UNIVERSIDAD DON VASCO, A.C.

INCORPORACIÓN No. 8727-48 A LA

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA DE INFORMÁTICA

Auditoría de la Seguridad Informática del departamento de Control de Gestión e Informática de la S.R.G.H.B.S. de C.F.E.

Tesis

Que para obtener el título de:

Licenciada en Informática

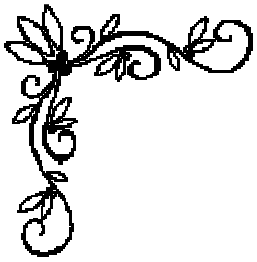
Presenta:

NORA LILIA SOLORIO NAVA

Asesor

I.S.C. Marta Catalina Núñez Escamilla

Uruapan, Michoacán. OCTUBRE de 2008



AGRADECIMIENTOS

A Dios por darme nuevamente la oportunidad de vivir y estar conmigo en cada instante. Por darme su amor, fortaleza, sabiduría, paciencia y a mis padres.

A mis Padres, por darme la vida, por haberme apoyado en todo momento, por sus consejos, sus valores, por enseñarme a ser una triunfadora, por los ejemplos de perseverancia y constancia que me ha infundado siempre, por el valor mostrado para salir adelante. Pero más que nada, por su amor.

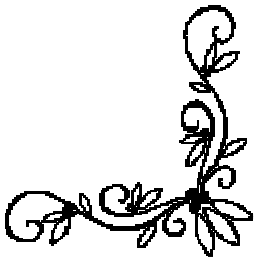
A mis abuelitos, por la motivación constante que me ha permitido ser una persona de bien.

A toda mi familia, que siempre me han dado su apoyo incondicionalmente.

A mi asesora, por su apoyo en mi formación profesional.

A mis profesores, que me ayudaron con la aportación de sus conocimientos.

Al Ing. José Antonio Portales Trujillo, Ing. Alberto Palomino Vázquez por su consentimiento para la realización de mi tesis y su apoyo.



ÍNDICE GENERAL

Capítulo IV.
Auditoría Informática

Capítulo V.
Auditoría de la Seguridad

Capítulo VI.
Caso Práctico

INTRODUCCIÓN

En la era digital en la que hoy vivimos y trabajamos, las tecnologías de la información y de las comunicaciones (TIC) resultan sumamente útiles en las tareas cotidianas de las personas y las empresas. Al mismo tiempo, son cada vez más las personas y las empresas que corren el riesgo de sufrir violaciones de la seguridad de su información. Esto se debe a los puntos vulnerables de estas tecnologías, tanto de las que ya existen como de las emergentes, así como a la convergencia, el uso cada vez más generalizado de conexiones permanentes y el crecimiento constante y exponencial del número de usuarios. Estas violaciones de la seguridad pueden ser de carácter informático, por ejemplo, causadas por virus informáticos, o bien pueden tener una motivación social, por ejemplo, debido al robo de equipos. En una época que depende tanto de la información digital los peligros van en aumento. Sin embargo, un gran número de personas desconoce los riesgos a los que está expuesta su seguridad.

Debido al avance y la proliferación de estos peligros, las actuales soluciones para la seguridad de la información pronto se quedarán obsoletas. La situación de la seguridad sufre constantes cambios. La mayoría de los analistas señalan que el eslabón más débil de todo sistema de seguridad de la información es el elemento humano. En este caso, únicamente un gran cambio en la percepción y la cultura organizativa de los usuarios podrá reducir realmente el número de violaciones de la seguridad de la información.

La institución que nos ocupa es la "Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago" de la Comisión Federal de Electricidad en el área del departamento de Informática. Es una empresa de clase mundial que participa competitivamente en la satisfacción de la demanda de energía eléctrica nacional e internacional, que optimiza el uso de su infraestructura física y comercial, a la vanguardia de la tecnología, rentable, con imagen de excelencia, industria limpia y recursos humanos altamente calificados.

Por lo anterior el motivo del presente trabajo es desarrollar un estudio completo del estado actual y futuro posible de Seguridad Informática, que continuamente se pone sobre el tapete y en realidad se conoce muy poco; se suele manejar con el amarillismo de los medios no especializados, dificultando esto su accionar y colocando en tela de juicio el arduo trabajo de los especialistas. También intentaré brindar un completo plan de estrategias y metodologías, que si bien no brindan la solución total, podrá cubrir parte del "agujero" que hoy se presenta al hablar de Seguridad Informática.

La mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni en el capital humano ni económico necesario para prevenir, principalmente, el daño y/o la pérdida de la información que, en última instancia es el Conocimiento con que se cuenta.

Conocer los riesgos a los que los sistemas y las redes de información están expuestos y los medios de protección de que se dispone para defenderlos constituye el primer paso en la protección de los mismos.

Paradójicamente, en el mundo informático, existe una demanda constante y muy importante que está esperando a que alguien los atienda.

El objetivo general consiste en la realización de una Auditoría Informática en la Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago de la C.F.E. con el fin de relevar las vulnerabilidades existentes en lo relativo a controles de seguridad, como medio para el desarrollo de una propuesta para el departamento de informática, de acuerdo a las Políticas de Seguridad y Protección Informática de la organización.

Para poder cumplir el objetivo principal es importante cumplir con otros objetivos particulares:

- Conocer el entorno y el ámbito de trabajo del departamento de informática de la C.F.E.
- Conocer cuales son los problemas a los que se ha enfrentado el departamento de informática de la C.F.E. en relación a la seguridad de su información.
- El análisis de la eficiencia de los Sistemas Informáticos.
- Sensibilizar a los profesionales del área de informática hacia la necesidad de proteger uno de los activos importantes en las organizaciones, cómo lo es la información.

JUSTIFICACIÓN

La elaboración de este trabajo tiene la finalidad de obtener el título correspondiente de Licenciado en Informática.

Considerando que la elaboración de una tesis ayuda a mejorar y a aprender nuevas formas de investigación, amplía los conocimientos y además permite la complementación de la investigación utilizando la propia experiencia y criterio.

La decisión de realizar una tesis sobre una Auditoría de la Seguridad Informática, surge de la inquietud por investigar qué aspectos de la seguridad pueden afectar a una organización como C.F.E. y en este caso a el departamento de Control de Gestión e Informática, que está en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Y así cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se tomen las acciones correctivas rápidamente para así reducir los riesgos. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la compañía como lo son la contabilidad y la nómina.

A lo largo de este trabajo se va a intentar hacer un repaso de los puntos habituales referentes a seguridad (problemas, ataques, defensas...), aplicando el estudio a entornos con requisitos de seguridad medios (universidades, empresas,

proveedores de acceso a Internet...); de esta forma se ofrecerá una perspectiva general de la seguridad, el funcionamiento de sus mecanismos, y su correcta utilización.

También se hablará, en menor medida, sobre temas menos técnicos pero que también afectan directamente a la seguridad informática, como puedan ser el problema del personal.

HIPÓTESIS

"Si la CFE utilizará sus recursos para tomar medidas de seguridad informática, no tendría amenazas dentro de su organización".

Para lograr los objetivos planteados con anterioridad, es necesario formularnos las siguientes preguntas para que nos sirvan de guía en el desarrollo de la investigación.

1. ¿Existe un control de la Seguridad Informática dentro de la empresa?
2. ¿La seguridad informática facilita el desempeño de una organización como la CFE?
3. ¿El Departamento Informático será vulnerable a las fugas de información por parte de su personal, intrusos, extorsiones, espionaje industrial, desastres naturales, accidentes, violación de la seguridad, etc.?
4. La Auditoría de Seguridad Informática, ¿ayudará a revisar la situación actual y la eficiencia o deficiencia de la seguridad?
5. ¿De qué manera se puede solucionar la falta de seguridad informática?

En nuestra investigación se emplean varias herramientas que son útiles para poder dar respuesta a los planteamientos y poder obtener conclusiones que nos sirvan para proponer una solución que ayude a mejorar la seguridad del área de informática, estas herramientas son:

- Investigación Documental.
- Observación Participativa y Experimental.

- Entrevistas Abiertas.
- Aplicación Cuestionarios.

Cada una de estas herramientas nos proporciona información de distintos aspectos del departamento analizado, y nos permite tener un panorama bastante amplio de la situación por la que atraviesa.

Para una mejor comprensión el desarrollo de la investigación se ha dividido en seis partes de las cuales presentamos una breve descripción a continuación.

Capítulo I.

En este capítulo se da una introducción al lector de conceptos como informática, las generaciones de las computadoras, lo que es un riesgo y los tipos de riesgos informáticos.

Capítulo II.

Aquí se analizan conceptos como administración, centro de cómputo, cuáles son los elementos que integran los recursos informáticos, cuál es el producto principal dentro del servicio informático y qué responsabilidades se deben asignar en un centro de cómputo.

Capítulo III.

En este capítulo se habla de la seguridad, de cómo ha ido evolucionando el término, cuál es su objetivo, analizaremos el concepto de la seguridad informática, sus objetivos, de quién debemos protegernos y sobre todo qué debemos proteger.

Capítulo IV.

Aquí se muestran conceptos cómo auditoría, auditoría informática, cuáles son las funciones de un auditor en el departamento de informática, cuál metodología se debe seguir para el trabajo de auditoría informática el cual

comprende siete etapas, cuáles son las herramientas y técnicas para la auditoría informática.

Capítulo V.

Aquí hablaremos de los objetivos de la auditoría de seguridad informática y cuáles son las áreas que comprende la auditoría de seguridad informática y que aspectos se ocupa de cubrir cada una.

Capítulo VI.

En este capítulo se lleva acabo el desarrollo del caso práctico del trabajo con el análisis de la seguridad informática del departamento de informática, exponiendo el marco de referencia de la institución objeto de estudio, presentando sus antecedentes, la evolución, la metodología que se empleo en el estudio, así como los resultados que se obtuvieron y la interpretación de estos para poder hacer la descripción de lo encontrado en el análisis y el porque de éstos.

CAPÍTULO I.
INFORMÁTICA

El objetivo principal de este primer capítulo consiste en ofrecer una visión general del significado de la palabra informática la cual no es lo mismo que computación, además de conocer de forma breve las seis generaciones de las computadoras hasta nuestros días.

Así mismo, los riesgos informáticos que generan incertidumbre ante las diversas amenazas de los bienes o servicios.

Esta primera aproximación nos permite situar cada uno de los temas siguientes en relación con los demás, y dentro del contexto de la informática.

1.1 ¿Qué es la informática?

En 1966, la Academia Francesa reconoció este concepto y lo definió del modo siguiente: "Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social". (ECHENIQUE, 1992:3)

En 1975, IBI (Oficina Intergubernamental de Informática formuló la siguiente definición: "Aplicación racional, sistemática de la información para el desarrollo económico, social y político". (ECHENIQUE, 1992:3)

En 1977, con la intención de actualizar y afinar el concepto, la Academia Mexicana de Informática propuso la siguiente definición: "Ciencia de los sistemas inteligentes de información". (ECHENIQUE, 1992:3)

Entonces como podemos ver la informática es la ciencia que se encarga del tratamiento automático de la información. Este tratamiento automático es el que

ha propiciado y facilitado la manipulación de grandes volúmenes de datos y la ejecución rápida de cálculos complejos.

1.2 Antecedentes Históricos de la Informática

Desde la antigüedad el hombre ha tenido la necesidad de la procesar información, y en un principio lo hizo de manera muy rudimentaria. La falta de elementos que le permitieran realizar los procedimientos para hacer cálculos, lo obligaban para operar mentalmente en la mayoría de los casos. Cuando las sumas eran sencillas, el proceso de contar lo efectuaban con ayuda de los dedos. El hombre, estaba limitado en un principio al número de sus dedos. Superó esto cuando fue capaz de usar otros medios, como cuentas, granos u objetos similares. Considerando que las computadoras solo son artefactos que pueden realizar cálculos a gran velocidad todos los dispositivos de cálculo son sus antecesores.

Según Vázquez algunos de los antecesores de la computadora son:

El Ábaco fue quizás fue el primer dispositivo mecánico de contabilidad que existió. Se ha calculado que tuvo su origen hace al menos 5000 años, y su efectividad ha soportado la prueba del tiempo y todavía se utiliza.

El inventor y pintor Leonardo da Vinci (1452-1519) trazó las ideas para una sumadora mecánica. Siglo y medio después, el filósofo y matemático francés Blaise Pascal (1623-1662) por fin inventó y construyó la primera sumadora mecánica en el año de 1642, se le llamó Pascalina y funcionaba con una maquinaria a base de engranes y ruedas. A pesar de ser un gran logro, la Pascalina resultó un desconsolador fallo, ya que resultaba más costosa que la labor humana para los cálculos matemáticos.

El telar de Jacquard, inventado en 1804 por el francés Joseph-Marie Jacquard (1753-1834), usado todavía en la actualidad, se controla por medio de

tarjetas perforadas. Se considera como el primer uso importante que se le dio a la automatización binaria.

Hacia la primera mitad de los 40's surgen las primeras computadoras, la idea original nace del genio Charles Babbage (1793-1871) catedrático de Cambrige, a quien se le considera "El padre de la computación", quién construyó su "Máquina de diferencias" hacia 1822 capaz de calcular tablas matemáticas. En 1834, mientras trabajaba en los avances de la máquina de diferencias, Babbage concibió la idea de una "máquina analítica" la cual podría sumar, substraer, multiplicar y dividir en secuencia automática; en esencia, ésta era una computadora de miles de engranes y mecanismos que cubrirían el área de un campo de fútbol.

En 1944, fue puesto en funcionamiento la primer computadora de la historia, con la ayuda económica y técnica de la compañía IBM, lo que dio origen a la Mark I. El esquema lógico de la Mark I, así como el de las siguientes computadoras, responde plenamente al diseño de Babbage, pues cuenta con unidades de entrada y salida, unidad aritmético-lógica, memoria y unidad de control.

Las máquinas de la primera generación, usaban cuartos enteros, costosos sistemas de aire acondicionado y pesaban varias toneladas, funcionaban con bulbos al vacío, lo que ocasionaba constantes fallas y excesivo calentamiento. Un ejemplo es el ENIAC.

En la segunda generación de computadoras se usaban transistores en lugar de tubos de vació. El uso de transistores tenía muchas ventajas, eran mucho más pequeños, posibilitando la construcción de computadoras más pequeñas. Una reducción considerable en el consumo de electricidad, lo que los hacia menos costosos, y no producían tanto calor por lo que no se averiaban con tanta facilidad. A finales de esta generación surgen los lenguajes de alto nivel.

En la tercera generación de computadoras surge con el descubrimiento del primer Circuito Integrado (Chip) por el ingeniero Jack S. Kilby de Texas Instruments, como elemento electrónico principal, que ocupaban el mismo lugar que un transistor, pero en el interior de estos cabían 200 transistores colocados sobre una oblea llamada chip. La distancia entre los transistores se reduce por lo que estas computadoras eran más rápidas.

En la cuarta generación de computadoras, Intel Corporation, que era una pequeña compañía fabricante de semiconductores ubicada en Silicon Valley, presenta el primer microprocesador o Chip de 4 bits, que en un espacio de aproximadamente 4 x 5 mm contenía 2 250 transistores. Durante esta generación tanto las computadoras como su precio se reduce considerablemente, así como el consumo de energía eléctrica, aparecen lenguajes de programación y paquetes de utilidad que pueden ser adquiridos a bajo costo.

La quinta generación de computadoras se inicia con la creación de la primera supercomputadora con capacidad de proceso paralelo, aproximadamente a partir de 1985 se inician sus aportes con conceptos tales como electrónica criogénica, superconductividad, comunicaciones con fibras ópticas, uso de rayos láser, uso de redes de área local, software, inteligencia artificial, sistemas expertos, redes neuronales, telecomunicaciones, etc., y otras todavía en el campo de la experimentación. El almacenamiento de información se realiza en dispositivos magneto óptica con capacidades de decenas de Gigabytes; se establece el DVD como estándar para el almacenamiento de video y sonido.

La sexta generación de computadoras, está en marcha desde principios de los años noventas. Las computadoras de esta generación cuentan con arquitecturas combinadas Paralelo/Vectorial, con cientos de microprocesadores trabajando al mismo tiempo; las redes de área mundial (WAN) seguirán creciendo desorbitadamente utilizando medios de comunicación a través de fibras ópticas y satélites, con anchos de banda impresionantes. Las tecnologías de esta generación ya han sido desarrolladas o están en ese proceso. Algunas de ellas

son: inteligencia artificial distribuida, transistores ópticos, seguridad informática, internet2, etcétera.

(VÁZQUEZ, 1996:5)

1.3 Riesgos Informáticos

1.3.1 ¿Que es un riesgo?

"Peligro, contingencia de un daño". (PELAYO, 1991:904)

"La probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad". (PIATTINI, 2001:50)

"Es el daño potencial que puede surgir por un proceso presente o suceso futuro". (http://es.wikipedia.org/wiki/Riesgo)

"Es una medida cuantitativa de la importancia de un incidente que es mayor cuanto mayor es su impacto y probabilidad". (ACEITUNO ,2006:21)

En función de lo anterior, podemos decir que los riesgos informáticos se refieren a la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos.

Los principales riesgos informáticos son los siguientes:

Riesgos de Integridad: Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización.

Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples

momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

- ✓ Interface del usuario.
- ✓ Procesamiento.
- ✓ Procesamiento de errores.
- ✓ Interface.
- ✓ Administración de cambios.
- ✓ Información.

Riesgos de relación: Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones.

Riesgos de acceso: Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

- ✓ Procesos de negocio.
- ✓ Aplicación.
- ✓ Administración de la información.
- ✓ Entorno de procesamiento.
- ✓ Redes.
- ✓ Nivel físico.

Riesgos de utilidad: Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- ✓ Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- ✓ Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- ✓ Backups y planes de contingencia controlan desastres en el procesamiento de la información.

Riesgos en la infraestructura: Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos)* para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (*servicio al cliente, pago de cuentas, etc.)*. Estos riesgos son generalmente se consideran en el contexto de los siguientes procesos informáticos:

- ✓ Planeación organizacional.
- ✓ Definición de las aplicaciones.
- ✓ Administración de seguridad.
- ✓ Operaciones de red y computacionales.
- ✓ Administración de sistemas de bases de datos.
- ✓ Información / Negocio.

Riesgos de seguridad general: Los estándar IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- ✓ Riesgos de choque de eléctrico.
- ✓ Riesgos de incendio.
- ✓ Riesgos de niveles inadecuados de energía eléctrica.

- ✓ Riesgos de radiaciones.
- ✓ Riesgos mecánicos.

Podemos observar que la informática es una ciencia relacionada directamente con la toma de decisiones. Que nos ayudará en un futuro a tener información útil que será de ayuda para formarse una idea clara y completa de la situación con anticipación y que pueda tomar objetivamente las decisiones convenientes.

Nos damos cuenta de que las computadoras no se hicieron de la noche a la mañana, si no que fue a través de generaciones las cuales poco a poco ha dado pasó a lo que hoy conocemos como las computadoras más modernas.

En el siguiente capítulo hablaremos del tema de los centros de computó y como deberíamos administrarlo.

CAPÍTULO II.
CENTRO DE CÓMPUTO

El objetivo principal del presente capítulo es ofrecer información acerca de lo qué es administración, qué son los centros de cómputo, los elementos que lo integran también abordaremos la información como el recurso principal, los servicios y las funciones del departamento dentro de una empresa u organización, de esta forma entenderemos como se debe administrar un centro de cómputo y las actividades que deben de administrarse con el fin de hacerlas más eficientes.

2.1 Administración de centros de cómputo

¿Qué es la Administración?

"Es la disciplina que planea, coordina, organiza, dirige y controla los recursos humanos, materiales, tecnológicos y financieros de una organización mediante procedimientos, técnicas y métodos para alcanzar sus objetivos, con eficiencia." (TERRY, 1991:22) (RIOS, 1990:37) (CHIAVENATO, 1989:6)

Podemos centrarnos en decir que el objetivo de la administración es el empleo eficiente de los recursos con los que cuenta la organización para lograr los objetivos de ésta con el mínimo de recursos.

¿Qué es un centro de cómputo?

"Un centro de cómputo representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna." (HERNANDEZ, 1994:20)

Por lo tanto un centro de cómputo, es una entidad (persona, sociedad, corporación u otra organización) dentro de una empresa que comprende el conjunto de recursos informáticos (físicos, lógicos y humanos) encargados del

diseño e implementación de sistemas, así como la administración de dichos recursos.

2.1.1 Elementos que integran los recursos informáticos

Los elementos informáticos que integran los recursos informáticos son: Elemento Humano (especializado), Hardware (equipo), Software (programas), Políticas, Procedimientos y Estándares.

Elemento Humano. Es el factor más importante de cuya habilidad depende la satisfacción de las necesidades de cómputo de la empresa. Y de acuerdo con ALVARADO se identifican como:

- Área Directiva. Realiza las funciones de planeación, organización, administración del personal y control. También es el enlace de comunicación con toda la empresa.

- Área Técnica. Está integrado por expertos en informática y su principal función es proporcionar soporte técnico especializado en las actividades de cómputo. Está integrado por:

    - Analistas y Diseñadores. Su función es la de establecer un flujo de información eficiente a través de toda la empresa. Sus proyectos no siempre requieren la computadora, ya que se enfocan a cambios y mejoras de la empresa.

    - Programadores. Elaboran los programas de acuerdo a la información proporcionada por los analistas.

    - Administradores de Bases de Datos. Establecen y controlan las definiciones y estándares de datos.

- Área Producción. Se encarga de supervisar que las entregas a los usuarios se lleven a cabo conforme a las fechas establecidas de tal manera que sean oportunas, además debe verificar el correcto funcionamiento de las computadoras y la red dentro de la organización, y programar mantenimientos periódicos para asegurar el correcto funcionamiento de los equipos.

- Área Operativa. Se encarga de brindar los servicios para el procesamiento de datos y vigilar que los elementos funcionen adecuadamente. Está integrada por:

  - Operadores. Preparan y limpian todo el equipo, administran las bitácoras e informes de la computadora.

  - Capturistas. Convierten los datos de su formato original a formato accesible para la computadora.

- Área Administrativa y Auditoría. Está encargada de controlar los recursos informáticos para el abastecimiento de materiales, también tienen control sobre el mantenimiento a instalaciones. Y debe verificar constantemente su funcionamiento para detectar fallas y corregirlas, además de establecer lineamientos en cuanto a la seguridad dentro del centro de cómputo.

- Área de Métodos y Procedimientos. Tiene por objeto la elaboración de métodos y procedimientos de trabajo, para que cada una de las otras áreas de informática pueda llevar a cabo sus funciones bajo estos lineamientos.

  (ALVARADO, 1992:118-121)

Hardware (equipo). Se refiere a todos los componentes físicos (que se pueden tocar), en el caso de una computadora personal serían los discos, unidades de disco, monitor, teclado, la placa base, el microprocesador, etc.

Software (programas). Son todas las aplicaciones necesarias en la empresa para el procesamiento de datos, que incluyen:

- Software elaborado por el usuario.
- Software comercial.
- Software gratuito (compartido y regalado).

Políticas. Son las directrices básicas de la empresa.

Si bien puede parecer trivial, el primer requisito es definir políticas "cumplibles". Para ello, al definir las políticas, es necesario identificar y analizar los factores que inciden en el cumplimiento de las mismas.

La necesidad de este análisis se hace evidente si consideramos factores como, por ejemplo, el entorno rápidamente cambiante en el cual la empresa se desenvuelve obliga a revisar y actualizar constantemente las políticas.

Procedimientos. Es decir es el conjunto de pasos para lograr un objetivo.

Estándares. Es una unidad de medida adoptada y aceptada normalmente como criterio. Es un patrón para actuar de manera homogénea.

Los estándares deben ser alcanzables e incluir:

- Estándares de compra.
- Estándares de productividad.
- Estándares de comunicación.
- Estándares de trabajo.

- Estándares de programación.

2.1.2 La información como el producto principal dentro del servicio informático

La información se ha colocado como recurso principal. Los tomadores de decisiones están empezando a comprender que la información no es sólo un subproducto de la conducción de información, sino que a la vez alimenta a las empresas y puede ser el factor crítico para la determinar el éxito o el fracaso de estos.

Para maximizar la utilidad de la información una empresa la debe manejar correctamente tal como los demás recursos. Los administradores necesitan comprender que hay costos asociados con la producción, distribución, seguridad, almacenamiento y recuperación de toda la información. Aunque la información está a nuestro alrededor no es gratis, su manejo por computadora aumenta el costo de organizarla y mantenerla.

Entre las herramientas utilizadas para definir los requerimientos de información en la empresa se encuentran: muestreo, entrevistas y cuestionarios.

2.1.3 Responsabilidades del centro de cómputo

1. La operación de los sistemas de procesamiento y comunicación de información.
2. Coordinar el adecuado uso de los sistemas de información en la organización y evaluar el rendimiento de los mismos.
3. Verificar que los equipos que se utilizan y los programas estén en óptimas condiciones para su uso a través de mantenimientos.
4. Actualización y divulgación de nuevos desarrollos de software y hardware.
5. Establecimiento de procedimientos y estándares de operación para las aplicaciones de información como paqueterías y bases de datos de toda la organización para su adecuado aprovechamiento.

6. Seleccionar el personal adecuado a cada puesto de acuerdo al perfil requerido.
7. Llevar una bitácora de las actividades que se realizan y mantener un inventario actualizado de hardware y software.

Hemos analizado los conceptos de administración y centros de cómputo, así como la importancia de su existencia en las organizaciones, cómo está conformado y qué necesidades resuelven, en el siguiente capítulo hablaremos de la seguridad y la importancia que debemos darle.

CAPÍTULO III.
SEGURIDAD

La seguridad es hoy en día una parte esencial para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o mal intencionados.

Por está razón el principal objetivo de este tercer capitulo es dar a conocer un panorama de la evolución del concepto seguridad, también contiene información de qué es la seguridad informática, un análisis del objetivo de seguridad informática, las características de un sistema de seguridad, de quién debemos protegernos y sobre todo qué debemos proteger.

3.1 Evolución del término seguridad

El término seguridad tiene en sí mismo dificultad de definición, por su versatilidad y por la dinámica evolución de los sistemas sociales en el cual surge y se desarrolla. La seguridad tiene dos componentes: la identificación de amenazas, vulnerabilidades y riesgos, y lo relacionado a como prevenirlos, contenerlos y enfrentarlos.

Los primeros conceptos de seguridad se evidencian en los inicios de la escritura con los Sumerios (3000 AC). Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos: las pirámides egipcias, el palacio de Sargón, el templo de Karnak en el valle del Nilo; el dios egipcio Anubis representado con una llave en su mano, etc.

Según la Real Academia Española, el origen del término Seguridad proviene:

- (Del lat. securĭtas, -ātis).
- f. Cualidad de seguro.
- Certeza (conocimiento seguro y claro de algo).

- loc. adj. Dicho de un ramo de la Administración Pública: Cuyo fin es el de velar por la seguridad de los ciudadanos.

  (http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=seguridad)
  "Protección de los datos contra el acceso no autorizado." (FREEDMAN, 1996:518)

"La Seguridad es hoy día una profesión compleja con funciones especializadas". (www.seguridadcorporativa.org)

Podemos definir a la seguridad, como el acto de protección que articula un sistema para con su entorno.

El objetivo de la Seguridad es salvaguardar propiedades y personas contra el robo, fuego, inundación, contrarrestar huelgas y felonías, y de forma amplía todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad al personal.

Es en este proceso en donde se aprecia que no se ha añadido ningún nuevo concepto a los ya conocidos en la antigüedad; los actuales sólo son perfeccionamientos de aquellos: llaves, cerraduras, cajas fuertes, puertas blindadas, trampas, vigilancia, etc.

3.2 ¿Qué es la seguridad informática?

"Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización." (http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica)

Podemos decir que la Seguridad informática, está conformada de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.

3.3 Objetivo de seguridad informática

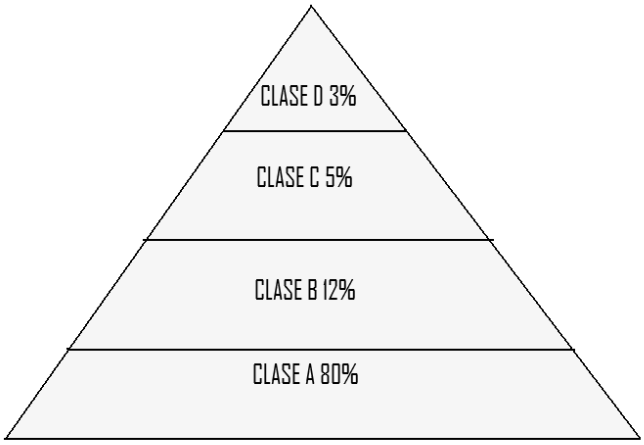
El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad y Privacidad, Control y Autenticidad de la información manejada por computadora.

3.4 ¿De quién debemos protegernos?

"Un atacante o Intruso es un individuo malintencionado, quien utiliza su conocimiento y experiencia en Informática y comunicaciones para penetrar los Sistemas de Información de las Empresas y Entidades de una forma desautorizada y utilizando herramientas especializadas, las cuales le permiten ganar acceso a información confidencial y realizar actos de sabotaje que van desde la denegación de servicios hasta el hurto y/o destrucción de información Crítica y Confidencial." (http://www.its-consultores.com/pop_hacker.htm)

En función de lo anterior, podemos decir que un Intruso o Atacante es la persona que accede sin autorización a un sistema ajeno, ya sea de forma intencional o no.

Basándonos en una entrevista de un directivo de CybSec y un ex-Hacker en el año 2001, los tipos de intrusos podríamos caracterizarlos formando una pirámide:



- Clase A: el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están "jugando" son pequeños grupitos que es juntan y dicen vamos a probar.

- Clase B: es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la víctima, testean las vulnerabilidades del mismo e ingresan.

- Clase C: en el 5%. Es gente que sabe, conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

- Clase D: el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la base hasta el último nivel se tarda de 4 a 6 años, por el nivel de conocimiento que se quiere o pretende asimilar.

(http://www.cybsec.com/)

3.5 ¿Qué debemos proteger?

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos

Por hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD-ROM, DVD, cintas, componentes de comunicación.

El software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades.

Los datos son el conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

Para cualquiera de los elementos mencionados existen multitud de amenazas y ataques que se pueden clasificar en: Ataques pasivos, Ataques activos.

Los Ataque pasivos consisten en "escuchar" la información, es decir, un usuario no autorizado dentro de la red accede a la información pero no la modifica.

En este tipo de ataque pasivo el atacante se ocupa de obtener la información que desea por medio de una examinación profunda del tráfico y sus patrones: a qué hora se encienden ciertos equipos, cuánto tráfico envían, durante cuánto tiempo, etc.

Los Ataque activos consisten en interceptar, modificar y/o denegar el acceso a la información, es decir, un usuario no autorizado dentro de la red no solo accede a la información sino que también la modifica y/o impide el acceso a esta. Y puede llegar destruirla y fabricar otra similar al original atacado.

Llegaremos a la conclusión de que el concepto de seguridad, ha evolucionado, se ha vuelto más complejo. Hemos analizado el concepto de la seguridad informática, que su principal objetivo será mantener la Integridad, Disponibilidad, Privacidad, Control y Autenticidad de la información manejada. Que un intruso es la persona que accede sin autorización a un sistema ajeno. Y que en cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

En el siguiente capítulo hablaremos de la auditoría informática, que actividades deben ser revisadas y verificadas.

CAPÍTULO IV.
AUDITORÍA INFORMÁTICA

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, los principales objetivos de este cuarto capítulo son dar a conocer que es la Auditoría, qué es una Auditoría informática, algunas funciones del auditor como lo son la recopilación, la evaluación de la estructura orgánica y recursos humanos y como se llevan a cabo las entrevistas con el personal del departamento de informática.

4.1 ¿Qué es la Auditoría?

Según ECHENIQUE y la Real Academia Española, la palabra Auditoría proviene del latín *auditorius.*
(ECHENIQUE, 1992:2)
(http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=auditoria)

"Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas." (PIATTINI, 2001:4)

Podemos decir que la Auditoría es la revisión independiente que realiza un auditor profesional aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar el resultado de dicha evaluación.

4.2 ¿Qué es la Auditoría Informática?

"Es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de

la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones." (ECHENIQUE, 1992:16)

"Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos." (PIATTINI, 2001:28)

Podemos decir que la Auditoría Informática, es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una empresa al nivel de tecnologías de la información.

4.3 Función de un auditor en el departamento de informática

Las funciones propuestas por ECHENIQUE, que un auditor debe realizar dentro del departamento de informática son:

- Verificar que todas las actividades relacionadas con la captación de datos, procedimiento y obtención de información, así como la utilización de los programas este debidamente autorizada.
- Revisión de los procesos que se llevan a cabo al procesar la información para asegurarse de que, se realicen de acuerdo a lo que ocurre realmente en la organización y se respeten los procedimientos que se han establecido.
- Revisión de las operaciones que tienen que ver con el almacenamiento de la información en archivos para verificar que no existan anomalías o malos manejos.

- Revisión de los programas empleados, verificando que cumplan con los objetivos planteados.
- Revisión de todas las modificaciones o actualizaciones que se hace al software para comprobar su adecuado funcionamiento.

(ECHENIQUE, 1992:15)

4.4 Metodología de Trabajo de Auditoría Informática

El método de trabajo del auditor pasa por las siguientes etapas:

1. Alcance y Objetivos de la Auditoría Informática.
2. Estudio inicial del entorno auditable.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Elaboración del plan y de los Programas de Trabajo.
5. Actividades propiamente dichas de la auditoría.
6. Confección y redacción del Informe Final.
7. Redacción de la Carta de Introducción o Carta de Presentación del Informe final.

(http://seguinfo.blogspot.com/search/label/auditoria)

1. Definición de Alcance y Objetivos

El alcance de la auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la auditoría, es decir cuales materias, funciones u organizaciones no van a ser auditadas.

Tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

Las personas que realizan la auditoría han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática.

(http://seguinfo.blogspot.com/search/label/auditoria)

2. Estudio Inicial

Para realizar dicho estudio ha de examinarse las funciones y actividades generales de la informática.

Para su realización el auditor debe conocer lo siguiente:

- Organización: Para el equipo auditor, el conocimiento de quién ordena, quién diseña y quién ejecuta es fundamental. Para realizar esto en auditor deberá fijarse en:

- *Organigrama:* El organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama fáctico diferente al oficial, se pondrá de manifiesto tal circunstancia.

- *Departamentos:* Se entiende como departamento a los órganos que siguen inmediatamente a la Dirección. El equipo auditor describirá brevemente las funciones de cada uno de ellos.

- *Relaciones Jerárquicas y funcionales entre órganos de la Organización:* El equipo auditor verificará si se cumplen las relaciones funcionales y Jerárquicas previstas por el organigrama, o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes.

  Las de Jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente subordinables.

- *Flujos de Información:* Los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama.

- *Número de Puestos de trabajo:* El equipo auditor comprobará que los nombres de los Puesto de los Puestos de Trabajo de la organización corresponden a las funciones reales distintas. Es frecuente que bajo nombres diferentes se realicen funciones idénticas, lo cual indica la existencia de funciones operativas redundantes.

- *Número de personas por Puesto de Trabajo:* Es un parámetro que los auditores informáticos deben considerar. La inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

✓ **Entorno Operacional**

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse.

Este conocimiento previo se logra determinando, fundamentalmente, los siguientes extremos:

a) Situación geográfica de los Sistemas: Se determinará la ubicación geográfica de los distintos Centros de Proceso de Datos en la empresa. A continuación, se verificará la existencia de responsables en cada unos de ellos, así como el uso de los mismos estándares de trabajo.

b) Arquitectura y configuración de Hardware y Software: Cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado. La configuración de los sistemas esta muy ligada a las políticas de seguridad lógica de las compañías.

   Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

c) Inventario de Hardware y Software: El auditor recabará información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a Hardware figurarán las CPUs, unidades de control local y remoto, periféricos de todo tipo, etc.

   El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico hasta los programas de utilidad adquiridos o desarrollados internamente. Suele ser habitual clasificarlos en facturables y no facturables.

d) Comunicación y Redes de Comunicación: En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones.

Igualmente, poseerán información de las Redes Locales de la Empresa.

- ✓ **Aplicaciones bases de datos y ficheros**

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

a) Volumen, antigüedad y complejidad de las Aplicaciones.

b) Metodología del Diseño: Se clasificará globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizados varias a lo largo del tiempo se pondrá de manifiesto.

c) Documentación: La existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes.

   La documentación de programas disminuye gravemente el mantenimiento de los mismos.

d) Cantidad y complejidad de Bases de Datos y Ficheros: El auditor recabará información de tamaño y características de las Bases de Datos, clasificándolas en relación y jerarquías. Hallará un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los ficheros, así como la frecuencia de actualizaciones de los mismos.

   Estos datos proporcionan una visión aceptable de las características de la carga informática.

(http://seguinfo.blogspot.com/search/label/auditoria)

3. Determinación de recursos de la auditoría Informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

- ✓ **Recursos materiales**

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente.

Los recursos materiales del auditor son de dos tipos:

a) Recursos materiales Software

- *Programas propios de la auditoria:* Son muy potentes y Flexibles. Habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

- *Monitores:* Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

b) Recursos materiales Hardware

- Los recursos hardware que el auditor necesita son proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las Computadoras del auditado.

- Para lo cuál habrá de convenir, tiempo de maquina, espacio de disco, impresoras ocupadas, etc.

- ✓ **Recursos Humanos**

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable.

Es igualmente reseñable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

Perfiles Porfesionales de los auditores informáticos

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos.

	Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

(http://seguinfo.blogspot.com/search/label/auditoria)

4. Elaboración del Plan y de los programas de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Decidido éste, se procede a la programación del mismo.

El plan se elabora teniendo en cuenta, entre otros criterios, los siguientes:

a) Si la Revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

b) Si la auditoría es global, de toda la Informática, o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

- En el plan no se consideran calendarios, porque se manejan recursos genéricos y no específicos.
- En el Plan se establecen los recursos y esfuerzos globales que van a ser necesarios.
- En el Plan se establecen las prioridades de materias auditables, de acuerdo siempre con las prioridades del cliente.
- El Plan establece disponibilidad futura de los recursos durante la revisión.

- El Plan estructura las tareas a realizar por cada integrante del grupo.
- En el Plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el Plan, se procede a la Programación de actividades. Esta ha de ser lo suficientemente como para permitir modificaciones a lo largo del proyecto.

(http://seguinfo.blogspot.com/search/label/auditoria)

5. Actividades de la Auditoría Informática

Auditoría por temas generales o por áreas específicas: La auditoría Informática general se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad.

Técnicas de Trabajo:

- Análisis de la información recabada del auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.
- Entrevistas.
- Simulación.
- Muestreos.

Herramientas:

- Cuestionario general inicial.
- Cuestionario Checklist.
- Estándares.
- Monitores.
- Simuladores (Generadores de datos).
- Paquetes de auditoría (Generadores de Programas).
- Matrices de riesgo.

(http://seguinfo.blogspot.com/search/label/auditoria)

6. Informe Final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad.

Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del informe final: El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.

Definición de objetivos y alcance de la auditoría.

Enumeración de temas considerados: Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

Cuerpo expositivo: Para cada tema, se seguirá el siguiente orden a saber:

a) Situación actual*.* Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real
b) Tendencias*.* Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c) Puntos débiles y amenazas.
d) Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
e) Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.
- La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El Informe debe consolidar los hechos que se describen en el mismo.

El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.
2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen al cambio propuesto.

4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

Flujo del hecho o debilidad:

1 – Hecho encontrado.

- ✓ Ha de ser relevante para el auditor y pera el cliente.
- ✓ Ha de ser exacto, y además convincente.
- ✓ No deben existir hechos repetidos.

2 – Consecuencias del hecho: Las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

3 – Repercusión del hecho: Se redactará las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la empresa.

4 – Conclusión del hecho: No deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

5 – Recomendación del auditor informático:

- ✓ Deberá entenderse por sí sola, por simple lectura.
- ✓ Deberá estar suficientemente soportada en el propio texto.
- ✓ Deberá ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación.

- ✓ La recomendación se redactará de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

7. Carta de introducción o presentación del informe final:

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la empresa, o a la persona concreta que encargo o contrato la auditoría.

Así como pueden existir tantas copias del informe Final como solicite el cliente, la auditoría no hará copias de la citada carta de Introducción.

La carta de introducción poseerá los siguientes atributos:

- ✓ Tendrá como máximo 4 folios.
- ✓ Incluirá fecha, naturaleza, objetivos y alcance.
- ✓ Cuantificará la importancia de las áreas analizadas.
- ✓ Proporcionará una conclusión general, concretando las áreas de gran debilidad.
- ✓ Presentará las debilidades en orden de importancia y gravedad.
- ✓ En la carta de Introducción no se escribirán nunca recomendaciones.

(http://seguinfo.blogspot.com/search/label/auditoria)

4.5 Herramientas y Técnicas para la Auditoría Informática

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la cumplimentación de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Cuestionarios. Son una herramienta útil para recabar información que podemos analizar para evaluar a la gente que está involucrada con el sistema que se estudia en cuanto a lo que piensa, en cómo actúa, cuáles son sus preferencias, qué opinión tiene acerca del sistema en el que se desenvuelve.

Es importante tomar en cuenta al realizar un cuestionario, que la mayoría de la veces, no podemos guiar a las personas que los responden, y por tal motivo debemos hacer las preguntas en la forma más clara posible, que al leerla, la persona que la responda tenga realmente idea de lo que se le está preguntando, de otra manera las respuestas pueden ser confusas, o no tener relación con lo que se preguntaba.

Es conveniente utilizar preguntas abiertas cuando lo que se quiere obtener opiniones del personal acerca de un tema, su aceptación o rechazo, o determinadas cuestiones de interés para el analista, se debe tener cuidado al formular las preguntas para que cuando sean respondidas, no se amplíen demasiado y el análisis de las respuestas no nos conduzca a nada, por lo anterior se debe tratar de orientar a quien nos responde hacia un tema específico, para que nos de su opinión y sea más fácil la interpretación de las respuestas.

Las preguntas cerradas son utilizadas con frecuencia cuando conocemos las posibles respuestas que se nos pueden dar a determinadas preguntas y cuando no buscamos establecer la opinión de quien responde y nos enfocamos más a situaciones reales que ocurren en el sistema, este tipo de cuestionarios limita la respuesta que da quien responde por lo que su análisis resulta sumamente sencillo.

Sin embrago, en ocasiones resulta mejor la combinación de preguntas cerradas y abiertas en los cuestionarios para obtener una información más completa.

KENDALL propone algunas alternativas que se pueden utilizar al aplicar un cuestionario, las cuales son:

1. Reunir a todas las personas en un solo sitio.

2. Entregar personalmente los cuestionarios en blanco y recogerlos una vez que se encuentren completos.

3. Permitir a quienes contestan el cuestionario que durante las horas de trabajo lo respondan por su cuenta y posteriormente lo depositen en un buzón central.

4. Enviar por correo el cuestionario a aquellos empleados de sucursales remotas, estableciendo una fecha límite, proporcionando instrucciones y el reembolso postal.

Cabe aclarar, que esta primera fase puede omitirse cuando los auditores hayan adquirido por otro medios la información que aquellos pre impresos hubieran proporcionado.

(KENDALL, 1991:203)

Entrevistas. La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas

escritas a cuestionarios. Consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente.

Según KENDALL, podemos realizar una entrevista satisfactoriamente llevando a cabo cinco pasos.

1. Lectura de antecedentes. Es conveniente buscar información acerca de los antecedentes de aquellas personas que vamos a entrevistar, así como la propia organización, para tener una idea de la cultura organizacional que tiene cada entrevistado y en general dentro de la empresa, y de esta forma poder elaborar el cuestionario adecuándolo a las características de las personas para que sea muy claro y fácil de comprender.

2. Establecimiento de los objetivos de la entrevista. Es importante definir claramente lo que se pretende conseguir con la entrevista, para poder orientar los esfuerzos de la misma y no perder el sentido que se le debe dar, al plantear los objetivos de la entrevista deberemos formular las preguntas acordes a éstos.

3. Selección de los entrevistados. Cuando se determina a qué personas se entrevistará se debe tomar en cuenta que sean seleccionadas de puntos estratégicos dentro del sistema que se analiza, de tal forma que se descubran las principales áreas, y se obtenga información que represente cada componente del sistema.

4. Preparación del entrevistado. Cuando se vaya a realizar la entrevista será conveniente comunicárselo a la persona con tiempo suficiente para que ésta se pueda organizar y aparte un tiempo para dedicarlo a la entrevista, y que no sea interrumpida por sus actividades, es importante tener en cuenta que la entrevista debe fluctuar entre los 45 minutos y una hora, para no cansar al entrevistado

5. Selección del tipo y estructura de las preguntas. Por otro lado se deben decidir que tipo de preguntas se van ha utilizar, ya sea preguntas abiertas o preguntas cerradas, también se debe elegir el tipo de estructura de las entrevistas entre tres tipos de estructura como lo son la pirámide, embudo o diamante.

(KENDALL, 1991:145-147)

Observación. Mediante la observación de las actividades y de las tareas que se llevan a cabo en un departamento se pueden evaluar qué tanto se apegan a los métodos, normas y procedimientos establecidos y qué tanto se observan las políticas y los objetivos al realizar las funciones dentro de un área o departamento.

Para la realización de la observación son útiles unas técnicas propuestas por KENDALL, llamadas muestreo por intervalos y muestreo por eventos.

Muestreo por intervalos. Es un método en donde las observaciones se realizan por intervalos de tiempo en distintas ocasiones elegidas al azar, de esta manera se obtiene una muestra de información obtenida mediante la observación, pero se pierden eventos que quizá requieren de un tiempo mayor al intervalo fijado para las observaciones, además se omiten situaciones que pueden ocurrir cuando no estamos observando, lo que ocasiona información incompleta.

Muestreo por eventos. Primero se definen aquellos eventos que se quieren observar sin importar el tiempo y se observan cuando éstos se llevan a cabo, con el inconveniente de no obtener una muestra representativa de observaciones con un tiempo similar, sin embargo dependiendo de lo que el analista requiere observar se pueden combinar ambos métodos para obtener mejores resultados.

(KENDALL, 1991:221)

Revisión de documentos. Esta técnica es muy útil cuando se busca obtener información acerca del cómo se deben llevar a cabo las actividades del departamento, las políticas y normas bajo las cuales el personal de un área debe conducirse, o para comprender mejor la forma en cómo funciona un determinado sistema, esta herramienta de análisis se aplica en todo tipo de documentación que posea la empresa o el departamento y que nos pueda proporcionar información que nos sirva para el análisis, como en manuales de políticas y procedimientos, folletos, guías, instructivos, manuales de usuarios de algún sistema, y en general cualquier documento que hable de la estructura del departamento, sus funciones, puestos, objetivos, entre otros.

La principal conclusión a la que hemos podido llegar, es que toda empresa, pública o privada, que posea Sistemas de Información, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. En cuanto al trabajo de la auditoría en sí, podemos remarcar que se precisa de gran conocimiento de Informática, seriedad, capacidad, minuciosidad y responsabilidad. En el siguiente capítulo hablaremos de la Auditoría de la Seguridad, como esta fundamentada.

CAPÍTULO V.

AUDITORÍA DE SEGURIDAD INFORMÁTICA

En este capitulo hablaremos de la Auditoría de Seguridad Informática, actualmente esta necesidad se está abriendo a las PYMEs (Pequeña y Mediana Empresa), de forma que tanto sus datos como el buen rendimiento de sus máquinas es vital para un correcto funcionamiento de la empresa. Tanto es así, que un solo día con los sistemas informáticos dañados o inactivos podría hacer que los trabajadores no pudieran desempeñar su labor o perder el trabajo de meses. Existen otros riesgos, tales como el uso de sus recursos por parte de piratas informáticos con fines maliciosos, suplantación de identidad y diversos perjuicios graves. Poner los servicios de la empresa de la forma más segura y rentable posible, se puede conseguir mediante una Auditoría de Seguridad Informática.

5.1 Objetivos de la Auditoría de Seguridad Informática

- Conocer todos los puntos vulnerables de su empresa frente a ataques externos.
- Evaluar minuciosamente la seguridad perimetral de su red y/o de sus servidores.
- Disponer de un informe totalmente detallado sobre sus vulnerabilidades y las distintas formas en que pueden ser solucionadas.
- Actualizar todos sus servicios y aplicaciones críticas.
- Para conseguir evaluar de forma eficiente cuáles son los fallos en su empresa se hará una amplia lista de pruebas y el testeo de las vulnerabilidades conocidas de todos los hosts y redes de su empresa. De esta forma cuando se produzca un ataque real contra su empresa, ya habrá sido simulado anteriormente ese ataque y habrán sido corregidos los posibles puntos vulnerables.

(PIATTINI, 2001:389-421)

5.2 Áreas de la Auditoría de Seguridad Informática

Según PIATTINI, las áreas que puede cubrir la Auditoría de la Seguridad son: Seguridad Física, Seguridad Lógica, Seguridad en el Personal, Seguridad en el Desarrollo de Aplicaciones, Seguridad en la Producción, Seguridad de los Datos, Seguridad en Comunicaciones y Redes, y Planes de Contingencia y Continuidad.

5.2.1 Seguridad Física

La Seguridad Física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

La Seguridad Física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. En este caso se contemplan situaciones como incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

En este tipo de auditorias se controlan, por ejemplo: control de accesos, identificación, instalaciones, Datacenters, servidores, medios y procesos de almacenamiento, etc.

Desde la perspectiva de las protecciones físicas:

- Ubicación de los servidores o cualquier elemento a proteger (portátiles, terminales en zonas de paso, etc.).
- Estructura, diseño, construcción y distribución de los edificios.
- Riesgos a los que están expuestos, tanto por agentes externos, causales como por accesos físicos no controlados.
- Controles preventivos.
- Control del acceso.
- Protección de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte.

Nota: Todos los puntos anteriores pueden estar cubiertos por seguros. (PIATTINI, 2001:389-421)

5.2.2 Seguridad Lógica

La Seguridad Lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

La Auditoria de Seguridad Lógica cubre los siguientes aspectos: arquitecturas, servidores (Windows, Unix y Linux), Políticas de filtrado del Firewall, configuración de electrónica y tráfico LAN/WAN. En el caso de auditorias de seguridad lógica se diferencian dos escenarios:

a) Auditoria de penetración externa, es decir se auditan los sistemas de forma que estén protegidos frente a ataques desde fuera de la organización. Para ello se utilizan herramientas comerciales y propias que permiten detectar las vulnerabilidades del sistema.
b) Auditoria de penetración interna, en este caso consiste en el mismo estudio que la penetración externa, pero haciendo la suposición que el ataque procederá desde el interior de la empresa, es decir, por usuarios del sistema.

Para llevar a cabo este tipo de auditorias es necesario contar con la tecnología apropiada que permita verificar el estado de la infraestructura de seguridad.

(PIATTINI, 2001:389-421)

5.2.3 Seguridad en el Personal

El factor humano es el principal a considerar, salvo en algunas situaciones de protección física muy automatizados, ya que es muy crítico: si las personas no

quieren colaborar de poco sirven los medios y dispositivos aunque sean caros y sofisticados.

Es necesaria una separación de funciones: es peligroso que una misma persona realice una transacción, la autorice, y revise después los resultados, porque podría planificar un fraude o encubrir cualquier anomalía, y sobre todo equivocarse y no detectarse; por ello deben intervenir personas diferentes y existir controles suficientes.

(PIATTINI, 2001:389-421)

5.2.4 Seguridad en el Desarrollo de Aplicaciones

Todos los desarrollos deben estar autorizados a distinto nivel según la importancia del desarrollo a abordar, incluso autorizados por un comité si los costos o los riesgos superan unos umbrales; la metodología seguida, ciclos de vida, gestión de proyectos, consideraciones especiales respecto a aplicaciones que traten datos clasificados o que tengan transacciones económicas o de riesgo especial, términos de los contratos y cumplimiento, selección y uso de paquetes, realización de pruebas a distintos niveles y mantenimiento posterior, así como desarrollos de usuarios finales.

El pase al entorno de explotación real debe estar controlado, no descartándose la **revisión de programas** por parte de técnicos independientes, o bien por auditores preparados, a fin de determinar la ausencia de "caballos de Troya", bombas lógicas y similares, además de la calidad.

La protección de los programas: sean propiedad de la entidad, realizados por el personal propio o contratado su desarrollo a terceros, como el uso adecuado de aquellos programas de los que se tenga licencia de uso.

(PIATTINI, 2001:389-421)

5.2.5 Seguridad en la Producción

En algunos casos también conocida como de Explotación u Operación, se ocupa de revisar todo lo que se refiere con producir resultados informáticos, listados impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

La producción, operación o explotación informática dispone de una materia prima, los datos, que sea necesario transformar, y que se sometan previamente a controles de integridad y calidad. La transformación se realiza por medio del proceso informático, el cual está gobernado por programas y obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente, al usuario.

Las entidades han de cuidar especialmente las medidas de protección en el caso de **contratación** de servicios: desde el posible marcado de datos, proceso, impresión de etiquetas, distribución, acciones comerciales, gestión de cobros, hasta el *outsourcing* más completo, sin descartar que en el contrato se prevea la revisión por auditores, internos o externos, de las instalaciones de la entidad que provee el servicio.

Otro aspecto a revisar es el control de los formularios críticos.

(PIATTINI, 2001:389-421)

5.2.6 Seguridad de los Datos

Decíamos que los datos y la información pueden llegar a constituir el activo más crítico para la entidad, hasta el punto de que en muchas multinacionales la función genérica de administración de seguridad tiene la denominación de Data Security.

Los datos, además de alfanuméricos, pueden consistir en imágenes de planos, en otros diseños u objetos, gráficos, acústicos, y otros, y estar almacenados en medios y soportes diversos.

La protección de los datos puede tener varios enfoques respecto a las características: la confidencialidad, disponibilidad e integridad.

(PIATTINI, 2001:389-421)

5.2.7 Seguridad en Comunicaciones y Redes

En las políticas de la entidad debe reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la entidad y no deben usarse para otros fines no autorizados, por seguridad y por productividad, tal vez salvo emergencias concretas si así se ha especificado.

En función de la clasificación de los datos se habrá previsto el uso del cifrado.

Los usuarios tendrán restricción de accesos según dominios, únicamente podrán cargar los programas autorizados, y sólo podrán variar las configuraciones y componentes los técnicos autorizados.

Existirán protecciones frente accesos sobre todo externos, así como frente a virus por diferentes vías de infección, incluyendo correo electrónico.

Se revisarán especialmente las redes cuando existan repercusiones económicas porque se trate de transferencia de fondos o comercio electrónico.

Este tipo de revisión se enfoca en las redes, líneas, concentradores, multiplexores, etc. Así pues, la Auditoría Informática ha de analizar situaciones y hechos algunas veces alejados entre sí, y está condicionada a la participación de la empresa telefónica que presta el soporte. Para este tipo de auditoría se requiere un equipo de especialistas y expertos en comunicaciones y redes.

El auditor informático deberá inquirir sobre los índices de utilización de las líneas contratadas, solicitar información sobre tiempos de desuso; deberá proveerse de la topología de la red de comunicaciones actualizada, ya que la desactualización de esta documentación significaría una grave debilidad. Por otro

lado, será necesario que obtenga información sobre la cantidad de líneas existentes, cómo son y donde están instaladas, sin embargo, las debilidades más frecuentes o importantes se encuentran en las disfunciones organizativas, pues la contratación e instalación de líneas va asociada a la instalación de los puestos de trabajo correspondientes (pantallas, servidores de redes locales, computadoras, impresoras, etc.).

(PIATTINI, 2001:389-421)

5.2.8 Planes de Contingencia y Continuidad

El proyecto, elaboración, puesta en vigor y mantenimiento de un plan de contingencia y continuidad o de recuperación de la actividad debe estar enmarcado en la política general de seguridad de la organización, emanada de la alta Dirección. Es una labor de significativa envergadura y complejidad que debe estar sujeta a los correspondientes requisitos de planificación previa y rigor en su desarrollo. La falta de estos requisitos puede dar lugar a elaborar un Plan que no cumpla o no satisfaga los objetivos para él establecidos y resulte ineficaz en el caso de tener que ponerlo en práctica ante una interrupción de las actividades.

Por otra parte, el alcance y complejidad del Plan, en cuanto a las acciones, funciones y recursos que debe contemplar, estará determinado por el grado en que las actividades ordinarias de la organización dependan del funcionamiento del centro de proceso de datos, y por el carácter crítico de algunas de las aplicaciones informáticas para el funcionamiento normal de la empresa.

Con respecto a los sistemas informáticos, debe darse por supuesto que, previamente, se han implantado en la Entidad las medidas de seguridad física y lógica que aseguran la integridad, fiabilidad y disponibilidad de la información, siguiendo los principios del plan de seguridad informática de la Entidad. Por otra parte, debe existir un plan de protección civil que establezca los procedimientos y medios para la evacuación del personal de los edificios.

Se trata, en primer lugar, de establecer una lista de elementos críticos (hardware, software, bases de Datos, aplicaciones, sistemas operativos, equipos, comunicaciones, periféricos, etc.) porque su carencia o mal funcionamiento afectaría en el desarrollo de las actividades en la organización.

Para ello, de cada uno de estos elementos se determina el tiempo durante el cual sería posible para la empresa asumir su falta de funcionamiento, ordenándolos de menor a mayor tiempo. De este modo, los elementos más críticos aparecerán en los primeros lugares. La elaboración de esta lista de elementos críticos requerirá la participación de los usuarios y propietarios de las aplicaciones que se considerasen críticas, además de todas las áreas del centro de proceso de datos.

Una vez realizado lo anterior, se debe determinar lo que podríamos denominar como nivel aceptable de seguridad. Se trata de encontrar un punto de equilibrio entre la seguridad que proporciona la diminución de riesgos, que de la implantación de estas medidas se puedan derivar, y el coste de implantación y mantenimiento de las técnicas y procedimientos a emplear. Por ello, es necesario tratar de cuantificar dos tipos de magnitudes:

- Por un lado, los costos de los daños que pueden ocasionar en la empresa el impacto derivado de la materialización de las amenazas.
- Por el otro, los costos de implantación y mantenimiento de las medidas apropiadas para su contención.

Para el caso de una destrucción o inhabilitación del centro de proceso de datos que impida la reanudación de las operaciones de forma inmediata, aunque sea de forma parcial o degradada, el Plan debe recoger la ubicación, características y necesidades para la utilización de un centro alternativo de respaldo (Centro Backup) hasta la reconstrucción o recuperación del centro origen.

Por último, el Plan debe adaptarse permanentemente a las circunstancias cambiantes, tanto del negocio como del entorno y de los medios tecnológicos y

humanos disponibles en cada momento, por lo que deben realizarse pruebas sistemáticas para mantenerlo eficazmente al día, revisándolo y actualizándolo con una periodicidad anual, como mínimo. Asimismo, el Plan debe contemplar la formación y entrenamiento del personal para caso de siniestros.

Por lo expuesto anteriormente, podemos establecer que el objetivo general del programa de auditoría consiste en verificar la existencia de unos planes de contingencia y de continuidad o de recuperación de la actividad ante desastres; que contemplan un conjunto de procedimientos de actuación y de recursos necesarios para la restauración progresiva de los servicios en el caso de paralización de las actividades; en los que están involucradas todas las áreas, departamentos y servicios de la Organización y que se mantienen debidamente actualizados, realizándose pruebas periódicas para comprobar su eficacia.

El logro de estos objetivos generales implica la verificación y evaluación de los siguientes aspectos del Plan:

1. Existencia y criterios de elaboración

El objetivo de este apartado es comprobar que en la Entidad realmente existe un plan de contingencia y continuidad o de reanudación de la actividad ante desastres, (en adelante Plan) formalizado por escrito y aprobado por la Dirección, que garantiza el respaldo de los recursos críticos y la recuperación de los servicios ante interrupciones imprevistas, permitiendo a la empresa dar continuidad a las operaciones ordinarias dentro de los plazos previamente establecidos.

2. Contenido y finalidad

La revisión del contenido del Plan tiene por objeto comprobar que responde al proyecto autorizado y elaborado según los criterios expuestos en el apartado anterior; y que, siguiendo las instrucciones y procedimientos indicados y utilizando los medios y recursos definidos, el equipo de recuperación podrá dar respuesta a una situación de emergencia en las actividades, garantizando la

continuidad de las mismas y la prestación de servicios a la Organización con los niveles de calidad y puntualidad previstos en el referido Plan en función del alcance o gravedad del siniestro.

3. Mantenimiento y pruebas

El objetivo de este apartado es verificar si se realizan puntualmente las labores de mantenimiento y pruebas del Plan, en consonancia con las modificaciones e innovaciones del entorno informático, de forma que dicho Plan se encuentre siempre a punto para ponerlo en marcha si fuera necesario.

(PIATTINI, 2001:389-421)

En el capítulo hemos indicado la utilidad de realizar una Auditoría de Seguridad Informática en las PYMEs. Es obvio, que para el desarrollo de las actividades de la organización el correcto funcionamiento de dicho centro es vital. Por lo tanto en el siguiente capítulo se presenta el caso práctico de una Auditoría de la Seguridad informática del Departamento Control de Gestión e Informática de la Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago C. F. E.

CAPÍTULO VI.

CASO PRÁCTICO Y PROPUESTA

En el presente capítulo abordaremos el caso en particular estudiando, para el desarrollo de este trabajo se ha aplicado la metodología, técnicas e instrumentos necesarios para una adecuada investigación, se muestran las técnicas que se emplearon en el estudio, el porqué de su uso, en el caso del cuestionario se presentan los modelos utilizados y finalmente se da una descripción de los resultados obtenidos al aplicar dichas técnicas y la interpretación de los resultados, para mostrar el panorama amplio de los problemas, el porqué de estos y en qué circunstancias se presentan.

6.1 Marco de referencia

La Institución objeto de estudio es la "Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago" de la Comisión Federal de Electricidad en el área del departamento de Control de Gestión e Informática. Dicha institución se encuentra ubicada en la calle de Bruselas s/n, esquina con Tlaxcala en la colonia La Joyita en esta cuidad de Uruapan, Michoacán.

Esta Institución surgió en el año de 1952 en que se constituyó la División Michoacán, ahora llamada División Centro Occidente, con los sistemas eléctricos que hasta la fecha existían en el estado. Anteriormente los sistemas eran administrados directamente por las oficinas centrales de la C.F.E., pero con motivo de su crecimiento, se vio la necesidad de descentralizar creando divisiones a las cuales se les dio cierta autonomía y facultades para hacer más flexible la prestación del servicio eléctrico y con funciones de generación, transmisión, transformación, distribución y comercialización.

El área que nos ocupa es el departamento de Informática de esta institución, el cual depende del departamento de Control de Gestión y funciona como un departamento de apoyo a toda la institución, en todo lo que al procesamiento electrónico de información se refiere, como ya se mencionó, dicho

departamento no es autónomo, depende del departamento de Control de Gestión, de hecho se denomina Departamento de Control de Gestión e Informática, aun cuando su ubicación física dentro de la subgerencia es distinta, informática debe reportar a Control de Gestión respecto a las actividades y funciones que realiza.

El personal del Departamento de informática

El personal que forma parte de este departamento consta de 6 personas sus nombres se omiten por cuestiones de confidencialidad y los puestos son los siguientes:

Puestos:

- Jefe del departamento Control de Gestión e Informática.
- Coordinador del departamento de Informática.
- Supervisor Regional de Sistemas y Hardware.

Funciones del Departamento de Informática

El Departamento de Informática tiene a su cargo las siguientes funciones:

a) Administración de recursos informáticos para la implementación de procesos y/o tecnologías que contribuyan a mejorar la calidad y eficiencia en las actividades.

b) Administración de los sistemas.

c) Capacitación de personal en temas informáticos.

d) Proporcionar servicios informáticos a todos los usuarios de equipo de cómputo en el ámbito de la subgerencia y centrales.

e) Mantener y administrar las redes, sistemas y equipos computacionales.

f) Mantener actualizado el inventario de equipos y software.

g) Mantenimiento preventivo y correctivo a los dispositivos y cableado de comunicaciones de la subgerencia.

h) Proporcionar mantenimiento preventivo y correctivo a los equipos de cómputo y programas de la subgerencia.

i) Adquisición e instalación de hardware y software, así como capacitación al personal para su uso.

j) Supervisar todo proyecto informático.

k) Velar por la integridad de la información almacenada en equipos computacionales.

l) Crear y administrar las bases de datos que sean relevantes para la toma de decisión y para el conocimiento de la comunidad.

m) Recopilar, actualizar y mantener datos e información estadística necesaria para la empresa, con la finalidad de que ésta sea útil en la toma de decisiones.

n) Elaborar y ejecutar los planes de contingencia necesarios en caso de pérdida de dicha información.

6.2 Metodología empleada en la investigación

Para llevar a cabo el análisis del departamento de Control de Gestión e Informática en su sistema de seguridad, se ha hecho uso de las herramientas que a continuación se muestran.

Observación Participativa:

Se utilizó esta herramienta, por la razón de que en la institución mencionada tuve la oportunidad de realizar mi servicio social precisamente en el departamento de Control de Gestión e Informática, en donde llevo a cabo el estudio, lo cual me permitió tener una convivencia con el personal del mismo, y darme cuenta de su problemática así como estar inmersa en las actividades que

el departamento desempeña y participar activamente en algunas de ellas, es por eso que en gran parte la información obtenida para el análisis del problema fue obtenida mediante la observación.

Investigación Documental:

Para obtener información sobre organigramas, misión, objetivos, políticas, puestos, funciones y actividades del personal departamento se utilizó esta herramienta, a través de la cual se recabo información de algunos documentos que se me permitió observar durante la investigación.

Cuestionarios:

El uso de esta herramienta favoreció la investigación, ya que me permitió obtener información referente al conocimiento del personal del departamento tiene acerca de la organización (objetivos, políticas, normas, etc.), además de conocer su opinión a cerca de la seguridad que se maneja en el área de informática y los planteamientos propuestos por ellos mismos y por parte de la organización para tratar de mejorarla.

Para la aplicación del cuestionario, no se realizo un muestreo debido a que el universo de investigación es de seis personas por esta razón se aplico a todo el universo.

6.3 Preguntas de investigación

1. ¿Existe un control de la Seguridad Informática dentro de la empresa?
2. ¿La seguridad informática facilita el desempeño de una organización como la CFE?
3. ¿El Departamento Informático será vulnerable a las fugas de información por parte de su personal, intrusos, extorsiones, espionaje industrial, desastres naturales, accidentes, violación de la seguridad, etc.?

4. La Auditoría de Seguridad Informática, ¿ayudará a revisar la situación actual y la eficiencia o deficiencia de la seguridad?
5. ¿De qué manera se puede solucionar la falta de seguridad informática?

6.4 Auditoría

AUDITORÍA SEGURIDAD INFORMÁTICA

La presente auditoría se realiza en el departamento de informática de la C.F.E., del 18/02/08 al 14/03/08.

1. Alcance de la Auditoría

La Auditoría Informática propuesta comprende fundamentalmente la planificación y ejecución de los siguientes aspectos:

1. EVALUACIÓN DE LA SEGURIDAD LÓGICA
1.1. Identificación de usuarios
1.2. Autenticación de usuarios
1.3. Passwords
1.4. Segregación de funciones
2. EVALUACIÓN DE LA SEGURIDAD EN LAS COMUNICACIONES
2.1. Topología de red
2.2. Comunicaciones externas
2.3. Configuración lógica de red
2.4. Mail
2.5. Antivirus
2.6. Firewall
2.7. Ataques de red
3. EVALUACIÓN DE LA SEGURIDAD DE LAS APLICACIONES
3.1. Software
3.2. Seguridad de bases de datos
3.3. Control de aplicaciones en PC´s

3.4. Control de datos en las aplicaciones
3.5. Ciclo de vida del desarrollo del software
4. EVALUACIÓN DE LA SEGURIDAD FÍSICA
4.1. Equipamiento
4.2. Control de acceso físico al centro de cómputos
4.3. Control de acceso a equipos
4.4. Dispositivos de soporte
4.5. Estructura del edificio
4.6. Cableado estructurado
5. EVALUACIÓN DE LA ADMINISTRACIÓN DEL CPD
5.1. Administración del CPD
5.2. Capacitación de usuarios
5.3. Copia de Seguridad (Backup)
5.4. Documentación
6. EVALUACIÓN DEL PLAN DE CONTINGENCIAS
6.1. Plan de administración de incidentes
6.2. Backup de equipamiento
6.3. Estrategias de recuperación de desastres

2. Objetivos generales de la Auditoría

1. Revisar los puntos vulnerables o fisuras en el sistema informático que ponga en riesgo la seguridad de la información y de las tecnologías empleadas para su procesamiento como base para la elaboración de un diagnóstico y la realización de un informe.
2. Revisar de las políticas y Normas sobre seguridad Física, para garantizar la seguridad e integridad de la información.
3. Verificar la seguridad de personal, datos, hardware, software e instalaciones, con el fin de prevenir o remediar los posibles riesgos.
4. Probar la seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático, para una buena gestión de los Sistemas de la Información en la empresa.

5. Verificar la existencia de controles preventivos, detectivos y correctivos, así como el cumplimiento de los mismos por los usuarios, para llegar a establecer el grado de eficiencia y efectividad.
6. Indagar las metodologías utilizadas, para desarrollar cualquier proyecto que se proponga de manera ordenada y eficaz.
7. Probar el control interno de las aplicaciones, satisfacción de los usuarios, control de procesos y ejecuciones de programas críticos, para verificar su calidad y suficiencia en cuanto a los requerimientos de control y para el mantenimiento de los mismos.
8. Revisar el ciclo de desarrollo del software, para asegurar que el ciclo de vida sea continuo para esos sistemas.
9. Evaluar el mantenimiento preventivo y mantenimiento correctivo, para que no puedan dañar el buen funcionamiento del equipo y posteriormente lograr un soporte técnico proactivo. De esa manera poder garantizar la continuidad del negocio con los costos más bajos.
10. Verificar la administración del entorno de la base de datos, para confirmar si la base de datos funciona como se espera.
11. Evaluar la capacidad del departamento de informática de realizar cualquier clase de trabajo, para atender cualquier contingencia que sea encomendada por los usuarios de la empresa.
12. Verificar las medidas aplicadas a las amenazas, para asegurar que las medidas de prevención, control, compensación y mitigación propuestas sean implementadas oportuna y efectivamente.
13. Incrementar la satisfacción de los usuarios de los sistemas informáticos, para poder garantizar un servicio de calidad.
14. Mejorar el apoyo del departamento de informática a las metas y objetivos de la organización, para disponer de un eficiente y eficaz Sistema de Información para la oportuna toma de decisiones.
15. Observar existencias de riesgos en el uso de Tecnología de información, para obtener un rendimiento adecuado.
16. Capacitar y educar al personal sobre los sistemas informáticos, para que los usuarios no sólo conozcan la paquetería de Office y la navegación por

Internet, sino para que utilicen crítica y reflexivamente la información que obtengan.

3. Metodología Aplicada

La metodología utilizada para la realización de la presente Auditoría Informática se basa en la teoría:

- Cualitativa/Subjetiva.
- Metodología de Evaluación de Riesgos (EDR) en inglés (ROA, Risk Oriented Approach), diseñada por Arthur Andersen, se basa en las listas de chequeo (Check-list) o cuestionarios.

A continuación se muestran los modelos de cuestionarios usados para evaluar cada área de la seguridad y fueron aplicados como entrevistas a los miembros del departamento.

AUDITORÍA LÓGICA

PREGUNTAS	SI	NO	N/A
1. ¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?			
2. ¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?			
3. ¿Existen procedimientos de notificación y gestión de incidencias?			
4. ¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?			
5. ¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			
6. ¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?			
7. ¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?			
8. ¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?			

9. ¿Existe una relación de personal autorizado a acceder a los soportes de datos?			
10. ¿Existe un período máximo de vida de las contraseñas?			
11. ¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?			
12. ¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran o deben estar-documentadas en el Documento de Seguridad?			
13. ¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?			
14. ¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			
15. ¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?			
16. ¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: · Un número máximo de intentos de conexión. · Un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad.			
17. ¿Existen procedimientos de asignación y distribución de contraseñas?			

Preguntas 1-17 del cuestionario de Seguridad Lógica.- Estas preguntas están encaminadas a determinar que tan adecuada es la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORIA FÍSICA 1

PREGUNTAS	SI	NO	N/A
1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?			
2. ¿Existe una persona responsable de la seguridad?			
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?			
4. ¿Existe personal de vigilancia en la institución?			
5. ¿Existe una clara definición de funciones entre los puestos clave?			
6. ¿Se investiga a los vigilantes cuando son contratados directamente?			
7. ¿Se controla el trabajo fuera de horario?			
8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?			
9. ¿Existe vigilancia en el departamento de cómputo las 24 horas?			
10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?			
11. ¿Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?			
12. ¿El centro de cómputo tiene salida al exterior?			
13. ¿Son controladas las visitas y demostraciones en el centro de cómputo?			
14. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?			
15. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?			
16. ¿Se ha adiestrado el personal en el manejo de los extintores?			
17. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?			
18. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?			
19. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?			
20. ¿Saben que hacer los operadores del departamento de cómputo, en			

caso de que ocurra una emergencia ocasionado por fuego?			
21. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?			
22. ¿Existe salida de emergencia?			
23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?			
24. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?			
25. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?			
26. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?			
27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?			
28. ¿Se tienen establecidos procedimientos de actualización a estas copias?			
29. ¿Existe departamento de auditoria interna en la institución?			
30. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?			
31. ¿Se cumplen?			
32. ¿Se auditan los sistemas en operación?			
33. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?			
34. ¿Existe control estricto en las modificaciones?			
35. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?			
36. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?			
37. ¿Se ha establecido que información puede ser acezada y por qué persona?			

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORIA FÍSICA 2

PREGUNTAS	SI	NO	N/A
1. ¿Existen procedimientos para la realización de las copias de seguridad?			
2. ¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana?			
3. ¿Hay procedimientos que aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido?			
4. ¿Existen controles para la detección de incidencias en la realización de las pruebas?			
5. ¿Existen controles sobre el acceso físico a las copias de seguridad?			
6. ¿Sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad?			
7. ¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones?			
8. ¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan?			
9. ¿Existe un inventario de los soportes existentes?			
10. ¿Dicho inventario incluye las copias de seguridad?			
11. ¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación?			
12. ¿Existen procedimientos de actualización de dicho inventario?			
13. ¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?			
14. ¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?			
15. ¿Se evalúan los estándares de distribución y envío de estos soportes?			
16. ¿Se Obtiene una relación de los ficheros que se envían fuera de la empresa, en la que se especifique el tipo de soporte, la forma de envío, el estamento que realiza el envío y el destinatario?			
17. ¿Se Comprueba que todos los soportes incluidos en esa relación se			

encuentran también en el inventario de soportes mencionado anteriormente?			
18. ¿Se Obtiene una copia del Registro de Entrada y Salida de Soportes y se comprueba que en él se incluyen: · Los soportes incluidos en la relación del punto anterior (y viceversa) · Los desplazamientos de soportes al almacenamiento exterior (si existiera)			
19. ¿Se Verifica que el Registro de Entrada y Salida refleja la información requerida por el Reglamento: a) Fecha y hora b) Emisor/Receptor c) Nº de soportes d) Tipo de información contenida en el soporte. e) Forma de envío f) Persona física responsable de la recepción/entrega			
20. ¿Se Analiza los procedimientos de actualización del Registro de Entrada y Salida en relación con el movimiento de soportes?			
21. ¿Existen controles para detectar la existencia de soportes recibidos/enviados que no se inscriben en el Registro de Entrada/Salida?			
22. ¿Se Comprueba, en el caso de que el Inventario de Soportes y/o el Registro de Entrada/Salida estén informatizados, que se realizan copias de seguridad de ellos, al menos, una vez a la semana?			
23. ¿Se realiza una relación de soportes enviados fuera de la empresa con la relación de ficheros de nivel alto?			
24. ¿Se Verifica que todos los soportes que contiene ficheros con datos de nivel Alto van cifrados?			
25. ¿Se Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala?			
26. ¿Se Verifica que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas?			
27. ¿Se Comprueba que la relación es "lógica" (¿personal de limpieza? ¿Vigilantes de seguridad?).			
28. ¿Existen políticas de la instalación en relación con los accesos ocasionales a la sala'			
29. ¿Se Determina que personas tienen llaves de acceso, tarjetas, etc.			

de acceso a la sala?			
30. ¿Se Comprueba que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto?			
31. ¿Se Analizan los procedimientos de descarga a cinta de este Registro de Accesos y el período de retención de este soporte?			
32. ¿Existen procedimientos de realización de copias de seguridad del Registro de Accesos y el período de retención de las copias?			
33. ¿Se Verifica la asignación de privilegios que permitan activar/desactivar el Registro de Accesos para uno o más ficheros?			
34. ¿Se Comprueba que el Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente?			

Preguntas 1-37 del cuestionario de Seguridad Física 1 y preguntas 1-34 del cuestionario de Seguridad Física 2, listado de verificación (Gestión física de seguridad, Evaluación de análisis física de cómputo, Análisis de la delimitación, Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de cómputo, Evaluación del diseño, según el ámbito, Análisis de la seguridad física).- Pretenden obtener información para el análisis en cuanto a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. (http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

LISTADO DE VERIFICACIÓN DE AUDITORÍA FÍSICA

Gestión física de seguridad.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Los objetivos de la instalación física de cómputo					
Las características físicas son seguras					

Los componentes físicos de computo					
La conexiones de los equipos de las comunicaciones e instalaciones Físicas					
La infraestructura es					
El equipos es					
La distribución de los quipos de computo es					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de análisis física de cómputo.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluación de la existencia y uso de normas, resolución base legal para el diseño del centro de computo.					
El cumplimiento de los objetivos fundamentales de la organización para instalar el centro de cómputo.					
La forma de repartir los recursos informáticos de la organización					
La confiabilidad y seguridades el uso de la información institucional					
La satisfacción de las necesidades de poder computacional de la organización.					
La solución a identificación del centro de cómputo (apoyó).					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Análisis de la delimitación la manera en que se cumplen:

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
La delimitación espacial, por las dimensiones físicas.					
La delimitación tecnológica, por los requerimientos y conocimientos informáticos.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de cómputo.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Análisis de la transparencia del trabajo para los usuarios.					
La ubicación del centro de computo					
Los requerimientos de seguridad del centro de computo					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación del diseño según el ámbito.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Análisis del ambiente de trabajo					
Evaluar el funcionamiento de los equipos					
El departamento para el trabajo es					
Los equipos cuentan con					

ventilación					
La iluminación					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Análisis de la seguridad física.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
La seguridad de los equipos.					
El estado centro de computo esta en					
Los accesos de salida son					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Preguntas del Listado de verificación de auditoría física.- Estas preguntas tienen el objetivo de conocer el análisis, diseño, seguridad del hardware, la estabilidad y el aprovechamiento de los recursos informáticos.

AREAS CRÍTICAS DE LA AUDITORIA DE SEGURIDAD

Evaluación de la seguridad en el acceso al Sistema.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluar los atributos de acceso al sistema.					
Evaluar los niveles de acceso al sistema.					
Evaluar la administración de contraseñas al sistema					
Evaluar el monitoreo en el acceso al sistema.					
Evaluar las funciones del administrador del acceso al					

sistema.					
Evaluar las funciones del administrador del acceso al sistema.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la seguridad en el acceso al Área Física

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluar el acceso del personal al centro de cómputo.					
Evaluar el acceso de los usuarios y terceros al centro de cómputo.					
Evaluar el control de entradas y salidas de bienes informáticos del centro de cómputo					
Evaluar la vigilancia del centro de cómputo.					
Evaluar las medidas preventivas o correctivas en caso de siniestro en el centro de cómputo.					
Analizar las políticas de la instalación en relación con los accesos ocasionales a la sala.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de los planes de contingencias informáticos.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluar la existencia, difusión, aplicación y uso de contra contingencias de sistemas.					
Evaluar la aplicación de simulacros,					

así como el plan contra contingencias.					
Evaluar la confidencialidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la seguridad en los sistemas computacionales

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.					
Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos, software e información importante de la organización.					
Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos					
Evaluar el rendimiento, aplicación y utilidad del equipo de cómputo, mobiliario y demás equipos.					
Evaluar la seguridad en el procesamiento de información.					
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la protección contra la piratería y robo de información.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas.					
Protección de archivos.					
Limitación de accesos.					
Protección contra robos					
Protección ante copias ilegales					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la protección contra virus informáticos.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas y correctivas.					
Uso de vacunas y buscadores de virus.					
Protección de archivos, programas e información.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la seguridad del hardware.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de hardware, equipos y periféricos asociados.					
Evaluar la configuración del equipo de computo (hardware).					
Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.					
Evaluar el estado físico del					

hardware, periféricos y equipos asociados					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de la seguridad del Software.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de software, paqueterías y desarrollos empresariales.					
Evaluar las licencias permisos y usos de los sistemas computacionales.					
Evaluar el rendimiento y uso del software de los sistemas computacionales.					
Verificar que la instalación del software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta ultima.					

Preguntas de las áreas críticas de la auditoria de seguridad (Evaluación de la seguridad en el acceso al Sistema, Evaluación de la seguridad en el acceso al Área Física, Evaluación de los planes de contingencias informáticos, Evaluación de la seguridad en los sistemas computacionales, Evaluación de la protección contra la piratería y robo de información, Evaluación de la protección contra virus informáticos, Evaluación de la seguridad del Hardware y Software).- Estas preguntas tienen el objetivo de de conocer el funcionamiento del hardware, la pérdida física de datos y el acceso es controlado impidiendo que otras personas puedan observar la pantalla de la computadora, manteniendo la información y los servidores bajo llave o si son retirados de los escritorios los documentos sensibles. (http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORÍA DESARROLLO DE APLICACIONES

PREGUNTAS	SI	NO	N/A
1. ¿Existe el documento que contiene las funciones que son competencia del área de desarrollo, esta aprobado por la dirección de informática y se respeta?			
2. ¿Se comprueban los resultados con datos reales?			
3. ¿Existe un organigrama con la estructura de organización del área?			
4. ¿Existe un manual de organización que regula las relaciones entre puestos?			
5. ¿Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona?			
6. ¿El plan existe, es claro y realista?			
7. ¿Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo en cuenta la experiencia y formación?			
8. ¿El área de desarrollo lleva su propio control presupuestario?			
9. ¿Se hace un presupuesto por ejercicio y se cumple?			
10. ¿El presupuesto esta en concordancia con los objetivos a cumplir?			
11. ¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?			
12. ¿Existen procedimientos de contratación?			
13. ¿Las personas seleccionadas cumplen los requisitos del puesto al que acceden?			
14. ¿Las ofertas de puestos del área se difunden de forma suficiente fuera de la organización y las selecciones se hacen de forma objetiva?			
15. ¿Existe un plan de formación que este en consonancia con los objetivos tecnológicos que se tenga en el área?			
16. ¿El plan de trabajo del área tiene en cuenta los tiempos de formación?			
17. ¿Existe un protocolo de recepción / abandono para las personas que se incorporan o dejan el área?			
18. ¿Existe un protocolo y se respeta para cada incorporación / abandono?			
19. ¿En los abandonos del personal se garantiza la protección del área?			
20. ¿Existe una biblioteca y una hemeroteca accesibles por el personal			

del área?			
21. ¿Esta disponible un numero suficiente de libros, publicaciones periódicas, monografías, de reconocido prestigio y el personal tiene acceso a ellos?			
22. ¿El personal esta motivado en la realización de su trabajo?			
23. ¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?			
24. ¿Existe rotación de personal y existe un buen ambiente de trabajo?			
25. ¿La realización de nuevos proyectos se basa en el plan de sistemas en cuanto a objetivos?			
26. ¿Las fechas de realización coinciden con los del plan de sistemas?			
27. ¿El plan de sistemas se actualiza con la información que se genera a lo largo de un proceso?			
28. ¿Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas?			
29. ¿Existe un procedimiento para la propuesta de realización de nuevos proyectos?			
30. ¿Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas?			
31. ¿Se respeta este mecanismo en todas las propuestas?			
32. ¿Existe un procedimiento de aprobación de nuevos proyectos?			
33. ¿Existe un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto?			
34. ¿Se tiene en cuenta a todas las personas disponibles cuyo perfil sea adecuado a los riesgos de cada proyecto y que tenga disponibilidad para participar?			
35. ¿Existe un protocolo para solicitar al resto de las áreas la participación del personal en el proyecto y se aplica dicho protocolo?			
36. ¿Existe un procedimiento para conseguir los recursos materiales necesarios para cada proyecto?			
37. ¿Se tiene implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda?			
38. ¿La metodología cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyectos?			
39. ¿La metodología y las técnicas asociadas a la misma están adaptadas			

al entorno tecnológico y a la organización del área de desarrollo?			
40. ¿Existe un catalogo de las aplicaciones disponible en el área?			
41. ¿Existe un registro de problemas que se producen en los proyectos del área?			
42. ¿Existe un catalogo de problemas?			
43. ¿El catalogo es accesible para todos los miembros del área?			
44. ¿Se registran y controlan todos los proyectos fracasados?			

Preguntas 1-44 del cuestionario de auditoría desarrollo de aplicaciones.- Buscan conocer si el departamento cuenta con personal que sea capaz de analizar, diseñar, desarrollar, probar, implantar y mantener software para facilitar al usuario la realización de un determinado tipo de trabajo. Y comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros. (http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORÍA MANTENIMIENTO

PREGUNTAS	SI	NO	N/A
1. Existe un contrato de mantenimiento.			
2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?			
3. ¿Se lleva a cabo tal programa?			
4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?			
5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?			
6. ¿Existe plan de mantenimiento preventivo. ?			
7. ¿Este plan es proporcionado por el proveedor?			
8. ¿Se notifican las fallas?			
9. ¿Se les da seguimiento?			
10. ¿Tiene un plan logístico para dar soporte al producto software?			
11. ¿Los requerimientos de mantenibilidad se incluyen en la Actividad de			

Iniciación durante el Proceso de Adquisición (ISO 12207) y se evalúa durante el Proceso de Desarrollo?			
12. ¿Las variaciones en el diseño son supervisadas durante el desarrollo para establecer su impacto sobre la mantenibilidad?			
13. ¿Se realizan varios tipos de medidas para poder estimar la calidad del software?			
14. ¿La mantenibilidad se tiene en cuenta antes de empezar a desarrollar?			
15. ¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, así como recursos y secuencias relevantes de actividades?			
16. ¿Durante el análisis de requerimientos, los siguientes aspectos que afectan a la mantenibilidad, son tomados en cuenta? • Identificación y definición de funciones, especialmente las opcionales. • Exactitud y organización lógica de los datos. • Los Interfaces (de máquina y de usuario). • Requerimientos de rendimiento. • Requerimientos impuestos por el entorno (presupuesto). • Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad. • Énfasis del Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de Documentación			
17. ¿La transición del software consiste en una secuencia controlada y coordinada de acciones para trasladar un producto software desde la organización que inicialmente ha realizado el desarrollo a la encargada del mantenimiento?			
18. ¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición? ¿Qué es lo que incluye este plan? • La transferencia de hardware, software, datos y experiencia desde el desarrollador al mantenedor. • Las tareas necesarias para que el mantenedor pueda implementar una estrategia de mantenimiento del software.			
19. ¿El mantenedor a menudo se encuentra con un producto software			

con documentación?			
20. ¿Si no hay documentación, el mantenedor deberá crearla? ¿Realiza lo siguiente? a) Comprender el dominio del problema y operar con el producto software. b) Aprender la estructura y organización del producto software. c) c. Determinar qué hace el producto software. Revisar las especificaciones (si las hubiera)			
21. ¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados, si fuese necesario?			
22. El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software			
23. ¿Los elementos software reflejan la documentación de diseño?			
24. ¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?			
25. ¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas?			
26. ¿La documentación de usuario cumple los estándares especificados?			
27. ¿Los costes y calendarios se ajustan a los planes establecidos?			

Preguntas 1-27 del cuestionario de Auditoría del Mantenimiento.- Su objetivo es descubrir si existe un programa de mantenimiento preventivo para cada dispositivo y si existe un plan de mantenibilidad que reduzca los costos de mantenimiento y medir la efectividad del mantenimiento. (http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORÍA BASES DE DATOS

PREGUNTAS	SI	NO	N/A
1. Existe equipos o software de SGBD			
2. La organización tiene un sistema de gestión de base de datos (SGBD)			
3. Los datos son cargados correctamente en la interfaz grafica			
4. Se verificará que los controles y relaciones de datos se realizan de acuerdo a Normalización libre de error			

5. Existe personal restringido que tenga acceso a la BD			
6. El SGBD es dependiente de los servicios que ofrece el Sistema Operativo			
7. La interfaz que existe entre el SGBD y el SO es el adecuado			
8. ¿Existen procedimientos formales para la operación del SGBD?			
9. ¿Están actualizados los procedimientos de SGBD?			
10. ¿La periodicidad de la actualización de los procedimientos es Anual?			
11. ¿Son suficientemente claras las operaciones que realiza la BD?			
12. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que están autorizados tengan una razón de ser procesados)			
13. ¿Se procesa las operaciones dentro del departamento de cómputo?			
14. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?			
15. ¿Existe un control estricto de las copias de estos archivos?			
16. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?			
17. ¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de cómputo?			
18. ¿Se tiene un responsable del SGBD?			
19. ¿Se realizan auditorias periódicas a los medios de almacenamiento?			
20. ¿Se tiene relación del personal autorizado para manipular la BD?			
21. ¿Se lleva control sobre los archivos trasmitidos por el sistema?			
22. ¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?			
23. ¿Existen integridad de los componentes y de seguridad de datos?			
24. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo capaz que soportar el trabajo?			
25. ¿El SGBD tiene capacidad de teleproceso?			
26. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?			
27. ¿La capacidad de almacenamiento máximo de la BD es suficiente para atender el proceso por lotes y el proceso remoto?			

Preguntas 1-27 del cuestionario de Auditoría de Bases de Datos.- Pretenden obtener información en cuanto a la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos. (http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORÍA CALIDAD

PREGUNTAS	SI	NO	N/A
¿Se reflejan el software codificado tal como en el diseño en la documentación?			
¿Fueron probados con éxito los productos de software usados en el centro de cómputo?			
¿Se cumplen las especificaciones de la documentación del usuario del software?			
¿Los procesos de gestión administrativa aplicados en el área de informática de la institución son lo suficientemente óptimos?			
¿El funcionamiento del software dentro del área de trabajo está de acuerdo con los requerimientos específicos?			
¿Los documentos de gestión administrativa se cumplen satisfactoriamente en el área de cómputo?			
¿Los productos de software que utilizan en el área de informática esta de acuerdo con los estándares establecidos?			
¿Los dispositivos de trabajo en el área de informática se les realizan una revisión técnica correcta?			
¿Los costos fijados en la revisión técnica se encuentran dentro de los límites fijados?			

Preguntas 1-9 del cuestionario de Auditoría de Calidad.- Estas preguntas nos dan a conocer todo el sistema de gestión de calidad, procedimientos y si son cumplidos.

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

AUDITORÍA COMUNICACIONES Y REDES

PREGUNTAS	SI	NO	N/A
1. ¿La gerencia de redes tiene una política definida de planeamiento de tecnología de red?			
2. Esta política es acorde con el plan de calidad de la organización			
3. ¿La gerencia de redes tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes, teniendo en cuenta los posibles cambios tecnológicos o en la organización?			
4. ¿Existe un inventario de equipos y software asociados a las redes de datos?			
5. ¿Existe un plan de infraestructura de redes?			
6. ¿El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes?			
7. ¿La responsabilidad operativa de las redes esta separada de las de operaciones del computador?			
8. Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados			
9. ¿Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas?			
10. ¿Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red?			
11. Existen protocolos de comunicaron establecida			
12. Existe una topología estandarizada en toda la organización			
13. ¿Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?			
14. ¿La transmisión de la información en las redes es segura?			
15. ¿El acceso a la red tiene password?			

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

ÁREA CRÍTICA DE AUDITORÍA DE REDES

Gestión administrativa de la red.

PREGUNTAS	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Los objetivos de la red de computo					
Las características de la Red de computo					
Los componentes físicos de la red de Computo					
La conectividad y las comunicaciones de la red de computo					
Los servicios que proporcionan la red de computo					
Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.					
Los protocolos de comunicación interna de la red.					
La administración de la red de Cómputo.					
La seguridad de las redes de cómputo.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación de análisis de la red de cómputo.

Evaluar y calificar el cumplimiento de los siguientes aspectos	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Evaluación de la existencia y uso de metodologías, normas, estándares y políticas para el análisis y diseño de					

redes de cómputo.					
Análisis de la definición de la problemática y solución para instalar redes de computo en la empresa					
Análisis de cumplimiento de los objetivos fundamentales de la organización para instalar una red de computo , evaluando en cada caso					
La forma de repartir los recursos informáticos de la organización, especialmente la información y los activos.					
La cobertura de servicios informáticos para la captura, el procesamiento y la emisión de información en la organización.					
La cobertura de los servicios de comunicación					
La frecuencia con que los usuarios recurren a los recursos de la red					
La confiabilidad y seguridades el uso de la información institucional					
La centralización, administración, operación asignación y el control de los recursos informáticos de la organización					
La distribución equitativa de los costos de adquisición y el control de los recursos informáticos de la organización					
La escalabilidad y migración de los recursos computacionales de la organización.					

La satisfacción de las necesidades de poder computacional de la organización, sea con redes, cliente/servidor o mainframe					
La solución a los problemas de comunicación de información y datos en las áreas de la organización.					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa:

Evaluar y calificar el cumplimiento de los siguientes aspectos	**100% Excelente**	**80% Buena**	**60% Regular**	**40% Mínimo**	**20% No cumple**
El estudio de factibilidad tecnológica					
El estudio factibilidad económica					
El estudio de factibilidad administrativa					
El estudio de factibilidad operativa					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Evaluación del diseño e implementación de la red según el ámbito de cobertura.

Evaluar y calificar el cumplimiento de los siguientes aspectos	**100% Excelente**	**80% Buena**	**60% Regular**	**40% Mínimo**	**20% No cumple**
Análisis de las redes de multicomputadoras					
Evaluar el funcionamiento de la cobertura de punto a punto					
Evaluar el funcionamiento de la					

tecnología que se usa con un solo cable entre las Máquinas conectadas					
Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes					

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

Análisis de la red de área local (L A N)

Evaluar y calificar el cumplimiento de los siguientes aspectos	**100% Excelente**	**80% Buena**	**60% Regular**	**40% Mínimo**	**20% No cumple**
Evaluar el uso adecuado y confiable de la tecnología utilizada internamente para la transmisión de datos.					
Evaluar la restricción adoptada para establecer el tamaño de la red					
Evaluar la velocidad.					

Preguntas 1-15 del cuestionario de Auditoría de Comunicaciones y Redes, así como las Áreas Críticas.- Estas preguntas nos dan a conocer como se encuentra la topología, configuraciones, tipo y cobertura de la red, si cuenta con protocolos bien definidos, si existe un control, si es confiable y segura.

(http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf)

A continuación se muestra una guía de cuestionario para ser usado para evaluar a los usuarios ajenos al área de informática.

Evaluar y calificar el cumplimiento de los siguientes aspectos
1. ¿Considera que el Departamento de Informática de los resultados esperados? Si ( ) No ( ) ¿Por que?
2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Informática? Deficiente ( ) Aceptable ( ) Satisfactorio ( ) Excelente ( ) ¿Por que?
3. ¿Cubre sus necesidades el sistema que utiliza el departamento de Informática? No las cubre ( ) Parcialmente ( ) La mayor parte ( ) Todas ( ) ¿Por que?
4. ¿Hay disponibilidad del departamento de Informática para sus requerimientos? Generalmente no existe ( ) Hay ocasionalmente ( ) Regularmente ( ) Siempre ( ) ¿Por que?
5. ¿Son entregados con puntualidad los trabajos? Nunca ( ) Rara vez ( ) Ocasionalmente ( ) Generalmente ( ) Siempre ( ) ¿Por que?
6. ¿Que piensa de la presentación de los trabajados solicitados al departamento de Informática? Deficiente ( ) Aceptable ( ) Satisfactorio ( )

Excelente ( ) ¿Por que?
7. ¿Que piensa de la asesoría que se imparte sobre informática? No se proporciona ( ) Es insuficiente ( ) Satisfactoria ( ) Excelente ( ) ¿Por que?
8. ¿Que piensa de la seguridad en el manejo de la información proporcionada por el sistema que utiliza? Nula ( ) Riesgosa ( ) Satisfactoria ( ) Excelente ( ) Lo desconoce ( ) ¿Por que?
9. ¿Existen fallas de exactitud en los procesos de información? ¿Cuáles?
10. ¿Cómo utiliza los reportes que se le proporcionan?
11. ¿Cuáles reportes no le sirven para tomar decisiones?
12. ¿Se cuenta con un manual de usuario por Sistema? SI ( ) NO ( )
13. ¿Es claro y objetivo el manual del usuario? SI ( ) NO ( )
14. ¿Que opinión tiene del manual? NOTA: Pida el manual del usuario para evaluarlo.
15. ¿Quién interviene de su departamento en el diseño de sistemas?
16. ¿Que sistemas necesitaría en su departamento para la realización de su trabajo?
17. Observaciones:

Preguntas 1-17 del cuestionario de entrevista a usuarios. Finalmente estas preguntas nos dan a conocer el punto de vista de los usuarios respecto al departamento de informática. (Nora Lilia Solorio Nava)

6.5 Resultados obtenidos de la aplicación de los cuestionarios

Los cuestionarios fueron aplicados a modo de entrevista ya que las múltiples ocupaciones de los integrantes del departamento no se los permitían, no se realizo un muestreo debido a que el universo de investigación es de únicamente seis integrantes por esta razón se aplico a todo el universo.

En lo que respecta a la estructura del departamento se refiere y cómo éste ayuda a cumplir con las funciones del mismo se determinó que existe una estructura adecuadamente definida, el personal que integra el departamento cumple con sus objetivos, el departamento cuenta con un organigrama y una estructura oficialmente definida.

Referente a la seguridad física (Gráfica 1), la ubicación del centro de cómputo se encontró que está a salvo de inundación, que da al exterior, que el edificio está construido con PTR y materiales prefabricados como Durok, que el centro de cómputo se encuentra en un lugar fuera del alto tráfico de personas, tiene paredes inflamables más no despiden polvo; se tiene lugar suficiente para los equipos y la instalación no está sobresaturada. Se cuenta con piso elevado, con una cámara plana limpia y el piso es antiestático.

En cuanto al aire acondicionado, la temperatura en la que trabajan los equipos es la adecuada, los ductos de aire están limpios, se controla la humedad con un equipo autoregulable de temperatura que es programado; los ductos de aire no cuentan con alarmas contra intrusos.

Se encontró que la instalación eléctrica y el suministro de energía cuenta con tierra física, el cableado se encuentra debidamente instalado y se identifican los cables de acuerdo a su tipo de carga, los contactos están bien identificados, se cuenta con planos de la instalación eléctrica; la instalación del equipo de cómputo se encuentra independiente de otras instalaciones eléctricas, se utiliza material antiestático, se cuenta con reguladores para los equipos de cómputo, se verifica la regulación de cargas máximas y mínimas, se cuenta con equipo

ininterrumpible y generadores de corriente ininterrumpida, se tiene un switch de apagado de emergencia.

Con respecto a los desastres provocados por agua, no se cuenta con alarmas contra inundaciones.

La detección de humo y fuego, existe una alarma manual para avisar de la presencia de fuego, existe una alarma en el cuarto de máquinas para detectar condiciones anormales del ambiente, la alarma es perfectamente audible y está conectada al puesto de guardias y a la estación de bomberos; se ha adiestrado a el personal en el manejo de extintores estos funcionan a base de un polvo, se revisa su funcionamiento con el proveedor, se cuenta con máscaras contra gases y sistemas portátiles de oxígeno, se tienen identificadas y señaladas las salidas de emergencia. Se han tomado medidas para minimizar la posibilidad de fuego evitando artículos inflamables, prohibiendo fumar, vigilando y manteniendo el sistema eléctrico.

Por otro lado la autorización de accesos se han adoptado medidas de seguridad, se controla el trabajo fuera de horario, existe una persona responsable encargada de la seguridad, se cuenta con cámaras de vigilancia, se identifica a la persona que ingresan, se cuenta con vigilantes en la institución, registro de entradas, las visitas y demostraciones son guiadas.

Otro aspecto es la seguridad lógica (Gráfica 2), fueron probados con éxito los productos de software usados en el centro de cómputo. Existen controles y medidas de seguridad en cuanto a salvaguardar la información en respaldos y a su vez en cajas de seguridad, también se cuenta con un control en transacciones de documentos (información confidencial, captación de documentos, cómputo electrónico), en los sistemas utilizados por el personal de informática y demás departamentos existe la identificación del usuario y autentificación; pero este control no es utilizado correctamente ya que no hay un cierto nivel de seguridad. Referente al modo de acceso que se permite al usuario sobre los recursos y a la

información, no existen limitaciones en cuanto a lectura, escritura, borrado y ejecución.

En cuanto al desarrollo de aplicaciones (Gráfica 3), no se toma en cuenta el ciclo de vida del software por parte del personal informático. Como consecuencia no existe documentación de ningún sistema desarrollado, manuales, etc. Los sistemas creados cuentan con identificación y autentificación, aunque no muy segura, ya que no se han establecido un número máximo de violaciones en sucesión para que la computadora o el sistema cierre esa terminal y se de aviso al responsable de ella.

En el mantenimiento (Gráfica 4), se realizan revisiones a equipos cuando estas son solicitadas por parte del personal de la organización al departamento informático, para verificar y actualizar la integración de los equipos y sus componentes; y mejorar el uso de los mismos.

Referente a Bases de datos (Gráfica 5), se tiene un control al respaldar y proteger la información vital para la empresa en una bóveda con acceso restringido, se tienen establecidos procedimientos de actualización de copias.

La seguridad de Redes y comunicaciones (Gráfica 6), su conectividad, cobertura y la comunicación de la red de cómputo, son buenas. Existe una topología estandarizada en toda la organización de tipo estrella, la transmisión de la información en las redes es segura y el acceso a la red tiene password. Las redes inalámbricas necesitan más seguridad en cuanto a que viajan en forma de ondas de radio y pueden viajar más allá de las paredes, filtrarse en casas/oficinas contiguas o llegar hasta la calle.

En cuanto a la calidad (Gráfica 7), la empresa tiene un conjunto de objetivos que se llevan al pie de la letra, consiguiendo certificaciones en calidad, seguridad empresarial, etc.

En lo que concierne a piratería y virus (Gráfica 8), en algunos equipos no están actualizados los últimos parches de seguridad para ambas opciones. En

cuanto a la piratería del software instalado se me comento que existe un control interno por parte de CFE.

Haciendo referencia a la opinión de una encuesta aplicada a personal de algunos departamentos que conforman la organización (Gráfica 9), en cuanto atención al servicio de fallas por parte del departamento informático es regular, aunque haya disponibilidad para requerimientos que se presentan, se menciona que la asesoría en temas informáticos es insuficiente. El personal piensa que es riesgosa la seguridad de los sistemas que utilizan para llevar a cabo sus labores, mencionan que no se les toma en cuenta a la hora del diseño de los sistemas y se menciona que requieren sistematizar algunos procesos que todavía se tienen que hacer en Word, Excel, etc. En general el personal comenta que falta más personal en el área informática.

6.6 Interpretación

Una vez aplicadas las distintas herramientas para el análisis de la seguridad del departamento de informática, se encontró lo siguiente:

Seguridad Física

La seguridad en el área informática es buena aunque podría llegar a ser excelente ya que es necesario poner atención en las ocasiones que por las actividades propias del personal el departamento se queda prácticamente solo y todos los sistemas en el son susceptibles de ser violados, de que se extraiga información de los mismos o que dicha información sea alterada de manera anónima ocasionando un grave daño a la información que es prioritaria en la institución.

Seguridad Lógica

Por medio de la observación pude darme cuenta que en los demás departamentos de la organización tanto los jefes, las secretarias y eventuales. Se saben las contraseñas de unos y de otros. Un ejemplo es que el jefe del depto. de

obra pública se sabe la contraseña de su secretaría y está a la vez sabe la de su jefe, y cuando son suplidos por cursos, vacaciones, etcétera. Los eventuales que ocupan sus puestos se saben también las contraseñas. Y esto puede ser grave porque se puede perder la integridad de la información.

El manejo de los equipos de cómputo en cuanto a su reemplazo y redistribución es eficiente ya que el departamento de informática cuenta con un sistema de inventario de hardware y software en el que se lleva un registro de cada equipo con que se cuenta en la subgerencia y las características del mismo así como quien tiene el resguardo del equipo con lo que la distribución del equipo a otras áreas es más fácil.

Seguridad Desarrollo de Aplicaciones

El personal informático no toma en cuenta el seguimiento de las fases del ciclo de vida del software, y puede llegar a ser un gran riesgo para la empresa.

La seguridad en los sistemas es ineficiente en el caso de que alguna persona quisiera modificar los datos para los cuales no tiene la autorización, en los sistemas no se han establecido un número máximo de violaciones en sucesión para que el sistema cierre esa terminal.

Seguridad Mantenimiento

El personal de informática cuenta con una bitácora de mantenimiento que le permite llevar un buen control de esta actividad, en este manual se registra la información necesaria de cada equipo con la cual se puede fácilmente corregir algún problema que ya se ha presentado con anterioridad, ya que se detalla el procedimiento usado para su corrección.

Seguridad Bases de Datos

Se hace un buen manejo de la integridad de la información que es vital para la empresa.

Seguridad Redes

Si nuestra instalación está abierta, una persona con el equipo adecuado y conocimientos básicos podría no sólo utilizar nuestra conexión a Internet, sino también acceder a nuestra red interna Si la infiltración no autorizada en redes inalámbricas de por sí ya es grave en una instalación residencial (en casa), mucho más peligroso es en una instalación corporativa.

Virus

Es fundamental que actualicen los parches con la mayor frecuencia posible (en rigor todos los días).

Personal

En lo que respecta a capacitación del personal de la subgerencia por parte del departamento de informática, se requiere que actualice periódicamente su conocimiento en el software utilizado y en la manera de manejo y uso correcto del hardware. Ya que con frecuencia ocurren problemas con el funcionamiento de la red sobre todo en el aspecto de impresión en impresoras de red.

Algunos comentarios de numerosos trabajadores de la organización estiman que la seguridad es responsabilidad exclusiva del departamento de informática. Es importante que los usuarios comprendan que el personal del departamento de informática no puede hacerse cargo de la seguridad de la información por sí solo.

Comentaron que las cargas de trabajo no son asignadas correctamente al personal de informática, ya que el personal en muchas ocasiones tiene demasiado trabajo en la subgerencia y no se da abasto para llevarlo a cabo.

Como hemos podido observar en este capítulo, se ha cumplido con algunos de los objetivos en cuanto a determinar la eficiencia y las deficiencias que tienen el departamento de informática.

6.7 Dictamen

Uruapan, Mich., 12 de marzo de 2008

COMISIÓN FEDERAL DE ELECTRICIDAD
SUBGERENCIA REGIONAL DE GENERACIÓN HIDROELECTRICA BALSAS SANTIAGO
ING. ALBERTO PALOMINO VÁZQUEZ
JEFE DEL DPTO. DE CONTROL DE GESTIÓN E INFORMÁTICA

He efectuado una auditoría a la seguridad informática de la COMISIÓN FEDERAL DE ELECTRICIDAD SUBGERENCIA REGIONAL DE GENERACIÓN HIDROELECTRICA BALSAS SANTIAGO del 11 de febrero al 14 de marzo de 2008.

Mi responsabilidad consiste en emitir una opinión sobre está en base a la auditoría que efectué.

Objetivos:

- Hacer un estudio cuidadoso de los riesgos potenciales a los que está sometida el área de informática, para detectar y corregir errores.

- Revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más Importantes de aquél.

Hallazgos:

1. Hay seguridad en cuanto a la identificación del personal de la institución y de la que no pertenece a la misma.
2. Los sistemas desarrollados cuentan con un sistema de passwords, pero no tienen un límite máximo de violaciones en sucesión para que el sistema cierre.

3. Falta de documentación de manera tal que se perdió el control en el desarrollo de cada una de las etapas del ciclo de vida (análisis, diseño, desarrollo, pruebas, implantación y manuales de usuario).
4. Falta de documentación de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción.
5. No existen copias de seguridad de los sistemas utilizados en la subgerencia y la frustrante experiencia de perder documentos importantes tras un incidente de seguridad sería fatal para la empresa.
6. En las ocasiones que por las actividades propias del personal el departamento se queda prácticamente solo, todos los sistemas en el son susceptibles, y puede que se extraiga información o que sea alterada de manera anónima ocasionando un grave daño a la información que es prioritaria en la institución.
7. Algunos sistemas operativos no tenían instalados los últimos "parches" de antivirus.
8. Existen programas de capacitación, pero el personal de la subgerencia comenta que requiere una actualización en temas de informática.
9. En el personal de la subgerencia falta más información a cerca de la seguridad informática ya que algunos trabajadores lo toman a mal los cambios que se han hecho.
10. Descontento general de los usuarios por plan de seguridad implementado en la subgerencia.

Recomendaciones:

- ✓ Instalar mejores controles de acceso con algo que solamente el individuo conozca: por ejemplo un número de identificación personal o PIN, etc.
- ✓ Instalar software de monitoreo contra detección de intrusos.
- ✓ Mejorar la seguridad de las telecomunicaciones.

- ✓ Mejorar la seguridad de las aplicaciones web y empresariales.
- ✓ Implementar auditorías de seguridad.
- ✓ Asegurar accesos remotos.
- ✓ Mejorar o crear la conciencia de los usuarios sobre seguridad.
- ✓ Establecer seguridad de redes inalámbricas.
- ✓ Implementar pruebas o auditorías de penetraciones, incluido hackeo ético.
- ✓ Restringir el acceso a los programas y archivos, esto se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información como: lectura, escritura, ejecución, borrado y todas las opciones anteriores.
- ✓ Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no les correspondan.
- ✓ Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro. Y que sea la misma que ha sido transmitida.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.
- ✓ Que la capacitación al personal no sea solamente por parte del personal informático de la subgerencia, sino que se exija que el personal que conforma la empresa tome cursos por cuenta propia con el fin de actualizarse en temas conocidos o nuevos.
- ✓ Los programas de sensibilización sobre seguridad no tendrán éxito si van en contra de la cultura de la organización. Esperemos que este no sea el caso de esta organización, que ya ha puesto en marcha. Deben de explicar a los usuarios por qué es importante la seguridad con el fin de motivarlos a modificar su comportamiento. Los usuarios desarrollan malos hábitos durante semanas, meses e incluso años, debido a que la cuestión de la seguridad no se atiende desde un principio. No sólo es necesario educar a

los usuarios en materia de seguridad, sino que éstos también tienen que "olvidar" los malos hábitos que han adquirido. Además, dichos usuarios suelen tener más problemas para reconocer la utilidad de la seguridad. En su opinión, la organización ha funcionado bien durante muchos años sin seguridad. Y consideran que los nuevos requisitos de seguridad son cambios innecesarios que les complican la vida.

Identificación y Firma del Auditor

_____

NORA LILIA SOLORIO NAVA

CONCLUSIONES GENERALES

Al realizar el presente trabajo se investigo acerca de todos los elementos que componen al departamento de Control de Gestión e Informática de la Subgerencia de la Comisión Federal de Electricidad de la ciudad de Uruapan, institución dentro de la cual estuve prestando mi servicio social por espacio de seis meses, durante este período, tuve la oportunidad de relacionarme con el personal del departamento de informática, de conocer sus actividades y darme cuenta de la manera en que organizaban sus funciones, así como el papel que el departamento tenía, por esta razón pude observar algunos problemas que presentaba en su organización y su seguridad interna, por ese motivo me pareció que sería un caso de estudio en el que podía aplicar mis conocimientos adquiridos en la universidad, y al ver el interés del mismo departamento en que se llevará a cabo un análisis para detectar sus deficiencias, decidí hacer la investigación, para lo cual se aplicaron diversas técnicas de recopilación de información, sustentadas en el marco teórico, presentado en los primeros capítulos, con las que se pretendió obtener información que nos permitiera conocer cuáles problemas se presentaban y las causas de los mismos, a fin de cumplir con el objetivo de:

Realizar una auditoría informática para analizar la seguridad del departamento de informática para determinar sus posibles deficiencias y proponer una solución al problema.

Para lo cual se busco cumplir con otros objetivos particulares:

1. Conocer el entorno y el ámbito de trabajo del departamento de informática de la C.F.E.
2. Conocer cuales son los problemas a los que se ha enfrentado el departamento de informática de la C.F.E. en relación a la seguridad de su información.
3. El análisis de la eficiencia de los Sistemas Informáticos.
4. Sensibilizar a los profesionales del área de informática hacia la necesidad de proteger uno de los activos importantes en las organizaciones, cómo lo es la información.

Por medio de la investigación se ha podido determinar que la hipótesis planteada desde la introducción es válida, ya que la C.F.E. ha empezado a preocuparse por la seguridad de la organización, trabajadores y visitantes, utilizando sus múltiples recursos para tomar medidas.

Se ha implantado un control de entrada de visitantes, un sistema biométrico de autenticación, un circuito cerrado, campañas sobre la seguridad informática, pláticas sobre la concientización de la seguridad informática.

Y se han podido contestar las preguntas de investigación planteadas en el capítulo VI, ya que se ha encontrado que existe un control de la Seguridad Informática dentro de la empresa la cual facilita el desempeño de la organización, se evaluó la situación actual así como la eficiencia o deficiencia de la seguridad dentro del departamento, se aplicaron cuestionarios-entrevistas al personal para saber si será vulnerable a las fugas de información por parte de su personal, intrusos, extorsiones, espionaje industrial, desastres naturales, accidentes, violación de la seguridad, etc.

Dentro de los capítulos teóricos, hemos aprendido conceptos que nos han hecho ver la importancia de contar con la seguridad informática, en el capitulo 1 vimos que la informática es una ciencia relacionada directamente con la toma de decisiones, que las generaciones de las computadoras han dado pasó a lo que hoy conocemos como las computadoras más modernas, también en el capítulo 2 fuimos analizado los conceptos de administración y centros de cómputo, así como la importancia de su existencia en las organizaciones, cómo está conformado y qué necesidades resuelven, por otro lado en el capítulo 3 encontramos el concepto de seguridad y su evolución, analizamos el concepto de la seguridad informática y su principal objetivo, además vimos qué es un intruso y que en cualquier sistema informático existen tres elementos básicos a proteger los cuales son: el hardware, el software y los datos. También en el capítulo 4 analizamos que toda empresa, pública o privada, que posea Sistemas de Información, deben de someterse a un control estricto de evaluación de eficacia y eficiencia, en cuanto al trabajo de la Auditoría Informática. Otro aspecto

importante de resaltar en el capitulo 5 es la utilidad de realizar una Auditoría de Seguridad Informática en las PYMEs.

Por lo tanto podemos afirmar que los centros de cómputo son muy importantes hoy en día para que una organización mantenga su flujo de información adecuado que le permita procesar grandes volúmenes de datos y obtenga información que sea útil en la toma de decisiones, además de facilitarle muchas actividades que en forma manual serían costosas y lentas, con todo esto debemos tomar conciencia de lo importante que es la seguridad informática, a fin de que el departamento de informática sea lo más eficiente posible y contribuya a que los demás departamentos de la organización cuenten con información oportuna y confiable para llevar a cabo sus funciones.

También a través de esta investigación hemos visto la importancia que tiene el evaluar constantemente el desempeño del centro de cómputo a fin de detectar problemas y corregirlos antes de que se agraven y sea más difícil resolverlos. Además de fomentar la cultura en el personal de la organización acerca de la seguridad informática.

Como ya lo mencionamos se cumplieron los cuestionamientos de la hipótesis y esto quiere decir que no se encontraron problemas tan serios en cuanto a la seguridad informática, se cumplió con uno de los objetivos planteados al principio el cual es proponer soluciones a mejorar en la seguridad del departamento de informática de acuerdo a lo encontrado como resultado de la Auditoria Informática realizada a el departamento de Control de Gestión e Informática, por el período comprendido entre el 11 de febrero al 14 de marzo del 2008, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoría. Y a continuación se presenta la propuesta de mejora.

PROPUESTA

En base a los resultados obtenidos del análisis se hacen las siguientes propuestas con la finalidad de que sean de utilidad para mejorar la eficiencia de la seguridad del departamento de informática.

a) Colocar detectores y extintores de incendios automáticos en los lugares necesarios. Y si es posible remover del centro de cómputo los materiales inflamables.

b) Elaborar toda la documentación técnica correspondiente a los sistemas implementados y establecer normas y procedimientos para los desarrollos y su actualización. Conservar todas las documentaciones de prueba de los sistemas, como así también las modificaciones y aprobaciones de programas realizadas.

c) En cuanto a la capacitación, que se lleven a cabo sondeos en los diferentes departamentos de la subgerencia para detectar las necesidades de capacitación del personal y se apliquen exámenes de manera periódica a fin de evaluar el avance en el dominio de equipos y software por parte del personal usuario. Ya que mientras más capacitado este el personal menor será la necesidad del departamento en actividades fáciles pero que requieren tiempo.

d) El costo de la seguridad debe considerarse como un costo más entre todos los que son necesarios para desempeñar la actividad que es el objeto de la existencia de la entidad, sea ésta la obtención de un beneficio o la prestación de un servicio público.

e) Respecto a la seguridad del departamento, manejar en los sistemas passwords que permitan bloquear los equipos del departamento sin tener que apagarlos para que no puedan ser accesados por ninguna persona cuando el personal no se encuentre en el área, otro aspecto que es

importante señalar es la asignación de personal de seguridad y/o cámaras de vigilancia a fin de garantizar la seguridad física de los equipos para evitar cualquier violación en el centro de cómputo o desde cualquier otra área de la subgerencia, es importante que se elaboren manuales de seguridad en los que se describan qué procedimientos se deben seguir en caso de que se presente algún siniestro, que llegue a dañar los equipos y la información, así como un método para evaluar los esquemas de seguridad a fin de asegurarse que sean eficientes y que se actualicen conforme se vaya requiriendo dadas las condiciones que se presenten.

f) Crear un puesto o cargo específico para la función de Seguridad Informática.

g) Por otro lado sería importante seguir promoviendo campañas que concienticen tanto al personal del área informática como al personal de otras áreas de la importancia de la seguridad en los sistemas de cómputo y que todas las áreas deben contribuir a que ésta exista, de esta manera se tendrá mayor seguridad tanto en los equipos del departamento como en su información reduciendo los riesgos de llegar a perder información o equipo valioso para la subgerencia.

h) Consideró que se realicen tres copias de respaldos de los sistemas y de las bases de datos en cintas magnéticas de las cuales, una se encuentre en el recinto del área de informática, otra en la bóveda de seguridad y la última en poder del Jefe de área.

i) Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operación normal de la institución y establecer los responsables de cada sistema.

j) Efectuar pruebas simuladas en forma periódica, a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.

k) Realizar periódicamente un estudio de vulnerabilidad, documentando efectivamente el mismo, a los efectos de implementar las acciones correctivas sobre los puntos débiles que se detecten.

l) También sería importante que tanto las funciones, como los objetivos del área de informática se dieran a conocer a los demás departamentos para crear una conciencia clara de la función tan importante que esta área cumple, con lo que el apoyo que prestarían las demás áreas redundaría en un mejor servicio.

BIBLIOGRAFÍA

ACEITUNO, Canal Vicente, Seguridad de la Información, Luces, México, 1996.

ALVARADO, Andrés y HERNÁNDEZ, Ricardo, Informática en Administración, Trillas, 1ª. Edición, México, 1992.

ECHENIQUE, García José Antonio, Auditoría en Informática, Mc Graw Hill, 1ª. Edición, México, 1990.

FREEDMAN, Alan, Diccionario de Computación, Mc Graw Hill, 7ª. Edición, México, 1996.

HERNANDEZ, Jiménez Ricardo, Administración de la función de Informática, Trillas, 4ª. Edición, México, 1994.

KENDALL, Kenneth E. y KENDALL, Julie, Análisis y Diseño de Sistemas, Prentice Hall, 1ª. Edición, México, 1991.

MORA, José Luis y MOLINO, Enzo, Introducción a la Informática, Trillas, 4ª. Edición, México, 1978.

PIATTINI, Velthuis Mario G. y NAVARRO, Emilio del Peso, Auditoría Informática, ALFAOMEGA RA-MA, 2ª. Edición, México, 2001

RIOS, Szalay Adalberto, Orígenes y Perspectivas de la Administración, Trillas, 2ª. Edición, México, 1990.

TERRY, George R., Principios de Administración, CECSA, 1ª. Edición, México, 1991.

VÁZQUEZ, Trujillo César R., Introducción a las Ciencias Computacionales, Universidad de Orizaba, México, 1996.

Auditoría Informática y Sistemas de Información
Dirección electrónica: http://www.auditoriasistemas.com/

Diccionario de la lengua española
Dirección electrónica: http://www.rae.es/

Enciclopedia Libre Wikipedia
Dirección electrónica: http://es.wikipedia.org/

Enciclopedia Virtual Informática
Dirección electrónica: http://www.terra.es/personal/lermon/esp/enciclo.htm

Revista informática
Dirección electrónica: http://www.informatica.cl/

SANS Institute – Network, Security, Computer, Audit Information & Training
Dirección electrónica: http://www.sans.org/

Seguridad Corporativa
Dirección electrónica: www.seguridadcorporativa.org

Soluciones de Seguridad Informática
Dirección electrónica: http://www.cybsec.com/

Auditoría de Seguridad Informática – Cuestionarios
Dirección electrónica:
http://www.upseros.com/fotocopiadora/ficheros/auditoria%20informatica-municipalidad%20moquegua.pdf

Seguridad de la Información
Dirección electrónica:
http://www.segu-info.com.ar/logica/seguridadlogica.htm

Seguridad en la Red – Listado de puertos usados por troyanos
Dirección electrónica: http://www.seguridadenlared.org/es/index5esp.html

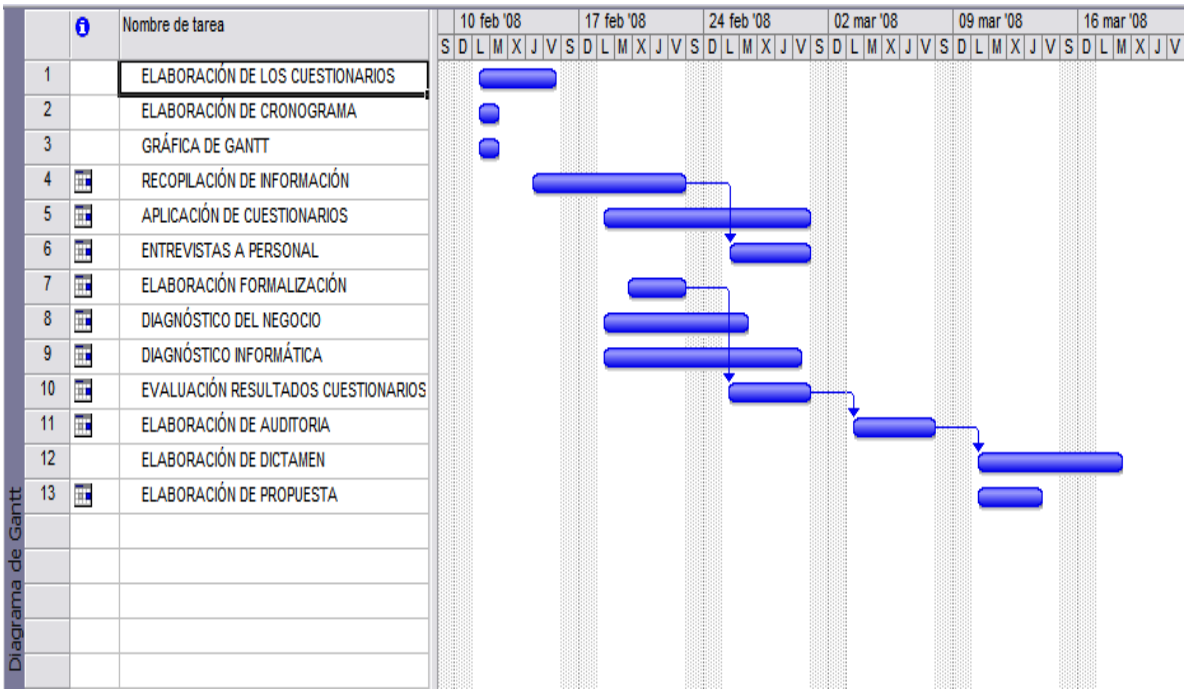
ANEXOS

CRONOGRAMA DE ACTIVIDADES (Anexo1)

PROGRAMA DE AUDITORIA		
EMPRESA: C.F.E. Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago Departamento de Control de Gestión e Informática	**FECHA:** 18/02/08 al 14/03/08	**NO.HOJA:** 1
FASE	**ACTIVIDAD**	**HORAS ESTIMADAS**
I. VISITA PRELIMINAR	•Solicitud de Manuales y Documentaciones. •Elaboración de los cuestionarios. •Recopilación de la información organizacional: estructura orgánica, recursos humanos, etc**.** •Elaboración de Formalización.	8 Hrs.
II. DESARROLLO DE LA AUDITORIA	•Aplicación de cuestionarios al personal. •Entrevistas al personal. •Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. •Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades. •Evaluación de los Recursos Humanos: desempeño, capacitación, condiciones de trabajo, recursos en materiales y financieros mobiliario y equipos. •Evaluación de los sistemas: relevamiento de Hardware y Software, evaluación del diseño lógico y del desarrollo del sistema. •Evaluación del Proceso de Datos y de los Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.	32 Hrs.

III. REVISION	.•Revisión de los papeles de trabajo. .•Determinación del Diagnostico e Implicancias. .•Elaboración del Borrador.	16 Hrs.
IV. INFORME Y PROPUESTA	.•Elaboración y presentación del Informe**.** •Propuesta.	8 Hrs.

GRÁFICA DE GANTT (Anexo2)



FORMALIZACIÓN (Anexo3)

ESCUELA DE INFORMATICA UCV

Uruapan, Michoacán a 22 de Febrero del 2008.

ING. ALBERTO PALOMINO VÁZQUEZ
Jefe del depto. de Control de Gestión e Informática

Estimado Ing. Alberto Palomino Vázquez, la presente pretende proponer los términos que regularán los compromisos asumidos.

Actualmente la Seguridad Informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca en la aparición de nuevas amenazas en los sistemas informáticos.

Por ello, el departamento de Control de Gestión e Informática está en el deber y en la responsabilidad de consagrar tiempo y recursos suficientes para asegurar que los activos de información estén suficientemente protegidos. Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

El objetivo es realizar una investigación sobre seguridad informática al departamento de Control de Gestión e Informática de la Subgerencia Regional de Generación Hidroeléctrica Balsas Santiago C.F.E. como parte del caso práctico de la tesis para obtener el título de Licenciado en Informática.

La tarea consistirá en la realización de una revisión de la información sobre cuestiones de seguridad en los aspectos: físico, lógico, en el personal, desarrollo de aplicaciones, producción, datos, comunicaciones y redes, planes de contingencia y continuidad. Una vez concluida dicha investigación y sujeto a las evidencias reunidas, se elaborará un reporte final con las observaciones pertinentes, para lo cual se utilizará toda la información recopilada con la colaboración por parte de los empleados y funcionarios de la empresa, teniendo en cuenta las limitaciones de su acceso y su confidencialidad.

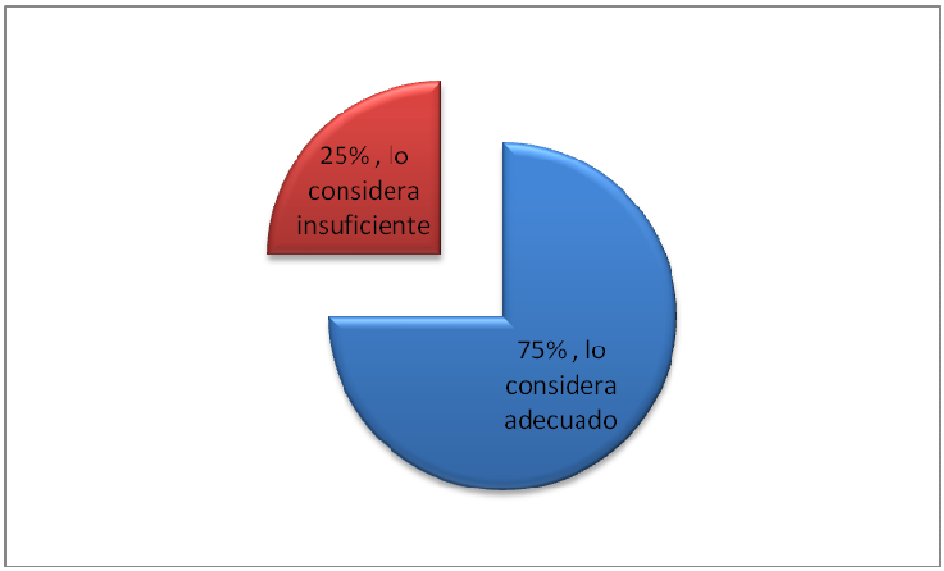
En caso de existir acuerdo respecto de las condiciones establecidas en esta carta, firme, por favor una copia y devuélvala para que procedamos a su archivo.

Lo saluda atentamente: Nora Lilia Solorio Nava.

ING. ALBERTO PALOMINO VÁZQUEZ
Jefe del depto. de Control de Gestión e Informática

GRÁFICA 1

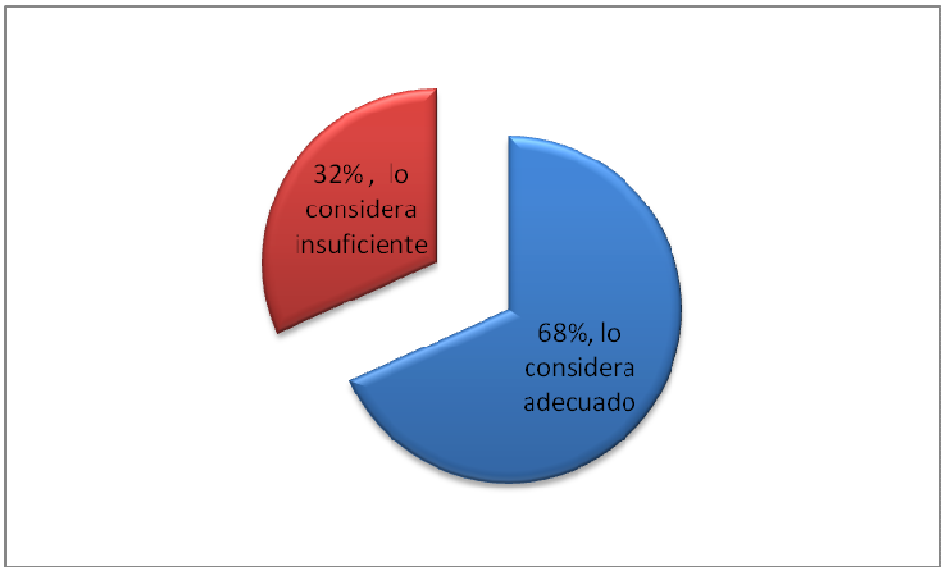
Personal que considera adecuada la seguridad física del departamento de informática.



Fuente: Encuesta directa febrero 2008

GRÁFICA 2

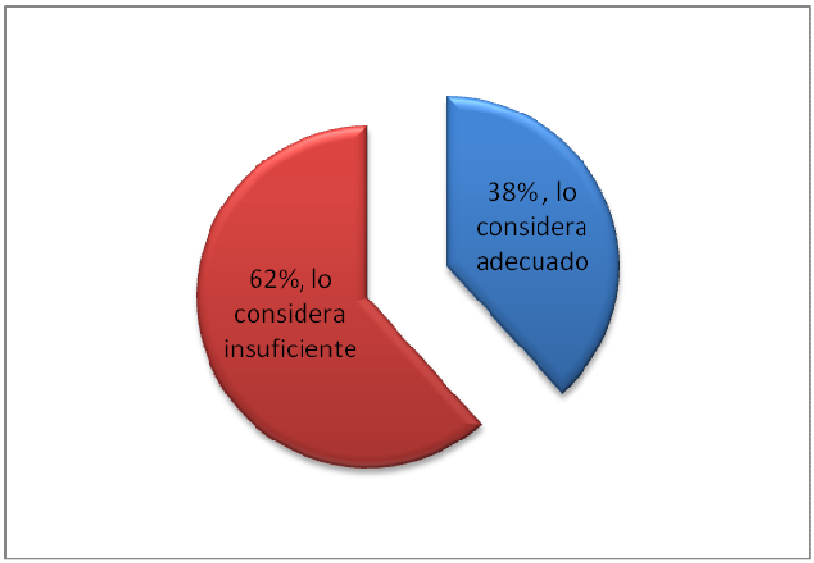
Personal que considera adecuada la seguridad lógica del departamento de informática.



Fuente: Encuesta directa febrero 2008

GRÁFICA 3

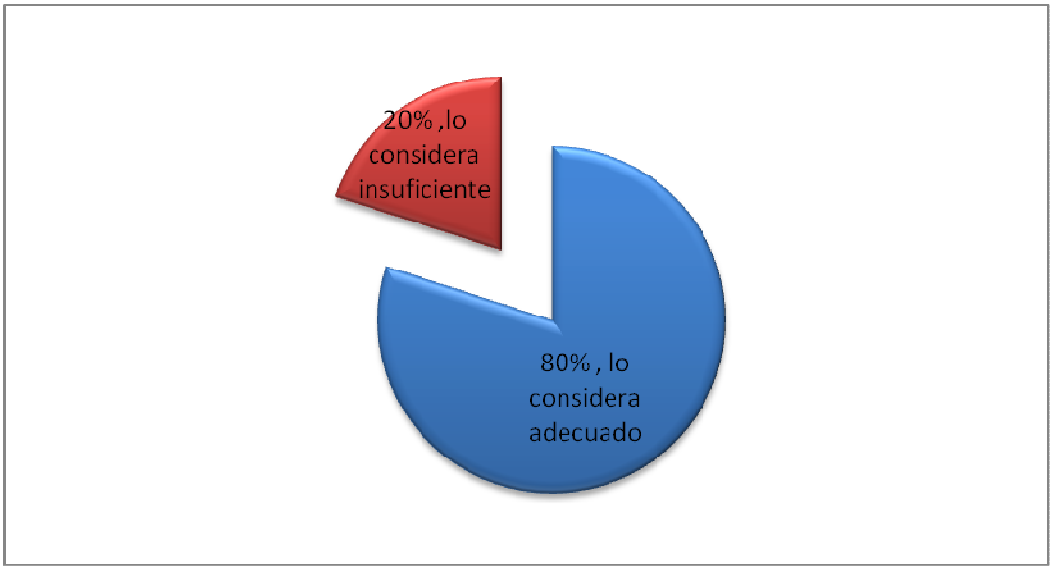
Personal que considera la seguridad en el desarrollo de aplicaciones como un riesgo.



Fuente: Encuesta directa febrero 2008

GRÁFICA 4

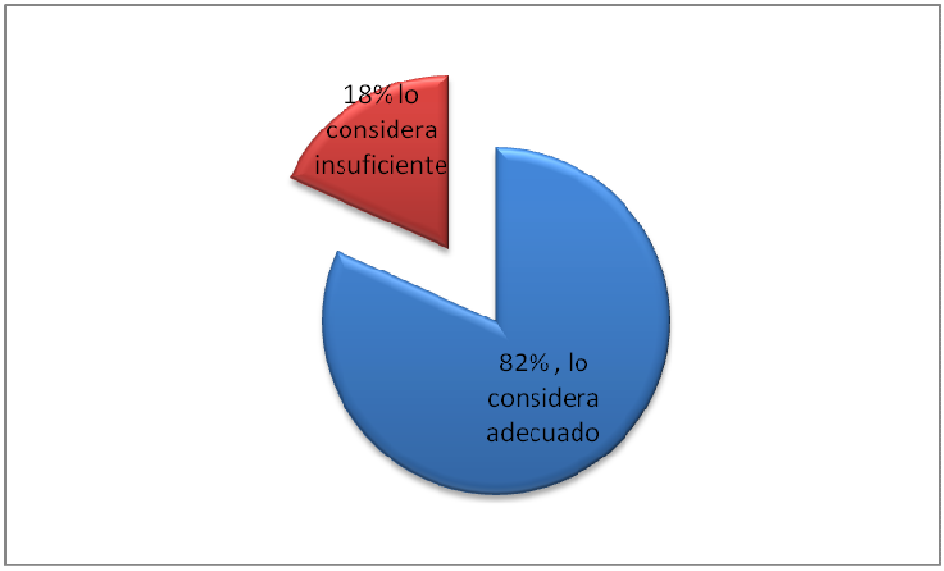
Personal que considera que el mantenimiento es adecuado.



Fuente: Encuesta directa febrero 2008

GRÁFICA 5

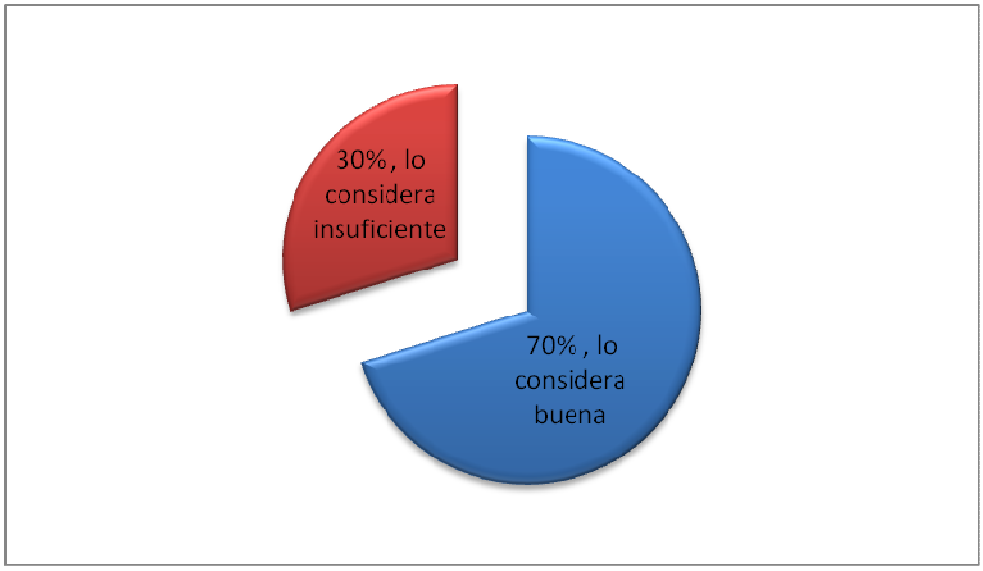
Personal que considera adecuada la Seguridad de Base de Datos.



Fuente: Encuesta directa febrero 2008

GRÁFICA 6

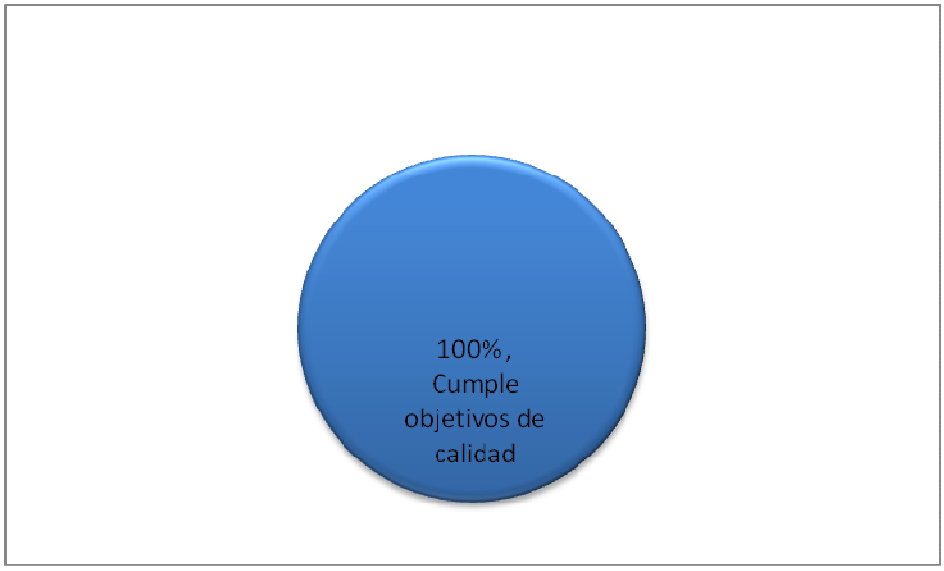
Personal que considera adecuada la seguridad de redes y comunicaciones.



Fuente: Encuesta directa febrero 2008

GRÁFICA 7

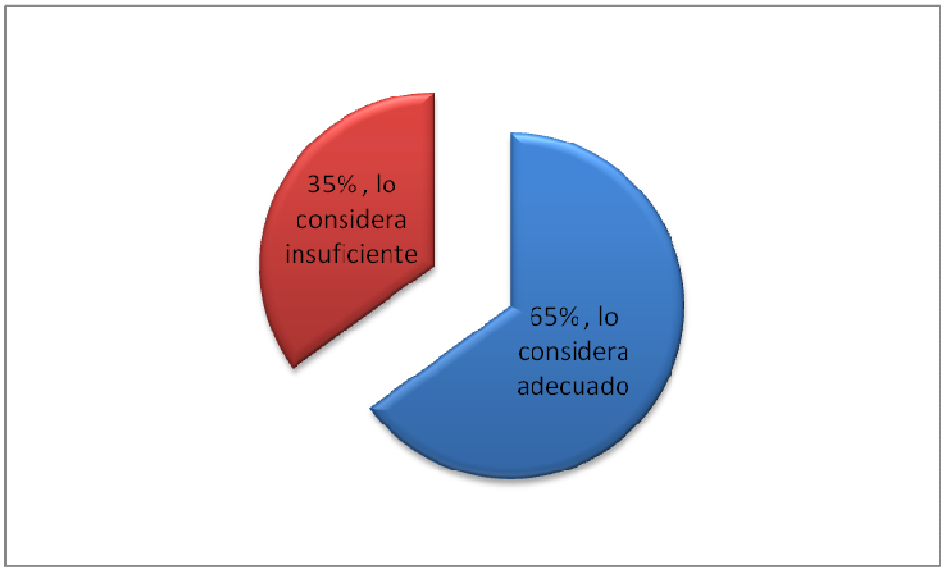
Personal que cumple los objetivos de calidad de la empresa.



Fuente: Encuesta directa febrero 2008

GRÁFICA 8

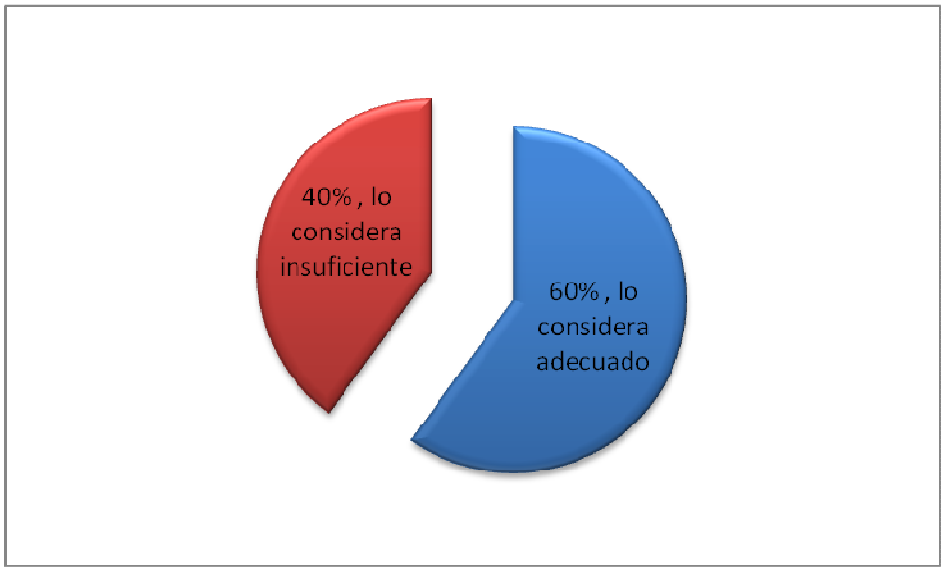
Personal que considera que los parches de antivirus tiene un adecuado funcionamiento dentro del departamento informático y demás departamentos que conforman la subgerencia.



Fuente: Encuesta directa febrero 2008

GRÁFICA 9

Personal de subgerencia que considera adecuada la función del departamento de informática.



Fuente: Encuesta directa febrero 2008