La auditoría informática como herramienta para el aseguramiento de los sistemas de información

Autor: Jessica Infante Esquivel

Tesina presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

" LA AUDITORIA INFORMATICA COMO HERRAMIENTA PARA EL ASEGURAMIENTO DE LOS SISTEMAS DE INFORMACIÓN "

TESINA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:

Jessica Infante Esquivel

No. DE ACUERDO 952006 CLAVE 16PSU0014Q

ASESOR DE TESINA

M.A. Ing. Sergio Francisco Barraza Ibarra

MORELIA, MICH., MEXICO. ABRIL 2004

DEDICATORIAS

Dedico mi tesina a **DIOS** por permitirme lograr esta meta, por dejarme llegar hasta este momento de mi vida y por ser la luz que ilumina mi camino.

A mis papás, **YOLANDA ESQUIVEL** y **ARTURO INFANTE** por su infinito apoyo, confianza y por ser más que mis padres mis amigos, gracias por todo, porque sin ustedes este sueño no se hubiera convertido en realidad. **LOS QUIERO MUCHO.**

A mi hermana **JOSCELINE** por estar a mi lado en todos y cada uno de los momentos de mi vida, por ser mi ejemplo a seguir y mi compañera fiel en esta vida.

A mi asesor **ING. SERGIO FRANCISCO BARRAZA** por su apoyo y ejemplo durante toda mi formación profesional.

A mi **FAMILIA** porque son y siempre serán una de las bases mas importantes que me impulsan a seguir siempre adelante; especialmente **LILIA ESQUIVEL Y JOSE HERRERA.**

A mis amigos **MAYRA, SUSANA, MARYSOL, KATIA, HASSEL, EUGENIA, DANIEL, JORGE, OSCAR, ARMANDO** y **MOISES** por todos los momentos compartidos durante este tiempo y porque sin su compañía mi etapa universitaria no hubiera sido la misma.

INDICE

I.- INTRODUCCION

A finales del siglo XX, los Sistemas Informáticos se han constituido en las herramientas más poderosas para conformar uno de los conceptos mas vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la Empresa.

La Informática hoy, forma parte importante de la misión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado gestión de la empresa. La informática no controla propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por lo tanto, debido a la importancia de la Informática en el funcionamiento de una empresa, existe la Auditoria Informática.

El término Auditoria se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; pero el concepto de Auditoria es mucho más que esto. **Es un examen crítico que se realiza con el fin de evaluar la eficacia y la eficiencia de una sección, un organismo, una entidad, etc.**

La palabra Auditoria proviene del Latin auditorius, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír; de esto se deduce que la auditoria es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad que es auditada y persigue el fin de evaluar y mejorar la eficacia y la eficiencia de una sección o de un organismo.

Los principales objetivos que constituyen a la Auditoria Informática son el control de la función Informática, el análisis de la eficiencia de los Sistemas Informáticos, la verificación del cumplimiento de la normativa general de la

empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

Para la realización de una Auditoria Informática eficaz se debe entender a la empresa en su más amplio sentido, ya que una Universidad, una dependencia o un Hospital son tan empresas como una sociedad anónima o institución publica. Todos utilizan la Informática para tratar sus negocios de forma rápida y eficiente con el fin de obtener beneficios económicos y de costos.

Los Sistemas Informáticos están sometidos a un control correspondiente; la importancia de llevar el control de esta herramienta se puede deducir de varios aspectos, a continuación se presentan algunos:

- ⇒ Las computadoras y los centros de proceso de Datos se convirtieron en blancos apetecibles para delincuencia, terrorismo y espionaje. En este caso interviene la Auditoria Informática de Seguridad.
- ⇒ Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus sistemas informático, con la posibilidad de que se provoque un efecto cascada y afecte aplicaciones independientes. En este caso interviene la Auditoria informática de los datos.
- ⇒ Un Sistema Informático mal diseñado puede convertirse en una herramienta muy peligrosa para la empresa, debido a que las máquinas obedecen ciegamente a las órdenes recibidas y el funcionamiento de la empresa esta determinada por computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un software y un hardware mal diseñados.

Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la **Auditoria Informática.**

II.- ANTECEDENTES

Existe la evidencia de que alguna especie de auditoria se practicó en tiempos remotos. El hecho de que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone en manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrollo el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoria como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el periodo de mandato de Ley "Un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude". También reconocía"Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas". Desde 1862 hasta 1905, la profesión de la auditoria creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. En Inglaterra se siguió haciendo hincapié en cuanto a la detección del fraude como objetivo primordial para la auditoria. En 1912 se dijo:

Los objetivos primordiales de la auditoria como tal eran:

- ⇒ Detección y prevención del fraude.
- ⇒ Detección y prevención de errores;

Sin embargo en los años subsecuentes hubo un cambio decisivo en la demanda y el servicio, y los objetivos de la auditoria cambiaron a ser:

⇒ Cerciorarse de la condición actual y de las ganancias de una empresa.

⇒ La detección y prevención del fraude siendo este un objetivo menos.

Paralelamente al crecimiento de la auditoria independiente en los Estados Unidos, se desarrollaba la auditoria interna y de Gobierno, lo que entro a formar parte del campo de la auditoria. La auditoria gubernamental fue oficialmente reconocida en 1921 cuando el Congreso de los Estados Unidos estableció la Oficina General de contabilidad.

Los trascendentales cambios operados en el mundo moderno, caracterizados por su incesante desarrollo; la acelerada Globalización de la Economía, la acentuada dependencia que incorpora en alto nivel la información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las practicas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoria, en particular a la Auditoria Interna.

Practicar auditorias en una organización en la que el éxito de su gestión depende, como factor crítico, de la eficiente administración de la información y la Tecnología de Información, en la que los sistemas de gestión y contable han alcanzado un desarrollo tan notable, demanda la introducción de una concepción muy diferente a la que primó a esta disciplina durante décadas. Tal concepción demanda, la participación inexcusable de la tecnología como herramienta, permitiéndole evolucionar al ritmo de las transformaciones incorporadas a la estructura del registro y del control interno y muy especialmente, para evaluar mediante auditorias a las Tecnologías de Información, los procedimientos de control específicos, dentro de ámbito de su soporte tecnológico, que a su vez garantice una información objetiva sobre el

grado de cumplimiento de las políticas y normativas establecidas por la organización para lograr sus objetivos.

La Auditoria Informática tiene como principal objetivo, evaluar el grado de efectividad de las Tecnologías de Información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la Organización, su grado de Eficacia, Eficiencia, Confiabilidad e Integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

La Auditoria Interna, en su desempeño, tiene también la responsabilidad de velar por el adecuado empleo y utilización de los recursos informáticos y por el cumplimiento de la misión que a éstos le ha asignado la Organización.

Todo esto nos conduce, a la inexplicable necesidad de practicar "Auditorias Informáticas", a partir de un conjunto de técnicas y procedimientos que evalúen los controles internos específicos de los sistemas de información; en consecuencia se determina que conceptualmente, no es dependiente ni evoluciona desde auditoria convencional; sus puntos de partida son esencialmente diferentes ya que no analiza la corrección o incorrección de cuentas contables, sino que constituye un instrumento de nivel superior para valorar la correcta administración de los recursos de tecnología de información como: Daos, Aplicaciones, Tecnología, Instalaciones, y Personal para valorar la efectividad de la información que requiere la Organización.

III.- OBJETIVO GENERAL

El presente trabajo tiene como finalidad la recopilación de diferentes técnicas de Auditoria informática en términos generales y su aplicación específica que conducirá a la garantizar la seguridad de la información dentro de las organizaciones.

3.1 OBJETIVOS PARTICULARES

⇒ Identificar las diferentes metodologías de la Auditoria Informática.

⇒ Conocer los términos y conceptos que son aplicados en la Auditoria Informática.

⇒ Identificar la relación existente entre la Auditoria Informática y la seguridad de la información.

⇒ Entender la importancia de la información; así como de su seguridad dentro de las organizaciones.

⇒ Conocer las características y finalidad de las Políticas de Seguridad Informática.

IV.- AUDITORIA INFORMATICA

4.1 AUDITORIA

La Auditoria nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico – financiera.

La función auditora debe ser absolutamente independiente: no tiene carácter ejecutivo. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoria contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antes mencionadas; estas sugerencias plasmadas en el Informe final, reciben el nombre de recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. El nivel técnico del auditor es a veces insuficiente, dada la gran complejidad de los sistemas, unidos a plazos demasiado breves de los que suelen disponer para realizar sus labor.

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados Check List, son guardados celosamente por empresas auditoras, ya que son activos importantes de su actividad. Los Check List tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicados se puede llegar a obtener resultados distintos a los esperados por la empresa auditora. Los cuestionarios pueden explicar como ocurren los hechos pero no porqué ocurren.

El auditor solo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificas la situación analizada por el mismo.

4.2 AUDITORIA INTERNA Y AUDITORIA EXTERNA

La auditoria interna es la realizada con recursos materiales y personas que pertenecen a la empresa auditada. Los empleados que realizan esta tarea son remunerados económicamente. La auditoria interna existe por expresa decisión de la Empresa, o sea, que puede optar por su disolución en cualquier momento.

Por otro lado, la auditoria externa por personas afines a la empresa auditada; es siempre remunerada. Se presupone una mayor objetividad que en la Auditoria Interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoria informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoria externa, las cuales no son tan perceptibles como en las auditorias convencionales. La auditoria interna tiene la ventaja de que puede actuar periódicamente realizando Revisiones globales, como parte de su plan anual y de su actividad normal. Los auditados conocen estos planes y se habitúan a las Auditorias, auditorias, especialmente cuando las consecuencias de las Recomendaciones habidas benefician su trabajo.

En una empresa, los responsables de Informática escuchas, orientan e informan sobre las posibilidades técnicas y los costos de tal sistema. El área de informática trata de satisfacer lo más adecuadamente posible aquellas necesidades. La empresa necesita controlar su informática y ésta necesita que su propia gestión este sometida a los mismos procedimientos y estándares que el resto de la empresa.

En cuanto a empresas se refiere, solamente las más grandes pueden poseer una Auditoria propia y permanente, mientras el resto acuden a las auditorias externas. Puede ser que algún profesional informático sea trasladado desde su puesto de trabajo a la Auditoria Interna de su empresa cuando ésta existe.

Una empresa o institución que posee una auditoria interna puede y debe en ocasiones contratar servicios de auditoria externa. Las razones para hacerlo suelen ser:

- ⇒ Necesidad de auditar una materia de gran especialización, para la cual los servicios propios no están suficientemente capacitados.
- ⇒ Contrastar algún informe interno con el que resulte del externo, en aquellos supuestos de emisión interna de graves recomendaciones que chocan con la opinión generalizada de la propia empresa.
- ⇒ Aunque la auditoria interna sea independiente del Departamento de Sistemas, sigue siendo la misma empresa, por lo tanto, es necesario que se realicen auditorias externas como para tener una visión desde fuera de la empresa.

La auditoria informática, tanto externa como interna, debe ser una actividad exenta de cualquier contenido "político" ajeno a la propia estrategia y política general de la empresa. La función auditora puede actuar de oficio, por iniciativa del propio órgano, o a instancias de parte, esto es, por encargo de la dirección o cliente.

4.3 ALCANCE DE LA AUDITORIA INFORMATICA

El alcance ha de definir con precisión el entorno y los limites en que va a desarrollarse la auditoria informática, se complementa con los objetivos de ésta. El alcance se ha de figurar en el informe final, de modo que quede perfectamente

determinado no solamente hasta que punto se ha llegado, sino cuales materias han sido omitidas.

4.4 CARACTERISTICAS DE LA AUDITORIA INFORMATICA

La información de la empresa y para la empresa, siempre importante, se ha convertido en un activo real de la misma, como sus stokcks o materias primas si las hay. Por consecuencia, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoria De Inversión Informática.

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular; a ello se debe la existencia de la Auditoria de la Seguridad Informática en general, o a la auditoria de Seguridad de alguna de sus áreas, como pudiera ser Desarrollo o Técnica de sistemas

Cuando se producen cambios estructurales en la Informática, se reorganiza de alguna forma su función: se esta en el campo de la Auditoria de Organización Informática.

Estos tres tipos de auditorias engloban a las actividades auditoras que se realizan en una auditoria parcial. De otra manera; cuando se realiza una auditoria del área de desarrollo de proyectos de la informática de una empresa, es porque en ese proceso existen, demás de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

4.5 SINTOMAS DE NECESIDAD DE UNA AUDITORIA INFORMATICA

Las empresas acuden a las auditorias externas cuando existen síntomas bien perceptibles de debilidad. Estos síntomas pueden agruparse en clases:

⇒ Síntomas de descoordinación y desorganización:
- No coinciden los objetivos de la informática de la compañía y de la propia compañía.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

⇒ Síntomas de mala imagen e insatisfacción de los usuarios:
- No se atienden a las peticiones de cambios de los usuarios.
- No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que esta abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos.

⇒ Síntomas de debilidades económico – financiero
- Incremento desmesurado de costos.
- Necesidad de justificación de inversiones informáticas; la empresa no esta absolutamente convencida de tal necesidad y decide contrastar opiniones.
- Desviaciones presupuestarias significativas.

⇒ Síntomas de inseguridad: evaluación de nivel de riesgos
- Seguridad Lógica
- Seguridad Física
- Confidencialidad

- Continuidad del servicio. Es un concepto aun mas importante que la Seguridad. Establece estrategias de continuidad entre fallos mediante Planes de Contingencia totales y locales.
- Centro de proceso de datos fuera de control.

Cada área específica puede ser auditada desde los siguientes criterios generales:

⇒ Desde su propio funcionamiento interno.
⇒ Desde el apoyo que recibe de la Dirección.
⇒ Desde la perspectiva de los usuarios, destinatarios reales de la informática.
⇒ Desde le punto de vista de la seguridad que ofrece la informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

4.6 OBJETIVO FUNDAMENTAL DE LA AUDITORIA INFORMATICA

Operatividad

La operatividad es una función de mínimos que consiste en que la organización y las máquinas funcionen, aunque sea de una forma mínima. No es admisible detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoria debe iniciar su actividad cuando los Sistemas estén operando, es el principal objetivo el de mantener tal situación. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los Sistemas ha de constituir entonces la principal preocupación del auditor informático.

4.7 AUDITORIA INFORMATICA DE DESARROLLO DE PROYECTOS O APLICACIONES

La función de Desarrollo es una evolución del llamado Análisis y Programación de Sistemas y Aplicaciones. A su vez, engloba muchas áreas, tantas como sectores informatizables tiene la empresa. Muy escuetamente, una aplicación recorre las siguientes fases:

⇒ Prerrequisitos del Usuario (único o plural) y del entorno
⇒ Análisis funcional
⇒ Diseño
⇒ Análisis Orgánico (preprogramación y Programación)
⇒ Pruebas
⇒ Entrega a explotación alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno. Finalmente, la auditoria deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Una auditoria de aplicaciones pasa seguramente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las futuras posibles ampliaciones de la aplicación y el fácil mantenimiento de las mismas.
2. Control interno de las aplicaciones: se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo.

a. Estudio de vialidad de la aplicación; importante para aplicaciones largas, complejas y caras.
b. Definición lógica de la aplicación.
c. Desarrollo técnico de la aplicación; se verificará que sea ordenado y correcto.
d. Diseño de programas.
e. Documentación; cumplirá la Normativa establecida en la instalación.
f. Métodos de pruebas; se realizaran de acuerdo a las normas de instalación.
g. Documentación.
h. Equipo de programación.

3. Satisfacción de los usuarios: una aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicito. La presencia e intervención del usuario proporciona grandes ventajas posteriores, ya que evitara reprogramaciones y disminuirá el mantenimiento de la aplicación.
4. Control de procesos y ejecuciones de programas críticos: el auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones. Si los programas fuente y los programas módulo no coincidieran se podría provocar, desde errores que producirían graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informativo, etc.

4.8 AUDITORIA INFORMATICA DE SISTEMAS

Se ocupa de analizar la actividad que se conoce como Técnica de Sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las Comunicaciones, Líneas y Redes de

las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de Sistemas.

Sistemas Operativos:

Engloba los Subsistemas de Teleproceso, Entrada/Salida, etc. Debe verificarse en primer lugar que los Sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera. El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de Software Básico adquiridos por la instalación y determinadas versiones de aquellas.

Software Básico:

Es fundamental para el auditor conocer los productos de software básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente. En cuanto al Software desarrollado por el personal informático de la empresa, el auditor debe verificar que éste no agreda ni condicione al Sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

Tunning:

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los Subsistemas y del Sistema en su conjunto. Las acciones de tunning deben diferenciarse de los controles habituales que realiza el personal Técnico de Sistemas. El tunning posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

⇒ Cuando existe sospecha de deterioro del comportamiento parcial o general del Sistema

⇒ De modo sistemático y periódico, por ejemplo cada 6 meses. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor deberá conocer el número de Tunning realizados en el último año, así como sus resultados. Deberá analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

Optimización de los Sistemas y Subsistemas:

Técnica de Sistemas que debe realizar acciones permanentes de optimización como consecuencia de la realización de tunnings preprogramados o específicos. El auditor verificará que las acciones de optimización fueron efectivas y no comprometieron la Operatividad de los Sistemas ni el plan crítico de producción diaria.

Administración de Base de Datos:

El diseño de las Bases de Datos, sean relaciones o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general desarrollada en el ámbito de Técnica de Sistemas, y de acuerdo con las áreas de Desarrollo y usuarios de la empresa. Al conocer el diseño y arquitectura de éstas por parte de Sistemas, se les encomienda también su administración. Los auditores de Sistemas han observado algunas disfunciones derivadas de la relativamente escasa experiencia que Técnica de Sistemas tiene sobre la problemática general de los usuarios de Bases de Datos.

Investigación y Desarrollo:

Como empresas que utilizan y necesitan de informáticas desarrolladas, saben que sus propios efectivos están desarrollando Aplicaciones y utilidades que, concebidas inicialmente para su uso interno, pueden ser susceptibles de adquisición por otras empresas, haciendo competencia a las Compañías del ramo. La auditoria informática deberá cuidar de que la actividad de

Investigación y Desarrollo no interfiera ni dificulte las tareas fundamentales internas.

4.9 Auditoria de la Seguridad informática

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional. Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus. El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

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

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

La seguridad informática se la puede dividir como Área General y como Área Especifica. Así, se podrán efectuar auditorias de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorias de la Seguridad de un área informática determinada – Seguridad Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica.

El sistema integral de seguridad debe comprender:

- ⇒ Elementos administrativos
- ⇒ Definición de una política de seguridad
- ⇒ Organización y división de responsabilidades
- ⇒ Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- ⇒ Prácticas de seguridad del personal
- ⇒ Elementos técnicos y procedimientos
- ⇒ Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- ⇒ Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- ⇒ El papel de los auditores, tanto internos como externos
- ⇒ Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoria Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan.

4.10 ANEXO DE AUDITORIA INFORMATICA Y CUESTIONARIOS

La auditoria informática deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoria en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

ENTREVISTA A USUARIOS

La entrevista se deberá llevar a cabo para comprobar datos proporcionados y la situación de la dependencia en el departamento de Sistemas de Información.

Su objeto es conocer la opinión que tienen los usuarios sobre los servicios proporcionados, así como la difusión de las aplicaciones de la computadora y de los sistemas en operación.

Las entrevistas se deberán hacer, en caso de ser posible, a todos los usuarios o bien en forma aleatoria a algunos de los usuarios, tanto de los más importantes como de los de menor importancia, en cuanto al uso del equipo.

Desde el punto de vista del usuario los sistemas deben:

- Cumplir con los requerimientos totales del usuario.
- Cubrir todos los controles necesarios.
- No exceder las estimaciones del presupuesto inicial.
- Serán fácilmente modificables.

Para que un sistema cumpla con los requerimientos del usuario, se necesita una comunicación completa entre usuarios y responsable del desarrollo del sistema.

A continuación se presenta una guía de cuestionario para aplicarse durante la entrevista con el usuario.

1. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?.-
Si ( ) No ( )
¿Por que? _____

2. ¿Cómo considera usted, en general, el servicio proporcionado por el Departamento de Sistemas de Información?
Deficiente ( )
Aceptable ( )
Satisfactorio ( )
Excelente ( )
¿Por que? _____

3. ¿Cubre sus necesidades el sistema que utiliza el departamento de cómputo?

No las cubre ( )

Parcialmente ( )

La mayor parte ( )

Todas ( )

¿Por que? _____

4. ¿Hay disponibilidad del departamento de cómputo 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 trabajadores solicitados al departamento de cómputo?

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 no Utiliza?

12. De aquellos que no utiliza ¿por que razón los recibe?

13. ¿Que sugerencias presenta en cuanto a la eliminación de reportes modificación, fusión, división de reporte?

14. ¿Se cuenta con un manual de usuario por Sistema?

SI ( ) NO ( )

15. ¿Es claro y objetivo el manual del usuario?

SI ( ) NO ( )

16. ¿Que opinión tiene el manual?

NOTA: Pida el manual del usuario para evaluarlo.

17. ¿Quién interviene de su departamento en el diseño de sistemas?

18. ¿Que sistemas desearía que se incluyeran?

19. Observaciones:

CONTROLES

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo cuidado que los demás inventarios de la organización, por lo cual se debe tener presente:

a) La responsabilidad de los datos es compartida conjuntamente por alguna función determinada y el departamento de cómputo.

b) Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

c) Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.

d) Se deben relacionar los elementos de los datos con las bases de datos donde están almacenados, así como los reportes y grupos de procesos donde son generados.

CONTROL DE LOS DATOS FUENTE Y MANEJO CIFRAS DE CONTROL

La mayoría de los Delitos por computadora son cometidos por modificaciones de datos fuente al:

- Suprimir u omitir datos.

- Adicionar Datos.
- Alterar datos.
- Duplicar procesos.

to es de suma importancia en caso de equipos de cómputo que cuentan con temas en línea, en los que los usuarios son los responsables de la captura y odificación de la información al tener un adecuado control con señalamiento e responsables de los datos (uno de los usuarios debe ser el único responsable e determinado dato), con claves de acceso de acuerdo a niveles.

primero que se debe evaluar es la entrada de la información y que se tengan s cifras de control necesarias para determinar la veracidad de la información, ara lo cual se puede utilizar el siguiente cuestionario:

Indique el porcentaje de datos que se reciben en el área de captación
Indique el contenido de la orden de trabajo que se recibe en el área de aptación de datos:

Número de folio ( ) Número(s) de formato(s) ( )
Fecha y hora de Nombre, Depto. ( )
Recepción ( ) Usuario ( )
Nombre del documento ( ) Nombre responsable ( )
Volumen aproximado Clave de cargo
de registro ( ) (Número de cuenta) ( )
Número de registros ( ) Fecha y hora de entrega de
Clave del capturista ( ) documentos y registros captados ( )
Fecha estimada de entrega ( )

Indique cuál(es) control(es) interno(s) existe(n) en el área de captación de atos:

Firmas de autorización ( )
Recepción de trabajos ( ) Control de trabajos atrasados ( )
Revisión del documento ( ) Avance de trabajos ( )
fuente legibilidad, verificación de datos completos, etc.) ( )

Prioridades de captación ( ) Errores por trabajo ( )

Producción de trabajo ( ) Corrección de errores ( )

Producción de cada operador ( ) Entrega de trabajos ( )

Verificación de cifras Costo Mensual por trabajo ( )

de control de entrada con las de salida. ( )

4. ¿Existe un programa de trabajo de captación de datos?

a) ¿Se elabora ese programa para cada turno?

Diariamente ( )

Semanalmente ( )

Mensualmente ( )

b) La elaboración del programa de trabajos se hace:

Internamente ( )

Se les señalan a los usuarios las prioridades ( )

c) ¿Que acción(es) se toma(n) si el trabajo programado no se recibe a tiempo?

5. ¿Quién controla las entradas de documentos fuente?

6. ¿En que forma las controla?

7. ¿Que cifras de control se obtienen?

8. ¿Que documento de entrada se tienen?

9. ¿Se anota que persona recibe la información y su volumen?

SI NO

10. ¿Se anota a que capturista se entrega la información, el volumen y la hora?

SI NO

11. ¿Se verifica la cantidad de la información recibida para su captura?

SI NO

12. ¿Se revisan las cifras de control antes de enviarlas a captura?

SI NO

13. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?

SI NO

14. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?

15. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?

16. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?

17. ¿Existe un registro de anomalías en la información debido a mala codificación?

18. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?

19. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?

20. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?
21. ¿Se controlan separadamente los documentos confidenciales?
22. ¿Se aprovecha adecuadamente el papel de los listados inservibles?
23. ¿Existe un registro de los documentos que entran a capturar?
24. ¿Se hace un reporte diario, semanal o mensual de captura?
25. ¿Se hace un reporte diario, semanal o mensual de anomalías en la información de entrada?

26. ¿Se lleva un control de la producción por persona?

27. ¿Quién revisa este control?

28. ¿Existen instrucciones escritas para capturar cada aplicación o, en su defecto existe una relación de programas?

CONTROL DE OPERACIÓN

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

El objetivo del presente ejemplo de cuestionario es señalar los procedimientos e instructivos formales de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.

1. ¿Existen procedimientos formales para la operación del sistema de computo?
SI ( ) NO ( )

2. ¿Están actualizados los procedimientos?

SI ( ) NO ( )

3. Indique la periodicidad de la actualización de los procedimientos:

Semestral ( ) Anual ( ) Cada vez que haya cambio de equipo ( )

4. Indique el contenido de los instructivos de operación para cada aplicación:

Identificación del sistema ( )

Identificación del programa ( )

Periodicidad y duración de la corrida ( )
Especificación de formas especiales ( )
Especificación de cintas de impresoras ( )
Etiquetas de archivos de salida, nombre, ( )
archivo lógico, y fechas de creación y expiración
Instructivo sobre materiales de entrada y salida ( )
Altos programados y la acciones requeridas ( )
Instructivos específicos
a los operadores en caso de falla del equipo ( )
Instructivos de reinicio ( )
Procedimientos de recuperación para proceso de
gran duración o criterios ( )
Identificación de todos los
dispositivos de la máquina a ser usados ( )

Especificaciones de resultados
(cifras de control, registros de salida por archivo, etc.) ( )

5. ¿Existen órdenes de proceso para cada corrida en la computadora (incluyendo pruebas, compilaciones y producción)?

SI ( ) NO ( )

6. ¿Son suficientemente claras para los operadores estas órdenes?
SI ( ) NO ( )

7. ¿Existe una estandarización de las ordenes de proceso?
SI ( ) NO ( )

8. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que se están autorizados y tengan una razón de ser procesados.

SI ( ) NO ( )

9. ¿Cómo programan los operadores los trabajos dentro del departamento de cómputo?

Primero que entra, primero que sale ( )
se respetan las prioridades, ( )
Otra (especifique) ( )

10. ¿Los retrasos o incumplimiento con el programa de operación diaria, se revisa y analiza?

SI ( ) NO ( )

11. ¿Quién revisa este reporte en su caso?

12. Analice la eficiencia con que se ejecutan los trabajos dentro del departamento de cómputo, tomando en cuenta equipo y operador, a través de inspección visual, y describa sus observaciones.

13. ¿Existen procedimientos escritos para la recuperación del sistema en caso de falla?

14. ¿Cómo se actúa en caso de errores?

15. ¿Existen instrucciones especificas para cada proceso, con las indicaciones pertinentes?

16. ¿Se tienen procedimientos específicos que indiquen al operador que hacer cuando un programa interrumpe su ejecución u otras dificultades en proceso?

17. ¿Puede el operador modificar los datos de entrada?

18. ¿Se prohíbe a analistas y programadores la operación del sistema que programo o analizo?

19. ¿Se prohíbe al operador modificar información de archivos o bibliotecas de programas?

20. ¿El operador realiza funciones de mantenimiento diario en dispositivos que así lo requieran?

21. ¿Las intervenciones de los operadores:

Son muy numerosas? SI ( ) NO ( )
Se limitan los mensajes esenciales? SI ( ) NO ( )
Otras (especifique)_____

22. ¿Se tiene un control adecuado sobre los sistemas y programas que están en operación?
SI ( ) NO ( )
23. ¿Cómo controlan los trabajos dentro del departamento de cómputo?

24. ¿Se rota al personal de control de información con los operadores procurando un entrenamiento cruzado y evitando la manipulación fraudulenta de datos?
SI ( ) NO ( )

25. ¿Cuentan los operadores con una bitácora para mantener registros de cualquier evento y acción tomada por ellos?
Si ( )
por máquina ( )
escrita manualmente ( )
NO ( )
26. Verificar que exista un registro de funcionamiento que muestre el tiempo de paros y mantenimiento o instalaciones de software.

27.¿Existen procedimientos para evitar las corridas de programas no autorizados?
SI ( ) NO ( )

28. ¿Existe un plan definido para el cambio de turno de operaciones que evite el descontrol y discontinuidad de la operación.

29. Verificar que sea razonable el plan para coordinar el cambio de turno.

30. ¿Se hacen inspecciones periódicas de muestreo?
SI ( ) NO ( )

31. Enuncie los procedimientos mencionados en el inciso anterior:

32. ¿Se permite a los operadores el acceso a los diagramas de flujo, programas fuente, etc. fuera del departamento de cómputo?

SI ( ) NO ( )

33. ¿Se controla estrictamente el acceso a la documentación de programas o de aplicaciones rutinarias?
SI ( ) NO ( )
¿Cómo?_____

34. Verifique que los privilegios del operador se restrinjan a aquellos que le son asignados a la clasificación de seguridad de operador.

35. ¿Existen procedimientos formales que se deban observar antes de que sean aceptados en operación, sistemas nuevos o modificaciones a los mismos?
SI ( ) NO ( )

36. ¿Estos procedimientos incluyen corridas en paralelo de los sistemas modificados con las versiones anteriores?
SI ( ) NO ( )

37. ¿Durante cuanto tiempo?

38. ¿Que precauciones se toman durante el periodo de implantación?

39. ¿Quién da la aprobación formal cuando las corridas de prueba de un sistema modificado o nuevo están acordes con los instructivos de operación.

40. ¿Se catalogan los programas liberados para producción rutinaria?

SI ( ) NO ( )

41. Mencione que instructivos se proporcionan a las personas que intervienen en la operación rutinaria de un sistema.

42. Indique que tipo de controles tiene sobre los archivos magnéticos de los archivos de datos, que aseguren la utilización de los datos precisos en los procesos correspondientes.

43. ¿Existe un lugar para archivar las bitácoras del sistema del equipo de cómputo?
SI ( ) NO ( )

44. Indique como está organizado este archivo de bitácora.

- Por fecha ( )
- por fecha y hora ( )
- por turno de operación ( )
- Otros ( )

45. ¿Cuál es la utilización sistemática de las bitácoras?

46. ¿Además de las mencionadas anteriormente, que otras funciones o áreas se encuentran en el departamento de cómputo actualmente?

47. Verifique que se lleve un registro de utilización del equipo diario, sistemas en línea y batch, de tal manera que se pueda medir la eficiencia del uso de equipo.

48. ¿Se tiene inventario actualizado de los equipos y terminales con su localización?
SI ( ) NO ( )

49. ¿Cómo se controlan los procesos en línea?

50. ¿Se tienen seguros sobre todos los equipos? SI ( ) NO ( )

51.¿Conque compañía?
Solicitar pólizas de seguros y verificar tipo de seguro y montos.

52. ¿Cómo se controlan las llaves de acceso (Password)?.

CONTROLES DE SALIDA

1. ¿Se tienen copias de los archivos en otros locales?

2. ¿Dónde se encuentran esos locales?

3. ¿Que seguridad física se tiene en esos locales?

4. ¿Que confidencialidad se tiene en esos locales?

5. ¿Quién entrega los documentos de salida?

6. ¿En que forma se entregan?

7. ¿Que documentos?

8. ¿Que controles se tienen?

9. ¿Se tiene un responsable (usuario) de la información de cada sistema? ¿Cómo se atienden solicitudes de información a otros usuarios del mismo sistema?

10. ¿Se destruye la información utilizada, o bien que se hace con ella?

Destruye ( ) Vende ( ) Tira ( ) Otro _____

CONTROL DE ALMACENAMIENTO MASIVO

El objetivo de este cuestionario es evaluar la forma como se administran los dispositivos de almacenamiento básico de la dirección.

1. Los locales asignados a la cintoteca y discoteca tienen:

- Aire acondicionado ( )
- Protección contra el fuego ( )
- (señalar que tipo de protección)_____
- Cerradura especial ( )
- Otra

2. ¿Tienen la cintoteca y discoteca protección automática contra el fuego?
SI ( ) NO ( )
(señalar de que tipo)_____

3. ¿Que información mínima contiene el inventario de la cintoteca y la discoteca?

Número de serie o carrete ( )
Número o clave del usuario ( )
Número del archivo lógico ( )
Nombre del sistema que lo genera ( )

Fecha de expiración del archivo ( )

Fecha de expiración del archivo ( )

Número de volumen ( )

Otros

4. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?

SI ( ) NO ( )

5. En caso de existir discrepancia entre las cintas o discos y su contenido, se resuelven y explican satisfactoriamente las discrepancias?

SI ( ) NO ( )

6. ¿Que tan frecuentes son estas discrepancias?

_____

7. ¿Se tienen procedimientos que permitan la reconstrucción de un archivo en cinta a disco, el cual fue inadvertidamente destruido?

SI ( ) NO ( )

8. ¿Se tienen identificados los archivos con información confidencial y se cuenta con claves de acceso?

SI ( ) NO ( )

¿Cómo?_____

9. ¿Existe un control estricto de las copias de estos archivos?

SI ( ) NO ( )

10. ¿Que medio se utiliza para almacenarlos?

Mueble con cerradura ( )

Bóveda ( )

Otro (especifique)_____

11. Este almacén esta situado:

En el mismo edificio del departamento ( )

En otro lugar ( )

¿Cual?_____

12. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?

SI ( ) NO ( )

13. ¿Se certifica la destrucción o baja de los archivos defectuosos?

SI ( ) NO ( )

14. ¿Se registran como parte del inventario las nuevas cintas que recibe la biblioteca?

SI ( ) NO ( )

15 ¿Se tiene un responsable, por turno, de la cintoteca y discoteca?

SI ( ) NO ( )

16. ¿Se realizan auditorias periódicas a los medios de almacenamiento?

SI ( ) NO ( )

17. ¿Que medidas se toman en el caso de extravío de algún dispositivo de almacenamiento?

18. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?

SI ( ) NO ( )

19. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?

SI ( ) NO ( )

20. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?

SI ( ) NO ( )

21. ¿Se lleva control sobre los archivos prestados por la instalación?

SI ( ) NO ( )

22. En caso de préstamo ¿Conque información se documentan?

Nombre de la institución a quién se hace el préstamo.

- fecha de recepción ( )
- fecha en que se debe devolver ( )
- archivos que contiene ( )
- formatos ( )
- cifras de control ( )
- código de grabación ( )
- nombre del responsable que los presto ( )
- otros

23. Indique qué procedimiento se sigue en el reemplazo de las cintas que contienen los archivos maestros:

24. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?

SI ( ) NO ( )

25. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?

SI ( ) NO ( )

26. ¿La operación de reemplazo es controlada por el cintotecario?

SI ( ) NO ( )

27. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?

SI ( ) NO ( )

28. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?
SI ( ) NO ( )

29. ¿Estos procedimientos los conocen los operadores?
SI ( ) NO ( )

30. ¿Con que periodicidad se revisan estos procedimientos?
MENSUAL ( ) ANUAL ( )
SEMESTRAL ( ) OTRA ( )

31. ¿Existe un responsable en caso de falla?
SI ( ) NO ( )

32. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?

33. ¿Existe un procedimiento para el manejo de la información de la cintoteca?
SI ( ) NO ( )

34. ¿Lo conoce y lo sigue el cintotecario?
SI ( ) NO ( )

35. ¿Se distribuyen en forma periódica entre los jefes de sistemas y programación informes de archivos para que liberen los dispositivos de almacenamiento?
SI ( ) NO ( )

¿Con qué frecuencia?

CONTROL DE MANTENIMIENTO

Para evaluar el control que se tiene sobre el mantenimiento y las fallas se pueden utilizar los siguientes cuestionarios:

1. Especifique el tipo de contrato de mantenimiento que se tiene (solicitar copia del contrato).

2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de computo?
SI ( ) NO ( )

3. ¿Se lleva a cabo tal programa?
SI ( ) NO ( )

4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?
SI ( ) NO ( )

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?
SI ( ) NO ( )

6. Solicite el plan de mantenimiento preventivo que debe ser proporcionado por el proveedor.-
SI ( ) NO ( )
¿Cual?

8. ¿Cómo se notifican las fallas?

9. ¿Cómo se les da seguimiento?

ORDEN EN EL CENTRO DE CÓMPUTO

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:

Semanalmente ( ) Quincenalmente ( )
Mensualmente ( ) Bimestralmente ( )
No hay programa ( ) Otra (especifique) ( )

2. Existe un lugar asignado a las cintas y discos magnéticos?
SI ( ) NO ( )

3. ¿Se tiene asignado un lugar especifico para papelería y utensilios de trabajo?
SI ( ) NO ( )

4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?
SI ( ) NO ( )

5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?
SI ( ) NO ( )

6. Indique la periodicidad con que se limpian las unidades de cinta:

Al cambio de turno ( ) cada semana ( )
cada día ( ) otra (especificar) ( )

7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?
SI ( ) NO ( )

8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?
SI ( ) NO ( )

9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?

SI ( ) NO ( )

10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO

Esta sección esta orientada a:

a) Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual o de comparar la capacidad instalada con los planes de desarrollo a mediano y lago plazo.

b) Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.

c) Evaluar la utilización de los diferentes dispositivos periféricos.

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo?
¿Con poco uso? SI ( ) NO ( )
¿Ocioso? SI ( ) NO ( )
¿Con capacidad superior a la necesaria? SI ( ) NO ( )

Describa cual es _____

2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro mas lento y de menor costo?
SI ( ) NO ( )

3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado?
SI ( ) NO ( )

4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado.

_____

5. ¿El sistema de cómputo tiene capacidad de teleproceso?
SI ( ) NO ( )

6. ¿Se utiliza la capacidad de teleproceso?
SI ( ) NO ( )

7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso?
SI ( ) NO ( )

8. ¿Cuantas terminales se tienen conectadas al sistema de cómputo?

9. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?
SI ( ) NO ( )

10. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente
para atender el proceso por lotes y el proceso remoto?
SI ( ) NO ( )

SEGURIDAD FISICA Y CONFIDENCIAL

Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:

1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
SI ( ) NO ( )

2. ¿Existen una persona responsable de la seguridad?
SI ( ) NO ( )

3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI ( ) NO ( )

4. ¿Existe personal de vigilancia en la institución?
SI ( ) NO ( )

5. ¿La vigilancia se contrata?
a) Directamente ( )
b) Por medio de empresas que venden ese servicio ( )
6. ¿Existe una clara definición de funciones entre los puestos clave?
SI ( ) NO ( )

7. ¿Se investiga a los vigilantes cuando son contratados directamente?
SI ( ) NO ( )

8. ¿Se controla el trabajo fuera de horario?
SI ( ) NO ( )

9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.
SI ( ) NO ( )

10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SI ( ) NO ( )

11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
a) Vigilante? ( )
b) Recepcionista? ( )
c) Tarjeta de control de acceso ? ( )
d) Nadie? ( )

12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI ( ) NO ( )

13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?
SI ( ) NO ( )

14. El edificio donde se encuentra la computadora esta situado a salvo de:
a) Inundación? ( )
b) Terremoto? ( )
c) Fuego? ( )
d) Sabotaje? ( )

15. El centro de cómputo tiene salida al exterior al exterior?
SI ( ) NO ( )

16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.

17. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal? ( )
b) Por tarjeta magnética? ( )
c) por claves verbales? ( )
d) Otras? ( )

18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
SI ( ) NO ( )

19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
SI ( ) NO ( )

20. ¿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?
SI ( ) NO ( )

21. ¿Existe alarma para
a) Detectar fuego(calor o humo) en forma automática? ( )
b) Avisar en forma manual la presencia del fuego? ( )
c) Detectar una fuga de agua? ( )
d) Detectar magnéticos? ( )
e) No existe ( )

22. ¿Estas alarmas están
a) En el departamento de cómputo? ( )
b) En la cintoteca y discoteca? ( )

23. ¿Existe alarma para detectar condiciones anormales del ambiente?
a) En el departamento de cómputo? ( )
b) En la cíntoteca y discoteca? ( )
c) En otros lados ( )
24. ¿La alarma es perfectamente audible?
SI ( ) NO ( )

25.¿Esta alarma también está conectada
a) Al puesto de guardias? ( )
b) A la estación de Bomberos? ( )
c) A ningún otro lado? ( )
Otro_____

26. Existen extintores de fuego
a) Manuales? ( )
b) Automáticos? ( )
c) No existen ( )

27. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI ( ) NO ( )

28. ¿Los extintores, manuales o automáticos a base de
TIPO SI NO
a) Agua, ( ) ( )
b) Gas? ( ) ( )
c) Otros ( ) ( )
29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
SI ( ) NO ( )

30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?
SI ( ) NO ( )

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause mas daño que el fuego?
SI ( ) NO ( )

32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego?
SI ( ) NO ( )

33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por
tratarse de falsas alarmas? SI ( ) NO ( )
b) Pueda cortar la energía Eléctrica SI ( ) NO ( )
c) Pueda abandonar el local sin peligro
de intoxicación SI ( ) NO ( )
d) Es inmediata su acción? SI ( ) NO ( )

34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI ( ) NO ( )

35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI ( ) NO ( )

36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?
SI ( ) NO ( )

37. ¿Existe salida de emergencia?
SI ( ) NO ( )

38. ¿Esta puerta solo es posible abrirla:
a) Desde el interior? ( )
b) Desde el exterior? ( )
c) Ambos Lados ( )

39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
SI ( ) NO ( )

40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
SI ( ) NO ( )

41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables
en el departamento de cómputo? ( )
b) Prohibiendo fumar a los operadores
en el interior? ( )
c) Vigilando y manteniendo el

sistema eléctrico? ( )
d) No se ha previsto ( )

42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
SI ( ) NO ( )

43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
SI ( ) NO ( )

44. ¿Se controla el acceso y préstamo en la
a) Discoteca? ( )
b) Cintoteca? ( )
c) Programoteca? ( )

45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.

46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
SI ( ) NO ( )

47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.

48. ¿Se tienen establecidos procedimientos de actualización a estas copias?
SI ( ) NO ( )

49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:
0 1 2 3

50. ¿Existe departamento de auditoria interna en la institución?
SI ( ) NO ( )

51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?
SI ( ) NO ( )

52. ¿Que tipos de controles ha propuesto?

53. ¿Se cumplen?
SI ( ) NO ( )

54. ¿Se auditan los sistemas en operación?
SI ( ) NO ( )

55.¿Con que frecuencia?
a) Cada seis meses ( )
b) Cada año ( )
c) Otra (especifique) ( )

56.¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
a) Usuario ( )
b) Director de informática ( )
c) Jefe de análisis y programación ( )
d) Programador ( )
e) Otras (especifique) _____

57.¿La solicitud de modificaciones a los programas se hacen en forma?
a) Oral? ( )
b) Escrita? ( )
En caso de ser escrita solicite formatos,

58.Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
SI ( ) NO ( )

59.¿Existe control estricto en las modificaciones?
SI ( ) NO ( )

60.¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SI ( ) NO ( )

61.¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SI ( ) NO ( )

62.Se verifica identificación:
a) De la terminal ( )
b) Del Usuario ( )
c) No se pide identificación ( )
63.¿Se ha establecido que información puede ser acezada y por qué persona?
SI ( ) NO ( )

64.¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI ( ) NO ( )

65.¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI ( ) NO ( )

66.¿Existen controles y medidas de seguridad sobre las siguientes operaciones? ¿Cuales son?

( )Recepción de documentos_____
( )Información Confidencial_____
( )Captación de documentos_____
( )Cómputo Electrónico_____
( )Programas_____
( )Discotecas y Cintotecas_____
( )Documentos de Salida_____
( )Archivos Magnéticos_____
( )Operación del equipo de computación_____
( )En cuanto al acceso de personal_____
( )Identificación del personal_____
( )Policia_____
( )Seguros contra robo e incendio_____
( )Cajas de seguridad_____
( )Otras (especifique)_____

V.- SEGURIDAD DE LA INFORMACION

La información es uno de los activos más importantes de las entidades, y de modo especial en algunos sectores de actividad.

Es indudable que cada día las entidades dependen en mayor medida de la información y de la tecnología, y que los sistemas de información están más soportados por la tecnología, frente a la realidad de hace pocas décadas.

Por otra parte, hace unos años la protección era más fácil, con arquitecturas centralizadas y terminales no inteligentes, pero hoy día los entornos son realmente complejos, con diversidad de plataformas y proliferación de redes, no sólo internas sino también externas, incluso con enlaces internacionales.

Entre las plataformas físicas ("hardware") pueden estar: computadoras grandes y medianas, departamentales y personales, solas o formando parte de redes, e incluso computadoras portátiles. Esta diversidad acerca la información a los usuarios, si bien hace mucho más difícil proteger los datos, especialmente

porque los equipos tienen filosofías y sistemas operativos diferentes, incluso a veces siendo del mismo fabricante.

Al hablar de seguridad he preferido centrarme en la información misma, aunque a menudo se hable de seguridad informática, de seguridad de los sistemas de información o de seguridad de las tecnologías de la información.

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona humana, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el centro de cómputo de una institución es su nervio central, que normalmente tiene información confidencial y que, a menudo, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

El secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que

puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.

Por otro lado, es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de añadirlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

5.1 CONCEPTOS GENERALES DE LA SEGURIDAD DE LA INFORMACION

a) Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

b) Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

c) Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

d) Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

e) Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

f) Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

g) Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

h) Ataque activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

i) Ataque pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

j) Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información

confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

k) Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

l) Golpe (breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

5.2 ASPECTOS PRINCIPALES DE LA SEGURIDAD DE LA INFORMACION

En cualquier caso hay tres aspectos principales de la seguridad:

La confidencialidad: se cumple cuando sólo las personas autorizadas (en un sentido amplio podríamos referirnos también a sistemas) pueden conocer los datos o la información correspondiente.

Podemos preguntarnos ¿qué ocurriría si un soporte magnético con los datos de nuestros empleados o clientes fuera cedido a terceros? ¿cuál podría ser su uso final? ¿Habría una cadena de cesiones o ventas incontroladas de esos datos, que podrían incluir datos como domicilios o perfil económico, o incluso datos médicos?

La integridad: consiste en que sólo las personas autorizadas puedan variar (modificar o borrar) los datos. Además deben quedar pistas para control posterior y para auditoria.

Pensemos que alguien variara datos de forma que perdiéramos la información de determinadas deudas a cobrar (o que sin perderla tuviéramos que recurrir a la información en papel), o que modificara la última parte de los domicilios de algunos clientes.

Algunas de estas acciones se podrían tardar en detectar, y tal vez las diferentes copias de seguridad hechas a lo largo del tiempo estarían "viciadas" , lo que haría difícil la reconstrucción.

La disponibilidad: se cumple si las personas autorizadas pueden acceder a tiempo a la información.

El disponer de la información después del momento necesario puede equivaler a la no disponibilidad. Otro tema es disponer de la información a tiempo pero que ésta no sea correcta, e incluso que no se sepa, lo que puede originar la toma de decisiones erróneas.

Otro caso grave es la no disponibilidad absoluta, por haberse producido algún desastre. En relación con ello deben existir soluciones alternativas, basadas en medios propios o contratados, copias actualizadas de la información crítica y de programas en un lugar diferente, y un verdadero plan de continuidad que permita restablecer las operaciones en un tiempo inferior o igual al prefijado.

En la preparación -y actualización- del plan debemos pensar en situaciones posibles y en el impacto que tendrían en nuestra entidad (en su caso en las de nuestros clientes), especialmente si no disponemos de la información necesaria almacenada en lugares alternativos.

5.3 CONTROLES DE ACCESO NO AUTORIZADO

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

⇒ **Área de Sistemas.**

La libertad de acceso al área de sistemas puede crear un significativo problema de seguridad.

El acceso normal debe ser dado solamente a la gente que regularmente trabaja en esta área. Cualquier otra persona, de otro modo puede tener acceso únicamente bajo control. Mantener la seguridad física de su área de sistema es su primera línea de defensa. Para ello deberá tomar en consideración el valor de sus datos, el costo de protección, el impacto que su pérdida podría tener en su organización y la motivación, competencia y oportunidades de la gente que podría querer dañar los datos o el sistema.

⇒ **Computadoras personales y/o Terminales de la red.**

Las terminales que son dejadas sin protección pueden ser mal utilizadas. Cualquier terminal que pueda ser utilizada como acceso a los datos de un Sistema controlado, debe estar encerrada en un área segura, de tal manera que no sea usada, excepto por aquellos que tengan autorización para ello.

Igualmente, se deberá considerar la mejor manera de identificar a los operadores de terminales del Sistema, y el uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (5 - 10 Min.).

⇒ **Información Confidencial**

- Programas de Control. Deben existir programas protegidos que mantengan y controlen a los usuarios y sus derechos de acceso, ya sea por grupos o individualmente.

  El uso de tal programa puede conceder al usuario algunos de los privilegios que corresponden al controlador de dichos programas. La transferencia de privilegios es adecuada si el programa actúa como filtro de la información.

- Palabra de Acceso (Password). Es una palabra especial o código que debe teclearse al sistema de computadora antes que se realice un proceso. Constituye un procedimiento de seguridad que protege los programas y datos contra los usuarios no autorizados.

  La identificación de un individuo debe ser muy difícil de imitar y copiar. Aunque su nombre pueda ser único, es fácil que cualquiera que observe a quienes tienen acceso al sistema lo copie, por lo que no es una clave adecuada.

- Niveles de Acceso. Los programas de control de acceso deberán identificar a los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidos a la lectura o modificación en sus diferentes formas.

5.4 DESTRUCCION

Sin adecuadas medidas de seguridad las empresas pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático.

La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Cuando se pierden los datos y no hay disponibles copias de seguridad, se han de volver a crear los datos o trabajar sin ellos. De hecho, se puede comprobar cómo una gran parte del espacio en disco está ocupado por archivos, que es útil tener a mano pero que no son importantes para el funcionamiento normal. Un ejemplo típico son las copias de la correspondencia en forma de archivos del procesador de textos. Estos archivos se guardan muchas veces como referencia o, por si hubiera que enviar cartas parecidas en un futuro. Sin embargo, probablemente también existe copia en papel de estas cartas. Si se borran los archivos, puede ser molesto, pero las consecuencias en la organización pueden ser mínimas.

Los archivos de contabilidad suponen una situación diferente, ya que volver a crearlos puede necesitar de mucho tiempo y costo. Muchas organizaciones basan en estos archivos la toma de decisiones diaria. Sin los datos al día, el funcionamiento se vería seriamente dañado. Para evitar daños mayores al ser destruida la información, debe hacerse backups de la información vital para la empresa y almacenarse en lugares adecuadamente preparados para ese fin y de preferencia aparte del local donde se encuentran los equipos que usualmente lo manejan.

Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado. Por ejemplo: hay casos en los que,

empleados que han sido recientemente despedidos o están enterados que ellos van a ser despedidos, han destruido o modificado archivos para su beneficio inmediato o futuro.

5.5 REVELACION O INFIDENCIA

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio. La información, que es de carácter confidencial, es vendida a personas ajenas a la institución. Para tratar de evitar este tipo de problemas se debe tener en cuenta lo siguiente:

⇒ **Control del uso de información en paquetes abiertos o cintas y otros datos residuales**

La información puede ser conocida por personas no autorizadas, cuando se deja en paquetes abiertos o cintas que otras personas pueden usar.

Se deben tomar medidas para deshacerse del almacenaje secundario de información importante o negar el uso de ésta a aquellas personas que pueden usar mal los datos residuales de éstas.

⇒ **Mantener datos sensitivos fuera del trayecto de la basura**

El material de papel en la plataforma de la descarga de la basura puede ser una fuente altamente sensitiva de recompensa para aquellos que esperan el recojo de la basura. Los datos sensitivos deben ser apartados de este procedimiento para tener una mayor seguridad de protección de la información, cuando éstos son descartados o eliminados, debiendo recurrirse a destructores de papel.

⇒ **Preparar procedimientos de control para la distribución de información**

Una manera de controlar la distribución y posible diversificación de información, es mantener un rastro de copias múltiples indicando confidencialidad o usando numeración como "Pág. 1 de 9".

Desafortunadamente, es muy común ver grandes volúmenes de información sensitiva tirada alrededor de las oficinas y relativamente disponible a gran número de personas.

5.6 MODIFICACIONES

La importancia de los datos que se modifican de forma ilícita, está condicionada al grado en que la organización depende de los datos para su funcionamiento y toma de decisiones. Si fuera posible, esto podría disminuir su efecto si los datos procedentes de las computadoras que forman la base de la toma de decisiones, se verificarán antes de decidir. Hay que estar prevenido frente a la tendencia a asumir que " si viene de la computadora, debe ser correcto "

VI.-POLITICAS DE SEGURIDAD INFORMATICA

6.1 Generalidades

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes ha las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas empresas desarrollen documentos y normas que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la misma, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

6.2 Definición de Políticas de Seguridad Informática

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

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

6.3 Elementos de una Política de Seguridad Informática

Como una política de seguridad debe orientar las decisiones que se toman en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante.

Las Políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- ⇒ Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- ⇒ Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- ⇒ Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- ⇒ Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- ⇒ Definición de violaciones y sanciones por no cumplir con las políticas.
- ⇒ Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismos y términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etc.

6.4 Parámetros para Establecer Políticas de Seguridad

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- ⇒ Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- ⇒ Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- ⇒ Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- ⇒ Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos su área.
- ⇒ Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal, que ante cambios las políticas puedan actualizarse oportunamente.
- ⇒ Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

6.5 Razones que Impiden la Aplicación de las Políticas de Seguridad Informática

A pesar de que un gran número de organizaciones canalizan sus esfuerzos para definir normas de seguridad y concretarlas en documentos que orienten las acciones de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes lo representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad, que llevan a los altos directivos a pensamientos como: "más dinero para juguetes del Departamento de Sistemas".

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva y por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por sí solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que

facilitan la formalización y materialización de los compromisos adquiridos con la organización.

6.6 ¿Cómo deben elaborarse las políticas?

a) Recopilar material de apoyo

Para elaborar eficazmente un conjunto de políticas de seguridad informática, debe haberse efectuado previamente un análisis de riesgo que indique claramente las necesidades de seguridad actuales de la organización. Antecedentes de fallas en la seguridad, fraudes, demandas judiciales y otros casos pueden proporcionar una orientación sobre las áreas que necesitan particular atención.

Para afinar aun más el proceso, se debe tener copia de todas las otras políticas de organización (o de otras organizaciones similares) relativas a compra de equipos informáticos, recursos humanos y seguridad física.

b) Definir un marco de referencia

Después de recopilar el material de apoyo, debe elaborarse una lista de todos los tópicos a ser cubiertos dentro de un conjunto de políticas de seguridad. La lista debe incluir políticas que se piensa aplicar de inmediato así como aquellas que se piensa aplicar en el futuro.

c) Redactar la documentación

Después de preparar una lista de las áreas que necesitan la atención y después de estar familiarizados con la manera en que la organización expresa y usa las políticas, se estará ahora listos redactar las políticas, para lo cual pueden servir de ayuda el ejemplo que se encuentra más adelante.

Las políticas van dirigidas a audiencias significativamente distintas, en cuyo caso es aconsejable redactar documentos diferentes de acuerdo al tipo de audiencia. Por ejemplo, los empleados podrían recibir un pequeño folleto que contiene las políticas de seguridad más importantes que ellos necesitan tener presente. En cambio, el personal que trabaja en informática y en telecomunicaciones podría recibir un documento considerablemente más largo que proporciona mucho más detalles.

Una vez que se hayan elaborado los documentos sobre las políticas, deben ser revisados por un comité de seguridad informática antes de ser sometido a consideración de la Presidencia y Junta Directiva para su aprobación. Este comité debería tener representantes de los distintos departamentos de la organización y una de sus funciones más importantes es evaluar las políticas en la luz de su viabilidad, análisis costo/beneficio y sus implicaciones. Las preguntas que debe contestar son, por ejemplo: ¿Son estas políticas prácticas y fácilmente aplicables? ¿Son estas políticas claras e inequívocas?

Es muy importante que la Junta Directiva apruebe las políticas en el caso frecuente que ciertos empleados objeten o piensen que ellos no necesitan obedecer.

Además es fundamental de que luego de la entrada en vigor, las políticas se apliquen estrictamente, ya que de otra forma se puede fomentar la hipocresía entre los empleados y la tolerancia por conductas inapropiadas. El tener políticas que no se aplican puede ser peor que no tener políticas en absoluto.

La aplicación de nuevas políticas es a menudo más eficaz si los empleados han sido informados de exactamente qué actividades representan trasgresiones de la seguridad y qué penalización recibirían si fueran encontrados culpables.

Un curso o taller de sensibilización es una forma muy efectiva para dar a conocer las nuevas políticas. Allí, por ejemplo, se explicaría que la información interna es la propiedad de organización, y que no puede ser copiada,

modificada, anulada o usada para otros propósitos sin la aprobación de la gerencia.

La longitud del documento sobre las políticas

Las políticas de seguridad deben diseñarse de acuerdo a las necesidades específicas e una organización. Algunas organizaciones tienen muchas políticas, mientras otros tienen sólo unas cuantas.

El personal de seguridad puede opinar que es necesario que todo esté absolutamente claro y explícito sobre los asuntos de seguridad informática. En estos casos puede que se requiere un conjunto de políticas. Otros serán renuentes a tener tantas políticas, prefiriendo enfatizar la confianza en buen juicio y buen comportamiento de los empleados.

6.7 Ejemplo de Políticas de Seguridad

a. Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra Compañía. Sin ellos nos quedaríamos rápidamente fuera del negocio y por tal razón la Presidencia y la Junta Directiva tienen el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la Compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se

procesa (PCs, servidores, correo de voz, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Las distintas gerencias de la Compañía están 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. En todo caso cada año el Comité de Seguridad Informática llevará a cabo un análisis de riesgos y se revisarán las políticas de seguridad. Así mismo, se preparará cada año un informe para la Junta Directiva que muestre el estado actual de la Compañía en cuanto a seguridad informática y los progresos que se han logrado.

A todos los empleados, consultores y contratistas debe proporcionárseles adiestramiento, información, y advertencias para que ellos puedan proteger y manejar apropiadamente los recursos informáticos de la Compañía. Debe hacerse hincapié en que la seguridad informática es una actividad tan vital para la Compañía como lo son la contabilidad y la nómina.

La finalidad de las políticas de seguridad que se describen más adelante es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la Compañía (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

b. Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la Compañía:

⇒ El Comité de Seguridad Informática está compuesto por los representantes de los distintos departamentos de la Compañía, así como por el Gerente de Informática, el Gerente de

Telecomunicaciones (cuando exista), y el abogado o representante legal de la Compañía. Este Comité está encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática y telecomunicaciones. También es responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones, el Comité efectuará la evaluación y revisión de la situación de la Compañía en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

⇒ La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

⇒ El Jefe de Seguridad es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

⇒ El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra. El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

⇒ Los usuarios son responsables de cumplir con todas las políticas de la Compañía relativas a la seguridad informática y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Compañía a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato a un funcionario de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

c. Políticas de seguridad para computadores

⇒ Las computadoras de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

⇒ Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

⇒ Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática

⇒ No se permite fumar, comer o beber mientras se está usando un PC.

⇒ Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

⇒ Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

⇒ Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

⇒ Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

⇒ Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

⇒ No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.

⇒ La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

⇒ Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

⇒ Si un PCs tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

⇒ Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

⇒ Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o

borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

⇒ No está permitido llevar al sitio de trabajo computadores portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.

⇒ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la Compañía.

⇒ A menos que se indique lo contrario, los usuarios deben asumir que todo el software la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales..

⇒ Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.

⇒ No pueden extraerse datos fuera de la sede de la Compañía sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

⇒ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

⇒ Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.

⇒ No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido

comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

⇒ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el Departamento de Informática.

⇒ Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

⇒ No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la Compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

⇒ Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Compañía debe guardarse en otra sede, lejos del edificio.

⇒ Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

⇒ La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada.

⇒ No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

⇒ El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

⇒ Siempre que sea posible, debe eliminarse información confidencial de de las computadoras y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Compañía.

⇒ No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañía.

⇒ El personal que utiliza una computadora portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

d. Políticas de seguridad para las comunicaciones

Propiedad de la información

Con el fin de mejorar la productividad, la Compañía promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la Compañía y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación

⇒ Los sistemas de comunicación de la Compañía generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la Compañía.

⇒ Se prohíbe el uso de los sistemas de comunicación para actividades comerciales privadas o para propósitos de entretenimiento y diversión.

⇒ La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos de la Compañía y en tal sentido deben usarse las horas no laborables.

Confidencialidad y privacidad

⇒ Los recursos, servicios y conectividad disponibles vía Internet abren nuevas oportunidades, pero también introducen nuevos riesgos. En particular, no debe enviarse a través de Internet mensajes con información confidencial a menos que estén cifrada.

⇒ Los empleados y funcionarios de la Compañía no deben interceptar las comunicaciones o divulgar su contenido. Tampoco deben ayudar a otros para que lo hagan. La Compañía se compromete a respetar los derechos de sus empleados, incluyendo su privacidad. También se hace responsable del buen funcionamiento y del buen uso de sus redes de comunicación y para lograr esto, ocasionalmente es necesario interceptar ciertas comunicaciones.

⇒ Es política de la Compañía no monitorear regularmente las comunicaciones. Sin embargo, el uso y el contenido de las comunicaciones puede ocasionalmente ser supervisado en caso de ser necesario para actividades de mantenimiento, seguridad o auditoria. Puede ocurrir que el personal técnico vea el contenido de un mensaje de un empleado individual durante el curso de resolución de un problema.

⇒ De manera consistente con prácticas generalmente aceptadas, la Compañía procesa datos estadísticos sobre el uso de los sistemas de comunicación. Como ejemplo, los reportes de la central telefónica (PABX) contienen detalles sobre el número llamado, la duración de la llamada, y la hora en que se efectuó la llamada.

Reenvío de mensajes

Tomando en cuenta que cierta información está dirigida a personas específicas y puede no ser apta para otros, dentro y fuera de la Compañía, se

debe ejercer cierta cautela al remitir los mensajes. En todo caso no debe remitirse información confidencial de la Compañía sin la debida aprobación.

Borrado de mensajes

Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.

e. Políticas de seguridad para redes

Propósito

El propósito de esta política es establecer las normas, los procedimientos y los requisitos para asegurar la protección apropiada de la Compañía al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los empleados, contratistas, consultores y personal temporal de la Compañía.

Aspectos generales

Es política de la Compañía prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria. Además, es su política proteger la información que pertenece a otras empresas o personas y que le haya sido confiada.

Modificaciones

Todos los cambios en la central telefónica (PABX) y en los servidores y equipos de red de la Compañía, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de routers y switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia. Todo esto es para evitar problemas por cambios apresurados y

que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Cuentas de los usuarios

- ⇒ Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- ⇒ La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
- ⇒ No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- ⇒ Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- ⇒ No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas o tarjetas inteligentes.
- ⇒ Se prohíbe el uso de cuentas anónimas o de invitado y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

⇒ Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

⇒ Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas y el control de acceso

⇒ El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.

⇒ Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

⇒ Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.

⇒ La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

⇒ Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

⇒ Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda

suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.

⇒ Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas o tarjetas inteligentes.

⇒ Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).

⇒ Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.

⇒ Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.

⇒ Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

⇒ Los archivos de bitácora y los registros de auditoria que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

⇒ Los servidores de red y los equipos de comunicación (PABX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

VII. PLANES DE CONTINGENCIA

Cada día es más la importancia que cobra el uso de la tecnología informática en todos los aspectos tanto laborales como personales. Si se utiliza el Internet con frecuencia, en el momento en que no puede acceder su buzón de correo, o conectarse a la Web, se siente que algo hace falta.

De igual manera cuando las líneas de comunicación en una empresa se interrumpen, desconectando los sistemas, o cuando se daña un disco duro, o se pierde el acceso al centro de cómputo, se corre el riesgo de grandes pérdidas.

Hace algunos años cuando el proceso de la información no dependía tanto del tiempo, ni tampoco la necesidad de la información era tan dependiente en su inmediatez, era muy sencillo también establecer un plan de contingencia.

Las aplicaciones trabajaban por lotes, y por lo general la interacción entre cada uno de lo que hoy se conocen como módulos (agrupaciones funcionales) se efectuaba mediante archivos que estarían disponibles al terminar uno de los procesos y al iniciar el otro. El concepto de diseño estaba orientado a utilizar de la mejor manera posible el espacio en disco y memoria (realmente limitados) De todas maneras había ganancia, porque se reemplazaba un proceso manual (que tomaba varias semanas) por uno computarizado que procesaría la misma información en pocos días.

Realmente solo intervenían tres componentes en el proceso de la información: el equipo, los programas, y los datos y solo a estos tres componentes se remontaba la posible falla. Las razones externas que podrían causar una falla incluían un problema laboral (como una huelga que impedía el acceso al centro de cómputo), o un desastre natural.

Hoy se mantienen los mismos problemas externos, pero se ha complicado y aumentado el numero de componentes que se pueden ver afectados por una falla, incluyendo las redes de comunicación, las estaciones de trabajo, y la multiplicidad de equipos de almacenamiento distribuido. Las implicaciones pueden ser de cuantía menor para una persona que trabaje con un PC pero igualmente desastrosas para la continuidad de su trabajo.

Lo único que realmente permite que una empresa (o una persona) pueda reaccionar adecuadamente a una falta en un proceso crítico es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia. El plan es precisamente lo que su nombre indica, una serie de actividades tendientes a restablecer la operación normal, en el evento de una calamidad (interna o externa).

A manera de comparación, cuando el sistema era centralizado, el proceso era por lotes, y la interfase con la máquina era una terminal, lo único que se requería para tener en pié un plan de contingencia de fácil ejecución, era un contrato de reciprocidad con una empresa que tuviera un equipo similar al de uno, y una copia alterna de la información más reciente, de tal manera que se pudiera trasladar el proceso a la instalación de la empresa recíproca. Normalmente se utilizaban horarios nocturnos que por lo general no se ocupaban en el proceso de la empresa que prestaba el servicio.

El proceso de la información era ejecutado en su mayoría, por no decir en su totalidad, por personal del Departamento de Sistemas, por lo que no se requería mayor contenido en un plan de contingencia y se puede decir que

tampoco ningún entrenamiento. Se ejecutarían las actividades necesarias para restablecer el servicio. Por último, la información era un reflejo de actividades históricas, no necesariamente se requería de la información para la toma de decisiones.

Para que hoy en día, con lo complejo de los sistemas de información actuales, además de la responsabilidad del usuario en el proceso de su información, los Planes de Contingencia formalizados y probados cobran una importancia máxima al interior de las empresas, e inclusive en el ámbito personal. Está tan dependiente nuestro trabajo de la información que tengamos a la mano, que se reducen los espacios para estar sin acceso a la misma.

El Plan de Contingencia debe obedecer a un proceso formal y debe ser la conclusión de un proyecto de elaboración del mismo que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba REAL del mismo plan, una capacitación de las personas involucradas y una constante actualización.

El establecimiento de un plan de contingencia se inicia por la identificación de los procesos críticos del negocio (o de su trabajo). La definición de estos procesos críticos se puede hacer de manera compleja mediante una matriz de impacto estratégico de los procesos, o simplemente identificando, por experiencia, cuales son aquellos procesos que se tienen que ejecutar SIEMPRE.

Una vez identificados los procesos se determinan escalas horarias entre las cuales se deban tomar acciones dependiendo del tiempo estimado en que estará por fuera el sistema de información. Es importante reconocer que dependiendo de la magnitud del daño y del tiempo estimado en su recuperación, es que se deben tomar las acciones pertinentes.

Si un daño causa que el sistema esté fuera de línea unos pocos segundos, no se requerirán mayores acciones, al menos que el sistema sea de misión crítica

y estén involucrados recursos irrecuperables. Tal puede ser el caso de un avión en el aire. Si el daño puede demorarse algunas horas en su reparación, el sistema de atención a los clientes se verá duramente afectado, impactando así en la satisfacción de los mismos. Es decir, aunque parezca obvio, que dependiendo del tamaño del mal, será la curación.

Se deben considerar daños tanto externos como internos. Los daños internos pueden ser propios del equipo, las líneas de comunicación, caídas de la base de datos, entre otros. Los externos son los que realmente no están bajo nuestro control pero se pueden presentar, como una inundación o una interrupción de electricidad.

Tomemos el caso de la electricidad a manera de ejemplo de las decisiones que habrán de tomarse una vez identificados los procesos. Podemos establecer un sistema de facturación en línea en una cadena de almacenes como el proceso crítico, y como daño, podemos establecer un corte de electricidad. Las acciones que se desprendan deben obedecer al tiempo estimado de recuperación, por lo que será importante establecer un lazo de información con las Empresas Proveedoras del servicio de energía para obtener de ellos la información requerida en la eventualidad de un daño.

Se pueden tener previsiones escalonadas así:

- ⇒ Una planta de energía eléctrica propia, que se encenderá en el instante en que se corte la electricidad.
- ⇒ Una Unidad de poder ininterrumpido (UPS) para que supla la fracción de minuto mientras se hace el cambio de energía de la calle a la de la UPS.
- ⇒ Se pudiera pretender que se esta cubierto para una falla eléctrica, sin embargo si la planta eléctrica no enciente al irse la luz, sólo tendríamos resuelto el problema por el tiempo que duren las baterías de la UPS. La decisión a está en qué tan frecuente se puede presentar este tipo de circunstancia, y qué tan frecuente sucede. Igualmente habrá que

utilizar estadísticas referentes a la duración de la suspensión de electricidad. Con toda esta información se analizarían alternativas de aumentar el tamaño de la UPS, instalar una segunda planta eléctrica, o cualquier otra alternativa.

En el caso de daños internos, como daños en la computadora, los discos, la memoria, fallas en las redes de comunicación, el análisis es similar al utilizado con el ejemplo de la electricidad. Habrá que tener una solución escalonada dependiendo del tiempo que demore el proveedor en resolver el problema.

Otro punto de vital importancia: la interacción del grupo de trabajo que atenderá la contingencia. No es suficiente con tener el plan escrito, es importante involucrar contractualmente a los diferentes actores externos que atenderán nuestro llamado de ayuda.

El plan deberá contener claramente estipuladas las actividades que se llevarán a cabo en cada una de las circunstancias, e incluir la responsabilidad de cada uno de los miembros del equipo de recuperación. Es importante entonces, establecer un directorio telefónico, o un esquema ágil de comunicación con los miembros principales del grupo, y establecer una forma ágil de entrar en contacto con los proveedores.

Por último, pero no menos importante, es la ejecución, por lo menos una vez al año, o cuando haya cambios mayores en el sistema, del plan de contingencia elaborado. Esta es la única forma de garantizar que se pueden eliminar las dudas durante la prueba, dudas que si surgen durante la emergencia real, pueden ocasionar un peor daño que el existente si no se hace nada.

VIII.- CONCLUSIONES Y RECOMENDACIONES

El presente trabajo me ha permitido identificar el importante papel que juega la Auditoria Informática en los procesos administrativos que enfrenta un centro de cómputo de cualquier organización, ya sea privada o pública de cualquier nivel; municipal, estatal o federal, ya que este brinda un servicio de apoyo para el manejo de la información.

En la actualidad la información es uno de los activos más importantes dentro de una empresa, sin embargo no se ha tomado conciencia de esto, lo que lleva a que se ponga en riesgo la integridad y el correcto funcionamiento de las instituciones.

En el desarrollo de este trabajo se encuentran una serie de preguntas sencillas, y practicas que se pueden ser de gran utilidad para comenzar a adquirir conciencia de auditoria para cualquier empresa.

Hoy en día, el 90 por ciento de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente, y para esto es importante conocer diferentes metodologías de auditoria informática que con su realización se logre tal objetivo.

Es importante también, que exista una serie de políticas dentro de las empresas, ya que es una forma directa de comunicarse con los usuarios respecto a los recursos y servicios informáticos de la organización; y éstas deben orientar a la toma de decisiones en relación con la seguridad.

Es por todo esto que después de haber hecho un amplio estudio sobre la Auditoria Informática y su relación con la seguridad de la información recomiendo ampliamente que en todas las empresas dependiendo de sus alcances y necesidades se practiquen auditorias aunque sea de una forma interna, no es necesario grandes investigaciones y cuestionarios para darse cuenta del flujo de la información que se da en cada institución y cómo este puede beneficiar o perjudicar a dicho organismo; recordando siempre que la información que se procesa debe ser confidencial, integra y disponible.

X.- BIBLIOGRAFIA

Internet

http://www.geocities.com/diana_m_alvarez/principal.htm

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

http://dmi.uib.es/~bbuades/auditoria/auditoria.PPT

http://www.delitosinformaticos.com/propiedadindustrial/auditoria.shtml

http://www.monografias.com/trabajos5/audi/audi.shtml

http://www.geocities.com/Athens/Olympus/7428/virus1.html

http://ciberconta.unizar.es/LECCION/SEGURO/101.HTM

http://www.criptored.upm.es/guiateoria/gt_m142a.htm

http://www.ctv.es/USERS/mpq/estrado/estrado004.html

http://web.bemarnet.es/seguridad.html

http://www.ispjae.edu.cu/eventos/citel/articulos/seguridad.htm

LIBROS

Pino Caballero Gil, Candelaria Hernández Goya "Cristología y Seguridad de La información" Editorial .Rama Publishing Company; Diciembre 2000.

Royal P. Fisher "Seguridad En Los Sistemas Informáticos"
Editorial: Díaz de Santos; Octubre 1991.

Gustavo Aldegani "Seguridad Informatica VIII " Editorial: M.P. Ediciones; Mayo 1997.