejo y ejecución del sistema de mantenimiento.

1. **No existe un plan documentado de desarrollo, mantenimiento y mejoras del sistema.**

SITUACIÓN ACTUAL.

Durante la revisión pudimos observar que la administración del sistema no posee un plan documentado de desarrollo, mantenimiento y mejoras del sistema.

EFECTO.

Esta Situación permite que:

- No se tenga una planificación adecuada de los trabajos necesarios que se deben ejecutar.
- No se posean un orden adecuado de las prioridades a ejecutarse.
- Los trabajos que se realicen no sean los adecuados o existan cambios o alteraciones innecesarias.
- Las modificaciones o mantenimiento no sean continuos, ordenados y bien realizados.

RECOMENDACIONES

Se debe establecer un plan debidamente estudiado y documentado de las actividades a realizar, tanto de los posibles cambios o modificaciones y de los mantenimiento preventivos del sistema. Este plan debe poseer como mínimo la siguiente información. Área, sección o módulo al cual se le va ejecutar dicho mantenimiento o modificación, las actividades a realizar, la fecha de ejecución y las posibles personas a intervenir en dicho trabajo.

2. **No existe manual de administrador actualizados a las últimas modificaciones del sistema.**

SITUACION ACTUAL

Durante la evaluación del Sistema, se solicitó una serie de documentación tales como manuales de administrador y manuales del usuario, de los cuales solo estaba actualizado el manual del usuario.

EFECTOS.

Esta situación conduce a problemas de:

- Dificultad y pérdida de tiempo en la implementación de cambios o modificaciones al sistema en el caso que estén ausente las personas que están familiarizadas con el sistema.
- Dificultad para los nuevos usuarios en aprender a utilizar el sistema.

RECOMENDACIONES

Es importante mantener la documentación del sistema completo los cuales deben incluir Manual de usuario, manual técnico, manual de operación y la documentación de los programas, Así mismo los registros de las modificaciones realizadas a la aplicación, en el cual se incluya la fecha, descripción, análisis, encargado, usuario, firma de revisión y aprobación del usuario con respecto a los cambios realizados, etc. Esto debe realizarse para cada modificación, a fin de tener un documento de respaldo en caso de reclamos posteriores.

3. **No Existe políticas ni procedimientos documentados y aprobados donde se establezcan los criterios estándares para la creación, asignación y eliminación de claves de acceso**

SITUACIÓN ACTUAL.

Durante la revisión pudimos observar que la administración de claves no posee una política formal y documentada.

EFECTO.

Esta Situación permite que:

- No se lleve un control adecuado de quiénes y cuántos poseen permisos de accesos y de autorización con los respectivos perfiles para ejecutar una actividad.
- No se tenga una normativa de respaldo para establecer un estándar en el diseño y asignación de usuarios.
- Muchas claves de acceso y aprobación sean repetidas.
- No exista un adecuado procedimiento y una norma que regularice las acciones para anular todas las claves que han dejado de ser usadas por personal que se cambia de departamento o reparto y/o sale de la empresa.

INFORME FINAL

RECOMENDACIONES

Elaborar, documentar y aprobar una política con sus respectivos ítems donde se establezca la metodología de manejo, generación y asignación de claves. Este documento debe tener como base la clasificación de claves de acuerdo al nivel de autorización, los procedimientos de asignar un USER y PASSWORD, la longitud de la clave, el periodo y la forma de actualización, los niveles emisión, autorización por perfiles de usuarios y la forma de combinar o generar claves estándares. Es muy importante que esta política defina los responsables de cumplir y hacer cumplir dicha norma.

4. **El sistema carece de una adecuada asignación de perfiles de acceso y ejecución de acciones que permita autorizar o restringir la programación, asignación de tareas, horas hombres, aprobación, anulación y cierre de Ordenes de trabajos.**

SITUACION ACTUAL

Durante la revisión se pudo observar que existen varias claves de acceso que permiten ejecutar acciones que no le conciernen; por ejemplo una persona de un reparto XX que debería tener permiso solo y exclusivamente para el reparto XX, pero estas personas puede tranquilamente generar una Orden de trabajo (O/T) de un reparto YY, así mismo emitirla, programarla, anularla y en otro de los caso Autorizarla (aprobar o cerrar) la O/T con cualquier clave de cualquier reparto que tenga permiso de autorización.

EFECTOS

Este tipo de errores puede causar que:

- La información que se presente hacia los superiores no será lo suficientemente veraz y confiable; por ende no se tomarán decisiones acertadas.
- Cualquier persona que sepa la clave de algún superior o que tenga alguna clave de acceso o de aprobación que no le pertenezca, puede que genere grandes problemas con respecto a quién fue el responsable de aprobar o autorizar tal actividad o ejecución de mantenimiento.

RECOMENDACIONES

Cada clave de acceso y autorización deben estar mejor definida especificando los niveles de acceso. Se deberá contactar al proveedor del sistema y solicitar que filtren con mayores controles los accesos de los usuarios, de tal forma que esto garantice que la información ingresada, borrada y actualizada esté dentro de los parámetros de control; para que a fechas posteriores esta información sea de mayor confianza y utilidad para una efectiva y acertada toma de decisiones.

5. No existe una adecuada periodicidad de cambio de las claves de acceso.

SITUACION ACTUAL

Durante la revisión se pudo observar que el tiempo de cambio o actualización de las claves de acceso y autorización es realizada una vez al año, sin utilizar un proceso y procedimiento definido y documentado.

EFECTO

Esta situación permite que:

- Personas no autorizadas lleguen a conocer con el tiempo la clave de algún usuario.
- Con estas claves pirateadas cualquier tipo de persona que no esté autorizada acceda a la información del sistema y realice operaciones no delegadas o acceda al sistema para sacar información confidencial.

RECOMENDACIONES

Se debe definir políticas de seguridad de datos que incluyan: Intervalo de tiempo para cambios de clave, administrador de las seguridades del sistema, estándares de creación de usuarios, entre otras cosas.

6. **Existen claves de acceso al sistema que son idéntica a las claves de aprobación.**

SITUACION INICIAL

Producto de la revisión y evaluación de la tabla donde se encuentra los usuarios con las respectivas claves de acceso al sistema y las claves para autorización, pudimos observar que el 40% De total de usuarios que poseen claves de acceso al sistema y claves de autorización son idénticas, es decir que no guardan independencia para ejecución de actividades.

EFECTO

Este tipo de situaciones puede causar:

- Que las claves sean de fácil deducción y por ende fácil de copiar y luego ser utilizada por otras personas.
- En caso que una persona utilice una clave no autorizada y/o equivocada afectará de manera considerable la integridad y proceso de la información.

RECOMENDACIONES

Cambiar todas las claves que sean iguales, y aplicar algún tipo de identificador de claves a nivel de tablas que permita evitar el registro de contraseñas iguales.

7. Existen claves de acceso al sistema que se repiten

SITUACION ACTUAL

Producto de la revisión y evaluación de la tabla donde se encuentra los usuarios con las respectivas claves de acceso al sistema y las claves para autorización, pudimos observar que el 25% del total de usuarios que poseen claves de acceso al sistema son repetidas.

EFECTO

Esta situación puede afectar en:

- La individualidad y confidencialidad de las claves, debido a que varias personas pueden deducir y aplicar sus claves pero con diferentes usuarios.
- Esta situación hará que cualquier persona que desea molestar o cometer fallas, procederá a crear y registrar información a nivel que le es permitido por la clave, lo cual afectará directamente la veracidad e integridad de la información. Esto indicará que la información no será confiable.

RECOMENDACIONES

Cambiar, redefinir y estandarizar las claves existentes que no guardan el modelo y formato con lo establecido por el programa de generación de claves que ya poseen, además registrar y controlar que cada persona posea una contraseña distintas de las demás y aplicar una rutina de programación que permita al sistema evaluar las claves de usuarios, a fin de verificar la redundancia o duplicidad de claves.

8. **Las claves de acceso y aprobación son significativas, no guardan un solo diseño y estandarización en longitud y forma de elaborarse.**

SITUACION ACTUAL

Durante el análisis conocimos que existe una diversidad de formatos de claves, es decir que unos están generados por números aleatorios, otras claves están registradas con nombres de personas, otros con años de nacimiento, otros con iniciales de alguna palabra, por ende no guarda un solo estándar en el registro y control de claves de acceso y aprobación.

EFECTO

Esta situación permite que:

- Se reste confidencialidad y seguridad al sistema, ya que las claves son muy distintas y en ciertas son muy pequeñas, las cuales son fácil de aprender y de copiar.
- Se produzcan eventualmente accesos no autorizados al sistema.

RECOMENDACIONES

Es recomendable utilizar un solo estándar para generar o crear claves, las cuales tengan como mínimo seis a ocho caracteres, así mismo debe existir una actualización y estandarización de todas las contraseñas que se encuentran registradas en la base de datos.

9. **Existen varias claves de acceso que no son individuales. (Son usadas por un grupo de personas).**

SITUACION INICIAL

Durante la revisión se pudo observar que existen varias claves de acceso que son asignadas a un grupo de usuarios, por ejemplo la clave para el laboratorio PL41 es asignada para las 4 personas que trabajan ahí.

EFECTO

Estas situaciones permiten que:

- No exista la característica básica de seguridad en la asignación de claves de forma individual.
- Se divulguen de manera considerable las claves y se dé el caso que personas no autorizadas hagan uso de la misma (claves).
- La información no sea íntegra y confidencial.
- Las claves y contraseñas se entreguen o se presten entre compañeros y en un momento dado varias personas querrán hacer uso de la misma, lo cual no permite el sistema. Luego surgirán problemas como atrasos, deficiencia y molestia para cumplir con las actividades de ingresos, consultas o cierres encomendadas dentro del sistema.

INFORME FINAL

RECOMENDACIONES

Recomendamos la creación de una clave de acceso para cada usuario, para que a su vez se pueda supervisar las acciones de cada uno, y en el caso de presentarse alguna anomalía se proceda a la sanción o a la observación de dicho usuario.
Esto permitirá monitorear la cantidad de trabajo, las transacciones realizadas, monitorear el cumplimiento de información, la calidad, la cantidad de datos que ingrese y la periodicidad de modificaciones y de acceso.

Se recomienda adquirir un número considerable de licencias concurrentes para trabajar al mismo tiempo, crear los usuarios y acceso por persona pero tomando como medida de seguridad una adecuada capacitación en el cual se explique las consecuencias de vulnerabilidad, integridad y confidencialidad de la información ingresada y las sanciones a las que estarán sujetos en caso de no cumplir con dicha política de individualidad y confidencialidad de claves de acceso.

10. No existe un documento donde se registre en forma ordenada y actualizada todos los cambios que se hacen al sistema.

SITUACION INICIAL

Durante la revisión observamos que no se tiene un documento donde se registre los cambios y actualizaciones que se le haya hecho al sistema.

EFECTO

Esta situación puede causar que:

- No se tenga un control de todas las modificaciones que se le haya efectuado al sistema.
- No se tenga un documento de respaldo en caso de problemas o acuerdos con el proveedor del sistema. Ya que en este debe ir todas las modificaciones y actualizaciones realizadas.

RECOMENDACIÓN

Elaborar una bitácora de control donde se registre todos y cada uno de los cambios y actualizaciones del sistema. Además se debe asignar una persona encargada para que lleve el control y a la dicha bitácora.

11. Existen varios campos de la Orden de trabajo y Solicitud de trabajo que no son validados.

SITUACION INICIAL.

Durante la revisión se pudo observar que faltan validaciones de ingreso de datos específicamente en el módulo de O/T en el menú editar en los campos UBICACIÓN del equipo a reparar, PORCENTAJE DE EJECUCIÓN de la O/T y el DESTINO de la orden de trabajo, ya que no son llenadas y aún así se permite generar, aprobar y trabajar en las O/Ts. Con lo que respecta a la S/T no se encuentra validado el campo SECCION SOLICITANTE.

También se da el caso de las Horas Hombres, ya que cualquier técnico puede ingresar desde minutos de trabajos hasta cientos y miles de horas por días. Sabemos que el día tiene 24 horas, y que generalmente ninguna persona puede trabajar más de 12 diariamente peor aún si se trata de esfuerzo físico, por dicha razón no se considera que este campo pueda registrar cualquier valor de horas.

Así mismo las fechas de programación de la O/T puede ser manipulada a conveniencia por ejemplo la O/T se programa para fechas futuras, pero esta permite que se programe para fechas pasadas; este tipo de fallas afectan totalmente la confiabilidad de los datos e información registrada.

EFECTO

Este tipo de errores puede causar:

- Que en Futuras auditorías se sancione y/o se determine que el sistema no posee medidas de seguridad sólida y controles que garanticen la integridad de información. Esta falta de validación demuestra que los datos no son

reales o pueden ser cambiados ya sea por error, desconocimiento o de mala intención y por ende esto causará diferencia significativas en los resultados del sistema.

- Que el sistema no pueda poseer información íntegra y disponible para uso de informes y tomas de decisiones.
- Afectar directamente la confiabilidad y la veracidad de la información expresada en los informes generados por el sistema o por los usuarios.

RECOMENDACIÓN

Recomendamos que el área de administración de este sistema contacte a los proveedores y revise las validaciones de ingreso de datos de estas aplicaciones y si es posible solicitar la ayuda de ciertos usuarios para revisar problemas puntuales y luego ser estudiadas y mejoradas, a fin de prevenir futuros inconvenientes.

12. No existe un plan de contingencia que delinee las acciones a ejecutar ante fallas en el sistema.

SITUACION ACTUAL

Durante la revisión pudimos observar que el departamento de administración del SMAC no cuenta con un procedimiento establecido y documentado para resolver fallas.

EFECTOS.

Esta situación puede conducir a Problemas tales como:

- Demora o redundancia de pasos para revisar, reparar o solicitar mantenimiento y/o arreglos de fallas. Esto acarreará mayor tiempo para solucionar problemas.
- Así mismo, entre mayor tiempo demore la búsqueda y ejecución de soluciones para reparar fallos del sistema, mayor será la paralización del proceso de registro de información de ingreso, aprobación y ejecución de trabajos mediante las Solicitudes y órdenes de trabajo.
- Dependencia total de la persona que administra el sistema; es decir que en el caso que esta persona se ausente se presentarán una serie de problemas ya que nadie más sabrá o podrá tomar acciones para solucionar fallos del sistema.

RECOMENDACIONES

Elaborar un manual donde consten las acciones principales para poder iniciar el proceso de resolución de fallos; en el caso de este sistema que es comprado se deberá registrar los nombres de las personas que generalmente contactan para estos acontecimientos, así mismo la dirección de las oficinas y las domiciliarias si es posibles, los números de teléfono y celular de Cada persona y el correo electrónico.

También deben registrarse los pasos para revisar controles generales que descarten o asegure que es un problema serio que necesita o no asistencia del proveedor.

Evaluación de Controles y seguridades del Sistema de Mantenimiento asistido por computadora de una empresa del sector Naviero.

13. El servidor de aplicaciones se encuentra en un lugar de fácil acceso a las personas. (Sabotajes, travesuras, daños, errores).

SITUACIÓN ACTUAL

Durante la revisión realizada pudimos observar que el lugar donde se encuentra el Servidor de Aplicaciones es de fácil acceso a las personas; cualquiera que desee puede tener contacto a poca distancia.

EFECTOS

Esta situación permite:

- Que cualquier persona que tenga grandes conocimiento de Informática pueda acceder al sistema Principal (servidor) para cometer un sabotaje, una travesura, un error y por ende la pérdida parcial o total de la información, del computador y del servidor.
- Se de el caso que alguien vierta sin intención un vaso o envase de algún liquido que origine un daño total del equipo de computo.
- Se dé el caso en que alguien tropiece o resbale y colapse con el servidor.
- Así mismo estas situaciones afectarían totalmente el desenvolvimiento y ejecución del registro de mantenimiento de las Solicitudes y ordenes de trabajo.

RECOMENDACIONES

Es Importante que todo servidor, de datos o aplicaciones esté debidamente resguardado en un lugar seguro y restringido, ubicado de tal manera que no exista la posibilidad de accidentes personales contra el computador ni manipulación del equipo por cualquier persona. Esto ayudará a resguardar de manera total e íntegra las acciones y aplicaciones para que nadie tenga acceso a modificaciones y pueda colocar algún aplicativo o sistemas que realicen actividades ilícitas tales como el sabotaje, robos o desviación de información para la competencia.

BIBLIOGRAFIA

Libros

1. Comité Directivo de COBIT y El IT Governance Institute traducido por Gustavo A. Solís Montes, COBIT- Objetivos de Control, Tercera Edición, Julio 2000.

2. Echenique José Antonio, Auditoría en Informática, Edit Mac Graw Hill.

3. Gordon B. Davis,CPA, PHD, La Auditoría y el procesamiento electrónico de Información, Instituto Mexicano de Contadores Públicos, A.C.1972.

4. Information Systems Audit. And control Foundation y COBIT- Directrices de Auditoría, Comité Directivo de COBIT, abril 1998.

5. Pinilla Forero José Dagoberto, Auditoría Informática Aplicaciones en Producción, Ediciones ECOE 1997.

Publicaciones

1. ISACA- Information Systems audit. And Control Association,COBIT 3rd Edition Control Objectives, IT Governance Institute, 2000.

2. ISACA-Information Systems Audit and Control Association, Standards For Information Systems Is Auditing,2000 2001 Standards Board.

3. Auditing Guideline Application Systems Review, Document # 060.020.020,ISACA-Information Systems Audit and Control Association,2000 2001 Standards Board.

Web site

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo4.html

Última visita 13 de Junio del 2004

http://www.monografías.com/trabajos12/fichagr/fichagr.shtml

Última visita 16 de junio del 2004

http://www.google.com.ec/search?q=CONTROLES+FISICOS+Y+LOGICOS&hl=es&lr=&ie=UTF-8&start=10&sa=N

Última visita 14 de julio 2004

http://www.rediris.es/cert/doc/unixsec/node31.html

Última visita 22 de agosto del 2004

http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml

Última visita 24 de Agosto del 2004

http://www.fisc.utp.ac.pa/unidades/auditoría/glosario/glosario_2.htm

Última visita 12 de octubre del 2004

www.gestiopolis.com/canales2/generncia/1/sisinfoej.htm

Última visita 12 de octubre del 2004

www.gratisweb.com/auditoriainformatica/doc-seg-inf-1.htm

Última visita 12 de octubre del 2004

http://www.monografías.com/trabajos16/auditoria-de-informacion/auditoria-de-informacion.shtml

Última visita 12 de octubre del 2004

http://www.aceproject.org/main/espanol/et/ete08.htm

Última visita 20 de Octubre noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo5.html

Última visita 03 de noviembre del 2004

http://www.monografías.com/trabajos/seguinfo.shtml

Última visita 06 noviembre del 2004

http://alarcos.inf-cr.uclm.es/doc/adbd/abd%20tema3.pdf

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo6.html

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo8-3.html

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo8-4.html

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo8-5.html

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo8-6.html

Última visita 16 de noviembre del 2004

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo8-7.html

Última visita 16 de noviembre del 2004

http://www.mcyt.es/asp/ministerio_informa/discursos/Certificacion_seguridad_informacion/05_AENOR_Antonio_Carretero.pdf

Última visita 16 de noviembre del 2004

http://www.iit.upco.es/palacios/seguridad/cap04.pdf

Última visita 18 de noviembre del 2004

http://www.cccure.org/Documents/DonaldGlass/2_AccessControlSystems.pdf

Última visita 19 de noviembre del 2004

http://aabbccddee.galeon.com/winpy.htm

Última visita 15 de diciembre del 2004

http://www.monografías.com/trabajos3/concepaudit/concepaudit.shtml

Última visita 28 de Diciembre del 2004

http://www.gestiopolis.com/canales2/gerencia/1/sisinfoej.htm

Última visita 05 de enero del 2005

http://www.google.com.ec/search?q=CONTROLES+FISICOS+Y+LOGICOS&hl=es&lr=&ie=UTF-8&start=10&sa=N

Última visita 08 de enero del 2005

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo3.html

Última visita 29 de enero del 2005

http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/lecciones/Capitulo7.html

Última visita 19 de marzo del 2005