ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

"Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial"

TESIS DE GRADO

Previa a la obtención del Título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

María Gabriela Hernández Pinto

GUAYAQUIL – ECUADOR

Año: 2006

AGRADECIMIENTO

A Dios, a mi mamita Albita y a mi papito Pinto quienes siempre han confiado en mí y me han dado su apoyo incondicional, a mi hermano Iván, a Maruja, a mi familia y a todas las personas que me ayudaron para culminar mi carrera.

A mi Directora de Tesis por su gran ayuda y colaboración.

DEDICATORIA

A Dios, a mi mamita Albita, a mi papito Pinto, a mi hermano Iván, a Maruja, a todos los que formamos la familia Pinto, a Nelly, Fanny, Lady, Pamela, Mariella, Luís, Manuel, Beto y a todos mis amigos quienes siempre de alguna manera me ayudaron y apoyaron.

TRIBUNAL DE GRADUACIÓN

Ing. Washington Armas
DIRECTOR DEL ICM
PRESIDENTE

Ing. Alice Naranjo
DIRECTORA DE TESIS

Ing. Dalton Noboa
VOCAL

Ing. Juan Alvarado Ortega
VOCAL

DECLARACIÓN EXPRESA

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

(Reglamento de Graduación de la ESPOL).

____

María Gabriela Hernández Pinto

RESUMEN

El contenido de este trabajo ayudará a las organizaciones comerciales a tener una concienciación permanente de mantener seguros sus activos, teniendo en cuenta que la palabra activo son todos los recursos informáticos o relacionados con éste para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

La meta de obtener un nivel considerable de seguridad se logrará con la propuesta que ofrece este proyecto mediante el "Diseño de un Plan Estratégico de Seguridad de Información" que puede ser aplicado por entidades dedicadas a cualquier tipo de actividad comercial que se proponga llevarlo a cabo. Este trabajo se desarrollará en los siguientes capítulos descritos a continuación.

En el primer capítulo se da a conocer la importancia, valor, razones de vulnerabilidades y vulnerabilidades de la información para formarnos un criterio del por qué es necesario mantenerla segura. En el segundo capítulo se desarrollará teóricamente el objetivo de este proyecto. En el tercer capítulo se da una breve descripción de las normas y estándares internacionales aplicables para el desarrollo de este tema. En el cuarto capítulo lleva a la práctica este proyecto. Finalmente se dan a conocer las conclusiones y recomendaciones de la práctica realizada para este trabajo.

INDICE GENERAL

Pág.

ABREVIATURAS

CSI	Instituto de Seguridad en Computación
FBI	Agencia Federal de San Francisco
ISO	Organización Internacional por la Normalización
ISMS	Information Security Management System / Dirección de la seguridad de los istemas de información
TI	Tecnología de Información
UPS	Uninterruptable Power Supply / Fuente Ininterrumpida de Energía

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Las tecnologías de la información actualmente son elementos fundamentales para la superación y desarrollo de un país, la información que en ellas se maneja es considerada un activo cada vez más valioso el cual puede hacer que una organización triunfe o quiebre, es por eso que debemos brindarle seguridad.

Para iniciar el tema de seguridad informática debemos tener claros los conceptos de información, riesgo, amenaza, vulnerabilidad, incidente de seguridad y seguridad de información, ya que estos términos son muy utilizados a lo largo del desarrollo de este tema.

- **Información:** Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización. La información da las pruebas de la calidad y circunstancias en las que se encuentra la empresa.

- **Vulnerabilidad:** Cualquier debilidad en los Sistemas que pueda permitir a las amenazas causarles daños y producir pérdidas.

- **Amenaza:** Cualquier evento que pueda provocar daño a la información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo.

- **Riesgo:** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema Informático, causando un impacto en la empresa.

- **Incidente de seguridad:** Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza.

- **Seguridad de Información:** Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas.

La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan considerando la seguridad como algo secundario y generalmente no se invierte el capital humano ni económico necesario para prevenir principalmente el daño y/o pérdida de la información que hoy en día con el uso de nueva tecnología para almacenarla, transmitirla y recobrarla está expuesta.

Las amenazas que afectan las características principales de la seguridad como son la confidencialidad, integridad y disponibilidad de la información pueden ser internas o externas, originadas accidentalmente o con un fin perverso dejando a la organización con problemas como por ejemplo la paralización de sus actividades que deja como resultado una perdida cuantiosa de tiempo de producción y dinero factores importantes para el desarrollo de una organización.

En vista que en la actualidad son muchos los riesgos que afectan la seguridad de nuestras empresas y por lo general el capital con el que se cuenta para protegerlas no es el suficiente debemos tener identificadas y controladas esas vulnerabilidades y esto se logra con un adecuado plan de seguridad elaborado en base a un análisis de riesgo previo.

Persiguiendo este objetivo que es la seguridad de la información, es que se presenta este proyecto de diseñar un plan estratégico de seguridad de información que se desarrollará en los siguientes capítulos de este trabajo.

CAPÍTULO 1

1. ANTECEDENTES

En el presente capítulo se dará a conocer la importancia de mantener segura la información en la empresa para prevenir el peligro de comprometer sus operaciones de negocios, la de sus inversores, clientes, socios y empleados; también se hará un breve análisis de las vulnerabilidades a los que está expuesta la información y que afectan a su funcionamiento normal y el impacto que tiene en las organizaciones los incidentes de seguridad.

1.1. Importancia de la Seguridad de Información

La información es importante para todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablemos de empresas altamente automatizados por lo que su seguridad sigue siendo un punto pendiente en las empresas, basta con mirar sus actividades para darnos cuenta que la seguridad es el factor más determinante por el cual fracasan las organizaciones. Así nos lo hace notar el estudio CSI/FBI año 2005 figura 1.1, realizado por el Instituto de Seguridad en Computación con la participación de la

Agencia Federal de San Francisco, escogiendo una muestra de 700 empresas de Estados Unidos, las cuales revelaron sus pérdidas causadas por tipo de amenaza de computadoras. Las pérdidas totales para el año 2005 eran de $130,104,542 para las 700 empresas que respondieron a este estudio, mostrando la grafica que mayores pérdidas se presentan en los virus, acceso no autorizado y el robo de información en comparación a las demás problemas que presentan las organizaciones. Se sospecha que el aumento en esas tres amenazas podría ser efecto del abuso y uso indiscriminado del internet por parte de los integrantes de la empresa.

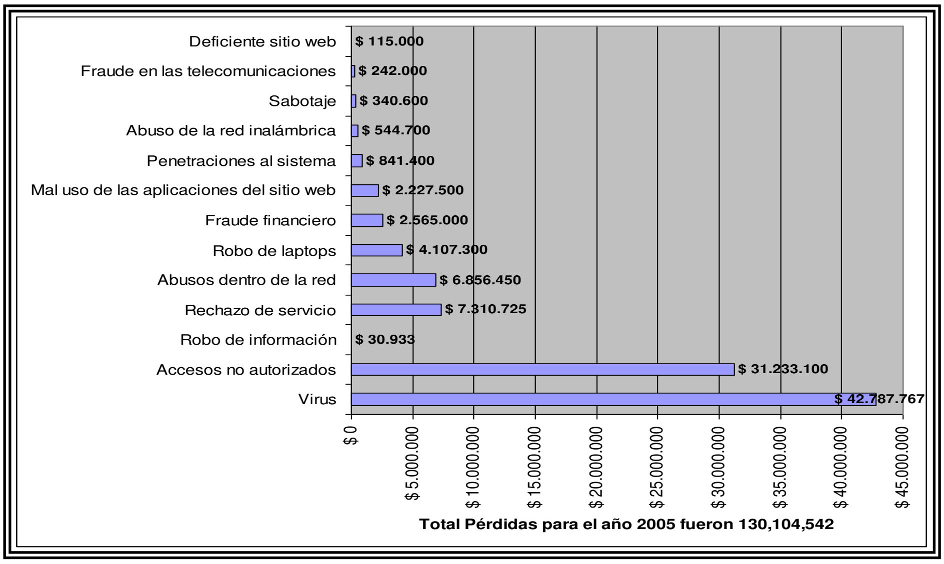

Figura 1.1 Pérdidas por tipo de amenaza
Fuente: CSI/FBI 2005 Computer Crime and Security Survey

Es muy importante ser conscientes de que por más que nuestra empresa a nuestro criterio sea la más segura, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas.

Es así como lo demuestra un estudio realizado por el grupo de seguridad Red IRIS figura 1.2 que ha tomado como población a las empresas de España ya que de este país es de donde recibe mayor cantidad de denuncias acerca de incidentes de seguridad cuyo objetivo ha sido el de reflejar el incremento de estos desde el año 1999 hasta el 2005; obteniendo los siguientes resultados:

- En el año 1999 se recibieron 195 denuncias de incidentes.

- En el año 2000 hubieron 416 denuncias incrementando los incidentes en un 113.33% con respecto al año anterior.

- En el año 2001 recibieron 1038 denuncias con un incremento del 149.51% en relación al año 2000.

- En el año 2002 hubieron 1495 denuncias aumentando los incidentes al 44.02% con respecto al año 2001.

- En el año 2003 se recibieron 1294 denuncias un valor menor al año anterior reduciendo los incidentes en un 13.44% en relación al año 2002.

- En al año 2004 aumentaron las denuncias a 1714 incrementando los incidentes en un 32.45%.

- Y finalmente en el año 2005 hubo una disminución del 27.18% de incidentes ya que se registraron 1248.

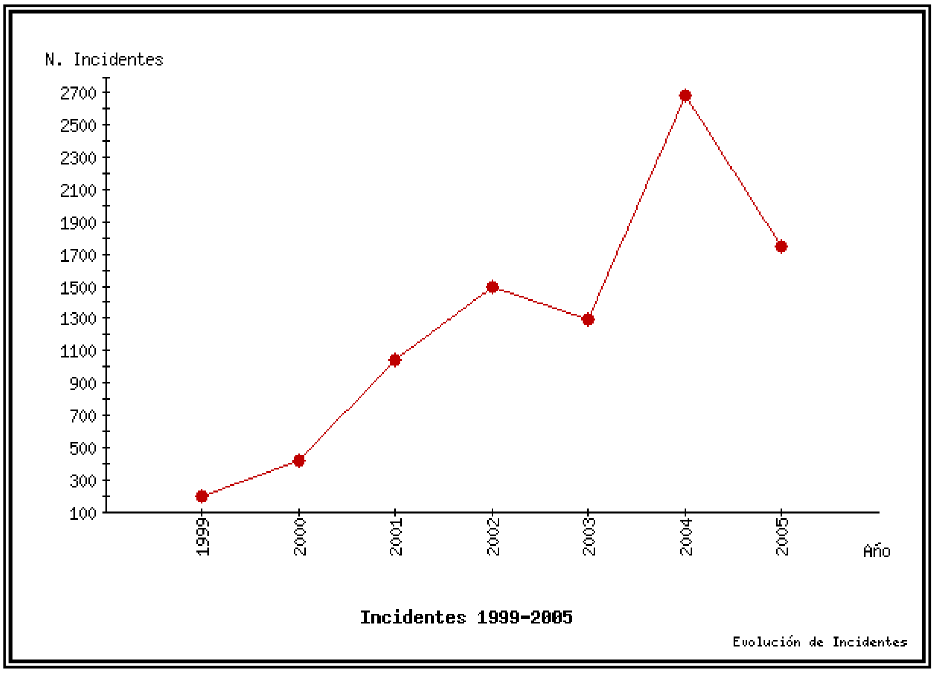

Figura 1.2 Tendencia de incidentes de inseguridad
Fuente: http://www.rediris.es/cert/servicios/iriscert/incidentes.html

Es por eso que en el ambiente competitivo de hoy, es necesario que las entidades aseguren la confidencialidad, integridad y disponibilidad de la información vital corporativa y así evitar sufrir amenazas de fuentes externas como los virus, hackers, troyanos entre otros y de fuentes internas como los originados por los empleados.

Por lo tanto, la seguridad informática debe ser dada por una colaboración entre los encargados de la seguridad de la información, que deben disponer de las medidas al alcance de su mano, y los usuarios, que deben ser conscientes de los riesgos que implican determinados usos de los sistemas y de los recursos que consumen cada vez que les pasa algún problema ya que esto les hace que pierdan tiempo de producción y el consumo de recursos en horas de la recuperación de la actividad normal es en muchos casos irrecuperable.

Sin embargo, gran parte de esa concientización está en manos de los responsables de seguridad de la información apoyados en todo momento por la gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas, impartiendo así procedimientos de actuación que permitan que las medidas técnicas que se disponen desde informática sean efectivas.

Por lo tanto en este nuevo entorno, es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio, sino también las de sus inversores, clientes, socios y empleados, reduciendo los problemas de seguridad que pueden surgir y dando a la información su valor.

1.2. Valor y costo de la información para las empresas

La información no tiene un valor específico; su valor está determinado únicamente por quienes la utilizan y desde la perspectiva de una corporación común, la información es cualquier elemento intangible que afecta al negocio. Al contrario de otros recursos corporativos tales como el dinero, la gente o el equipo, la información es fácil de alterar y duplicar. Algunas veces, de hecho, el valor de la información depende de que se mantenga en secreto.

Aunque una computadora puede ayudar a la gente a manejar datos e información, los seres humanos todavía deben evaluar esta información y tomar decisiones tales como las predicciones acerca del comportamiento del mercado de valores, planes para nuevos productos, revisiones a los empleados, listas de precios, entre otros.

Los tres factores que afectan al valor de la información son la oportunidad, la precisión y la presentación[1]. Equilibrar estas necesidades crea muchos retos para la gente que maneja esta información; determinar qué guardar y qué descartar, encontrar la mejor manera de organizar la información y controlar quién tiene acceso. Todas estas decisiones tienen que ser evaluadas contra el costo de la administración de la información. El valor de la información puede ser difícil de definir, el costo de su administración no lo es, aunque su valor aumenta mientras mas rápido se la requiera y mientras más compleja y detallada sea la información, requiere de mayor espacio de almacenamiento y éste cuesta dinero; por lo tanto la información para las organizaciones es un factor importante al momento de tomar decisiones que afecten o no a la rentabilidad de la misma, es por eso que esta información debe ser integra, disponible y confiable, es decir, debe contar con estos elementos de seguridad para garantizar el cumplimiento de los objetivos de la empresa.

El siguiente punto a tratar en este capítulo nos dará a conocer los riesgos que no solamente afectan el trabajo normal de la

---

[1] Introducción a la Computación, Primera Edición, Peter Norton, Mc Graw Hill pág: 50, 52,53.

organización y producen pérdidas monetarias sino que en algunos casos son capaces de llevar a la ruina a nuestras empresas.

1.3. Razones de vulnerabilidades de los Sistemas

Existen muchas ventajas para los sistemas de información que están adecuadamente salvaguardados. Pero cuando grandes cantidades de datos están almacenados electrónicamente, son más vulnerables que cuando se tienen en forma manual.

Estas vulnerabilidades se pueden originar por factores técnicos, institucionales, ambientales y en conjunto por malas decisiones administrativas.

Los sistemas computarizados son especialmente vulnerables a tales desafíos por las siguientes razones:

- <u>Complejidad en los sistemas de información</u>: Un sistema de información complejo no puede ser duplicado a mano. La mayor parte de la información no puede imprimirse o es demasiado voluminosa para ser tratada manualmente.

- Registros propios del computador: En general no quedan huellas visibles de cambios en los sistemas computarizados, porque los registros de computadoras solo pueden ser leídos por la máquina.

- Procedimientos computarizados: Parecen ser invisibles y no son bien entendidos y auditados.

- Por cambios: Los cambios en los sistemas automatizados son más costosos y con frecuencia más complejos que los cambios en los sistemas manuales.

- El desarrollo y operación de los sistemas: Los sistemas están abiertos al abuso de miembros del personal altamente capacitados técnicamente que no estén bien integrados a la institución. (Los programadores y los operadores de computadoras pueden hacer cambios no autorizados en el software mientras la información se procesa o pueden utilizar instalaciones de cómputo para propósitos no autorizados. Los empleados pueden hacer copias no autorizadas de archivos de datos con fines ilegales.)

- Sistemas automatizados: Aunque las posibilidades de desastre en los sistemas automatizados no son mayores que en los sistemas manuales, el efecto puede ser mucho mayor. En algunos casos, todos los registros del sistema pueden quedar destruidos y perdidos para siempre.

  Se tienen menos documentos en papel para procesar y revisar cuando los sistemas están automatizados. Es posible tener menor inspección manual.

- Acceso a los sistemas: La mayor parte de los sistemas son accesibles a muchas personas. La información es más fácil de recopilar pero más difícil de controlar.

- Procesamiento de datos: Los datos en los sistemas de cómputo pasan por más pasos de procesamiento que en los sistemas manuales, cada uno de los cuales está abierto a errores o a abusos. Cada una de estas funciones (origen de los datos, registro, transmisión, procesamiento, almacenamiento, recuperación y distribución) requiere de un conjunto independiente de controles físicos, administrativos y técnicos.[2]

1.4. Vulnerabilidades

Los avances en las telecomunicaciones y en el software de las computadoras han aumentado las vulnerabilidades a la seguridad de los sistemas que pueden ser interconectados en diferentes puntos, es decir que el potencial para acceso no autorizado, abuso o fraude no se limita a un solo lugar sino que puede ocurrir en cualquier punto de acceso a la red, lo que crea nuevas áreas y oportunidades para penetración y manipulación de los sistemas.

El entorno de internet es un peligro constante para las organizaciones que ahora trabajan con este servicio. Los peligros más frecuentes de los que deben protegerse las empresas mientras navegan en internet sus integrantes son los siguientes:

---

(2) Administración de los Sistemas de Información, Organización y Tecnología, Tercera Edición, Kenneth C. Laudon y Jane P. Laudon,Prentice Hall Hispanoamericana S.A., Impreso en México Copyright MCMXCIV. Pag: 702, 703, 704.

- Hackers: También llamados piratas informáticos accedan a la información que existe y se transmite por internet, no solo tienen acceso a e-mails sino a computadoras que están enlazadas a la red perjudicando a las empresas haciendo mal uso de la información.

- Cracker: Son personas que intentan romper la seguridad de un sistema, accediendo con malas intenciones a la información que se mantiene guardada en ellos.

- Virus: Son programas diseñados para modificar o destruir datos, pueden ser ingresados al sistema por un dispositivo externo o través de la red (e-mails) sin intervención directa del atacante.

- Gusanos: Son virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

- Caballos de Troya: Son virus que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

- Spam: También llamado correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y organismos.

Pero no sólo el internet es una amenaza para las organizaciones podemos encontrar otras tantas dentro de la propia empresa. Una amenaza siempre latente es el personal de la organización que por muchas circunstancias puede ser un peligro ya sea por los errores que pueda cometer sin intención como aquellos que son hechos con el objetivo de dañar a la organización un ejemplo claro es cuando en el Departamento de Sistemas no genera registros de las actividades de los usuarios en la red, esto provoca que no se pueda identificar anomalías que pueden realizar los empleados mientras se encuentren conectados al sistema volviendo a la información que se genera poco confiable; si continuamos explorando dentro de la empresa podemos encontrar otras vulnerabilidades como son los equipos que no reciben el mantenimiento adecuado o que por fallas eléctricas suelen dañarse y dejar a la organización con menos recursos para realizar sus operaciones. Las organizaciones siempre estarán expuestas a estos tipos de riesgos o ataques informáticos y a otros más ya que a medida que avanza la tecnología también habrá personas que intenten mejorar las formas de vulnerar la seguridad.

CAPÍTULO 2

2 MARCO TEORICO

2.1 Evolución histórica de la seguridad.

Hablar de evolución de seguridad es complejo, desde el inicio de la vida en comunidad, existían acciones para evitar amenazas, proteger la vida y las posesiones, allí se usaban métodos defensivos y se manejaban conceptos de alertar, evitar, detectar, alarmar y reaccionar a los diferentes hechos que podían suceder.

La familia, posteriormente diseñó esquemas de protección y se crearon lugares para resguardarse.

Algunos descubrimientos arqueológicos denotan con evidencias la importancia de la seguridad para los antiguas generaciones, entre estos tenemos las pirámides egipcias, el palacio de Sargon, el Dios egipcio Anubis, los Sumaricos, el Código de Hammurabi, entre otros.

Hasta se dice que Julio César utilizaba esquemas de seguridad en época de guerra y en el gobierno.

La seguridad moderna se originó con la revolución industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico y pionero de la administración Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales, luego de la técnica comercial, financiera, contable y directiva.

Al definir el objetivo de la seguridad Fayol dice: "salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y traiciones por parte del personal, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio."

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese los equipos, ni siquiera el empleado. Con la aparición de las computadoras, esta mentalidad se mantuvo, porque ¿Quién seria capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy, la seguridad, desde el punto de vista legislativo, está en manos de los políticos, a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera.

Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento en este nuevo milenio.

2.2 ¿Qué es seguridad informática?

Para llegar a una correcta definición de seguridad informática se debe conocer primero los conceptos de informática y seguridad respectivamente:

2.2.1 Definición de seguridad

La definición de seguridad trae consigo una ausencia de amenazas, situación que en el mundo contemporáneo es muy difícil de sostener, las sociedades actuales son sociedades de riesgo. El componente riesgo es permanente y da carácter propio de los estados y sociedades nacionales, como tal la seguridad no puede ser entendida como ausencia de amenazas.

Según la Real Academia Española, seguridad es cualidad de seguro y seguro es libre y exento de todo peligro.

Según Microsoft Encarta 2004, seguridad es cualidad de seguro y define a este a su vez como libre y exento de todo peligro, daño o riesgo.

Según Nambela en el año 1996 dijo seguridad es todo aquello que permite defenderse de una amenaza.

Para mi seguridad es eliminar la incertidumbre ante lo que puede pasar, la seguridad total no existe, debemos hablar de seguridad razonable.

2.2.2 Definición de informática

La informática surge en la preocupación del ser humano por encontrar maneras de realizar operaciones matemáticas de forma cada vez más rápida y fácilmente. Pronto se vio que con ayuda de aparatos y máquinas las operaciones podían realizarse de forma más eficiente, rápida y automática.

Según la definición de la Real Academia Española, la palabra informática significa “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores”.

2.2.3 Definición de seguridad informática

La definición de seguridad informática proviene entonces de los dos términos antes definidos.

La seguridad informática son técnicas desarrolladas para proteger los equipos informáticos y la información de daños accidentales o intencionados.

2.2.4 Objetivo de la seguridad informática

La seguridad informática tiene como principal objetivo proteger el activo más importante que tiene la empresa que es su información de los riesgos a los que está expuesta.

Para que la información sea considerada confiable para la organización ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

- Confidencialidad. Se define como la capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados.

- Integridad. Se define como la capacidad de garantizar que una información o mensaje no han sido manipulados.

- Disponibilidad. Se define como la capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial.

2.2.5 Riesgos

Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO) define riesgo tecnológico como “La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños”

A raíz de esta definición podemos concluir que cualquier problema que afecte al total funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad.

2.2.5.1 Tipos de amenazas a la seguridad

Ninguna empresa está exenta de sufrir amenazas a su seguridad, estas amenazas a las que son vulnerables las organizaciones son expuestas en la siguiente figura 2.1

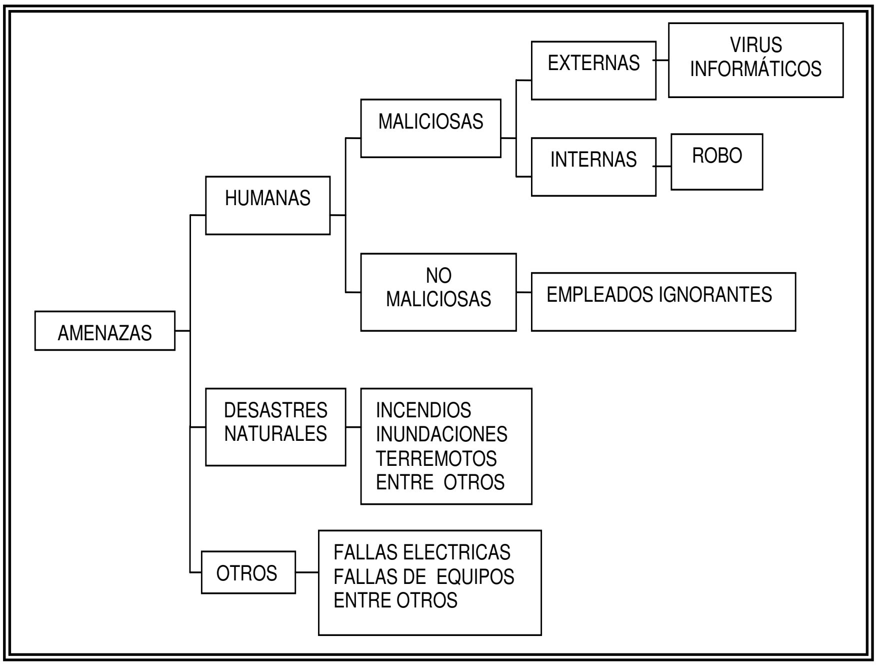

Figura 2.1 Tipos de Amenazas

El estudio CSI/FBI año 2005 figura 2.2, realizado por el Instituto de Seguridad en Computación con la participación de la Agencia Federal de San Francisco, tomando como población a las empresas de Estados Unidos, seleccionando una muestra de 700 organizaciones; destaca que el mal uso de los sistemas de información a tenido un crecimiento lento y a la vez disminuido firmemente en varios años.

En la única amenaza donde se percibe un aumento ligero es en el abuso de redes inalámbricas, esta categoría junto con el deficiente sitio web han sido agregadas solo desde el año 2004 en este estudio.

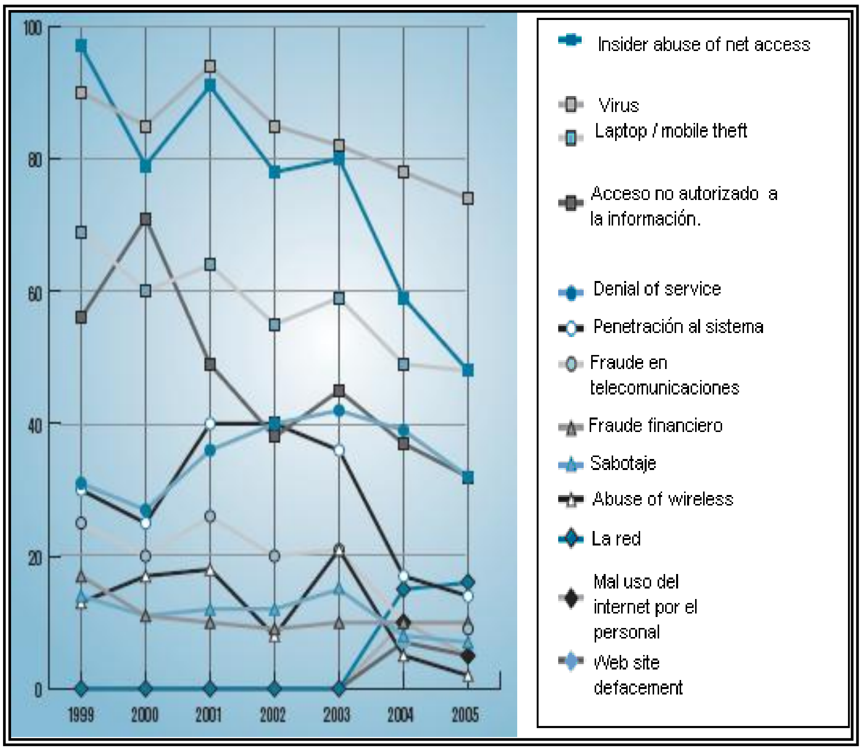

Figura 2.2 Amenazas/ Ataques detectados entre los años 1999-2005

2.2.5.1.1 Amenazas humanas

Las amenazas humanas como su nombre lo indica son aquellas acciones provocadas por el hombre y pueden ser de dos tipos maliciosas y no maliciosas

2.2.5.1.1.1 Maliciosas

Las amenazas maliciosas son aquellas que se llevan a efecto con el propósito de causar daño a la organización.

2.2.5.1.1.1.1 Externas

Las amenazas externas que pueden afectar al desarrollo y buen funcionamiento de las actividades de las empresas son frecuentemente originadas por el acceso a internet, ya que en esta red existen una serie de peligros como son los virus, hackers, entre otros que infiltrándose en la red interna de la organización provocando daños como mal funcionamiento de los sistemas y pérdida de información.

2.2.5.1.1.1.2 Internas

Las amenazas internas más frecuentes son las originadas por los propios funcionarios y ex - funcionarios de la organización motivados por la falta de dinero o represalia por algún tipo de enfrentamiento que hayan tenido con un superior.

2.2.5.1.1.2 No maliciosas

Este tipo de amenazas son producidas en la mayoría de los casos por errores ocasionados por empleados que no cuentan con el conocimiento o adecuada capacitación en el manejo de equipos y sistemas.

2.2.5.1.2 Amenazas por desastres naturales

Estas amenazas originadas por la naturaleza son las menos frecuentes en las organizaciones pero aún así no podemos dejar de considerarlas.

2.2.5.1.3 Otros

Otras amenazas son aquellas referentes a las que están fuera del alcance del hombre como son las interrupciones eléctricas, fallas de equipos originadas por los cortes de energía o no mantenerlos en el ambiente adecuado aunque esta es una responsabilidad más bien de carácter humano; entre otros.

2.2.5.2 ¿Cómo enfrentar los riesgos?

Los problemas de seguridad se multiplican con gran facilidad, por lo que las empresas deben perfeccionar los sistemas y los procesos para evitar amenazas o abordarlas cuando se produzcan. Para garantizar que la información de nuestra organización posea las características de seguridad ya mencionadas como son la confidencialidad, integridad y disponibilidad se debe poner en práctica un plan de seguridad informática.

2.2.6 Plan estratégico de seguridad informática

Un plan estratégico de seguridad informática está basado en un conjunto de políticas de seguridad elaboradas previo a una evaluación de los riesgos que indicará el nivel de seguridad en el que se encuentre la empresa. Estas políticas deben ser elaboradas considerando las características del negocio, la organización, su ubicación, sus activos y tecnología que posee la empresa.

2.2.6.1 Evaluación de los riesgos

La evaluación de los riesgos es el proceso por el cual se identifican las vulnerabilidades de la seguridad.

Por tanto el objetivo general de evaluar los riesgos será identificar las causas de los riesgos potenciales, en toda la organización, a parte de ella o a los sistemas de información individuales, a componentes específicos de sistemas o servicios donde sea factible y cuantificarlos para que la Gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos, en los diferentes puntos de análisis.

Los pasos para realizar una valoración de riesgos se detallan a continuación:

1. Identificar los riesgos
2. Análisis de los riesgos

2.2.6.1.1 Identificar riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático, existen formas de identificarlos como:

- <u>Cuestionarios de análisis de riesgos</u>: La herramienta clave en la identificación de riesgos son los cuestionarios los mismos que están diseñados para guiar al administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en algunas instancias, este instrumento esta diseñado para incluir riesgos asegurables e in-asegurables. El cuestionario de análisis de riesgos esta diseñado para servir como un repositorio de la información acumulada de documentos, entrevistas e inspecciones. Su propósito es guiar a la persona que intenta identificar exposiciones a riesgo a través del proceso de la identificación en un modelo lógico y consistente.

- Listas de chequeo de exposiciones a riesgo: Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.

- Listas de chequeo de políticas de seguridad: Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar. El administrador de riesgos consulta las políticas recolectadas y aplicadas a la firma.

- Sistemas expertos: Un sistema experto usado en la administración de riesgos incorpora los aspectos de las herramientas descritas anteriormente en una sola herramienta. La naturaleza integrada del programa permite al usuario generar propósitos escritos y prospectos.

2.2.6.1.2 Análisis de riesgos

Una vez se hayan identificado los riesgos, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

2.2.6.1.2.1 Ponderación de los Factores de riesgo

Ponderar el factor de riesgo es darle un valor de importancia en términos porcentuales al mismo bajo los criterios de especialistas en el área informática que pueden identificar su impacto en la organización, teniendo en cuenta las posibilidades de que se puedan convertir en realidad.

2.2.6.1.2.2 Valoración del riesgo

La valoración del riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de las prioridades.

TABLA 1

VALORACIÓN DEL RIESGO

Cuadrante	**Valoración del riesgo**
Impacto significante y probabilidad Alta	Alto
Impacto significante y probabilidad Baja	Medio-alto
Impacto insignificante y probabilidad Alta	Medio-bajo
Impacto insignificante y probabilidad Baja	Bajo

Fuente: http://www.monografias.com/trabajos14/datos/datos.html

Una explicación más clara de la valoración es la siguiente:

- Riesgo alto: Todos las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.

- Riesgo medio: Son exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.

- Riesgo bajo: Exposiciones a pérdidas que no causan un gran impacto financiero.

2.2.6.1.2.3 Crear la matriz descriptiva

El objetivo de esta matriz la cual podemos ver su formato en la tabla 2 es la de asignar un valor a los recursos informáticos que posea la organización de acuerdo al impacto que el riesgo tenga sobre cada uno de ellos.

TABLA 2

MATRIZ DESCRIPTIVA

Escala de Riesgos: 1 (Bajo), 2 (Medio Bajo), 3 (Medio Alto), 4 (Alto)

No.	Recursos Informáticos	R1	R2	R3	R….
1	A	3	3	1	…
2	B	2	2	2	…
3	C	1	1	3	…
4	D	2	4	3	…
5	E	3	2	2	…

Fuente: http://www.monografias.com/trabajos14/datos/datos.html

2.2.6.1.2.4 Crear la matriz ponderada

Esta matriz tiene como objetivo el determinar la prioridad de riesgo que tiene cada recurso informático mediante la obtención de un resultado determinado por la sumatoria de de cada una de las multiplicaciones realizadas entre la ponderación de cada riesgo con la valoración de cada recurso informático como lo muestra la tabla 3. Y así determinar la categoría de riesgo que tiene cada recurso.

TABLA 3

MATRIZ PONDERADA

	PONDERACIÓN	P1%	P2%	P3%	P…%	100%
No.	**RECURSOS INFORMÁTICOS**	**R1**	**R2**	**R3**	**R…**	**TOTAL**
1	A	3	3	1	…	(P1%x3) + (P2%x3)+…
2	B	2	2	2	…	(P1%x2) + (P2%x2) +…
3	C	1	1	3	…	(P1%x1) + (P2%x1) +…
4	D	2	4	3	…	(P1%x2) + (P2%4) +…
5	E	3	2	2	…	(P1%3) + (P2%x2) +…

Fuente: http://www.monografias.com/trabajos14/datos/datos.html

2.2.6.1.2.5 Crear la matriz categorizada

El objetivo de esta matriz como observamos en la tabla 4 es la de definir la categoría del riesgo (Alto, Medio y Bajo) para cada recurso informático. Para determinar que recursos informáticos están dentro de cada categoría nos ayudamos de formulas básicas de estadística para encontrar el rango y tamaño de intervalo que dividirán las categorías.

Para encontrar el rango tomamos el valor mayor de la columna total menos el valor menor. Este valor nos ayudará para definir el tamaño de intervalo, mediante la división del valor rango para la cantidad de categorías de riesgo que deseamos definir para nuestro análisis. Una vez obtenido este valor empezamos a segmentar los valores por intervalos para asignar las categorías ya definidas dando a los valores altos la definición de “riesgo alto”, a los valores medios “riesgo medio” y a los valores bajos “riesgos bajos”.

TABLA 4

MATRIZ CATEGORIZADA

	PONDERACIÓN	P1%	P2%	P3%	P…%	100%
No.	**RECURSOS INFORMÁTICOS**	**R1**	**R2**	**R3**	**R…**	**TOTAL**
1	A	3	3	1	…	RIESGO ALTO
2	C	1	1	3	…	RIESGO ALTO
3	E	3	2	2	…	RIESGO MEDIO
4	B	2	2	2	…	RIESGO MEDIO
5	D	2	4	3	…	RIESGO BAJO

Fuente: http://www.monografias.com/trabajos14/datos/datos.html

2.2.6.2 Políticas de seguridad

Una política de seguridad informática es aquella que fija los lineamientos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Si bien existen algunos modelos o estructuras para su diseño, estás tienen que ser elaboradas de forma personalizada para cada empresa para así recoger las características propias que tiene la organización.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos, es decir que estás políticas de seguridad deben abarcar las siguientes áreas.

- Seguridad Física
- Seguridad Lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el Outsourcing
- Planes de Contingencia

2.2.6.2.1 Elementos de una política de seguridad

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.

- Deberán establecer las expectativas de la organización, tales expectativas deben tener relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

- Las políticas 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.

- 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.

2.3. Seguridad Física

La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir el procesamiento de la información.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro de cómputo.

Las principales amenazas que se prevén en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas e inundaciones.

- Amenazas ocasionadas por el hombre.

- Disturbios, sabotajes internos y externos deliberados.

- Otras amenazas como las fallas de energía eléctrica o las fallas de los equipos.

Los recursos que se deben proteger físicamente van desde un simple teclado hasta un respaldo de toda la información que hay en el sistema, pasando por la propia máquina, igualmente se deben tener medidas de protección contra las condiciones climáticas y suministros de energía que pueden afectar la disponibilidad de los sistemas de información e interrumpir los procesos de la organización.

2.3.1. Seguridad de acceso físico

Se refiere a las medidas de seguridad para evitar el acceso de personas no autorizadas a los dispositivos de hardware y cualquier medio de salida de información como fax, copiadoras entre otros, ubicados tanto en el área de sistemas como en las áreas usuarias.

2.3.1.1. Organización

Para llevar un buen control de los accesos a la organización no sólo se requiere la capacidad de identificación, sino también negar asociarla a la apertura o cerramiento de puertas, permitir o negar accesos basados en restricciones de tiempo, área o sector de la empresa.

Existen varios métodos de control entre ellos están:

- Guardias de seguridad
- Detectores de Metales

- Sistemas Biométricos
- Seguridad con Animales
- Protección Electrónica

2.3.1.1.1. Guardias de seguridad

La utilización de guardias de seguridad será con el fin de controlar el acceso de personas ajenas a la organización y del mismo personal que ahí trabaje; la guardianía debe ser durante las 24 horas del día y deben estar armados para lo cual el personal de seguridad debe poseer un permiso para el manejo de armas otorgado por la autoridad pertinente.

Algunas medidas de seguridad podrían ser(3):

- Credenciales de identificación: Cualquier persona que ingrese a la organización deberá llevar una credencial.

(3) http://www.segu-info.com.ar/fisica/guardias.htm

Estás credenciales pueden clasificarse de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.

- Temporaria: para personal recién ingresado.

- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.

- Visitas.

* <u>Bitácora de registro de accesos:</u> Las personas ajenas a la organización deberán llenar este formulario que deberá contener el motivo de la visita, hora de ingreso, etc.

* <u>Control de Vehículos</u>: Para controlar el ingreso y egreso de vehículos, el personal de vigilancia debe asentar en una planilla los datos personales de los ocupantes del vehículo, la marca y patente del mismo, y la hora de ingreso y egreso de la empresa.

La utilización de guardias de seguridad también tiene su desventaja que es el soborno del guardia por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o salir de la empresa con equipos que no ha sido autorizado su salida.

2.3.1.1.1.1. Detectores de Metales

El detector de metales es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual[(4)].

La sensibilidad del detector es regulable, permitiendo de esta manera establecer un volumen metálico mínimo, a partir del cual se activará la alarma.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

---

(4) http://www.segu-info.com.ar/fisica/metales.htm

2.3.1.1.2. Sistemas Biométricos

La biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas[5].

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos.

Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas digitales y voz).

El beneficio de utilizar está técnica es en los costos de administración que son bajos debido a que se solo se realiza el mantenimiento del lector y una persona se encarga de mantener la base de datos actualizada.

Sumado a esto, las características biométricas de una persona son intransferibles a otra.

---

[5] http://www.segu-info.com.ar/fisica/biometricos.htm

2.3.1.1.3. Seguridad con Animales

Sirven para grandes extensiones de terreno, y además tienen órganos sensitivos mucho más sensibles que los de cualquier dispositivo y, generalmente, el costo de cuidado y mantenimiento se disminuyen considerablemente utilizando este tipo de sistema(6).

Así mismo, este sistema posee la desventaja de que los animales pueden ser engañados para lograr el acceso deseado.

2.3.1.1.4. Protección Electrónica

Se llama así a la detección de robo, intrusión, asalto e incendios mediante la utilización de sensores conectados a centrales de alarmas. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia.

---

(6) http://www.segu-info.com.ar/fisica/animales.htm

Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o luminosas alertando de la situación[7].

2.3.1.2. Área de sistemas

El área de sistemas es considerada como la más sensible a las amenazas debido a que en ella están ubicados los equipos que contienen toda la información que es procesada en las áreas usuarias y se le debe brindar un control adecuado y exclusivo.

Dentro de la organización lo más optimo para mantener la seguridad y evitar accesos no permitidos al área de sistemas es implementar como medio de protección los siguientes recursos[8]:

- Puerta con cerradura

[7] http://www.segu-info.com.ar/fisica/electronica.htm
[8] Auditoria en Informática, Segunda Edición, José Antonio Echenique García, Mc Graw Hill pág: 225.

- Puerta de combinación
- Puerta electrónica
- Puertas sensoriales
- Registros de entrada
- Videocámaras
- Escolta controladora para el acceso de visitantes
- Puertas dobles
- Alarmas

2.3.1.2.1. Puerta con cerradura

Requiere de la tradicional llave de metal, la cual debe ser difícil de duplicar.

2.3.1.2.2. Puerta de combinación

En este sistema se usa una combinación de números para permitir el acceso.

La combinación debe ser cambiada regularmente o cuando el empleado sea transferido o termine su función laboral dentro de ese centro de cómputo. Esto reduce el riesgo de que la combinación sea conocida por gente no autorizada.

2.3.1.2.3. Puerta electrónica

El sistema más común es el que se usa una tarjeta de plástico magnética como llave de entrada. Un código especial interno en la tarjeta es leído por un sensor activando el seguro de la puerta.

2.3.1.2.4. Puertas sensoriales

Son activadas por los propios individuos con alguna parte de su cuerpo, como puede ser la huella dactilar, voz, retina, geometría de la mano o bien por la firma.

2.3.1.2.5. Registros de entrada

Todos los visitantes deben firmar el registro de visitantes indicando su nombre, su compañía, la razón para la visita, la persona a la que visita. El registro se encontrará en la recepción del centro de cómputo. Es importante que el visitante proporcione una identificación con foto (licencia de manejo o credencial), ya que de otra forma podría inventar el nombre y no se tendría seguridad.

Los empleados deben de portar la credencial de la empresa con foto, la cual además de servir de identificación, se utilizará para señalar las áreas de informática a las cuales tiene autorización de entrar.

2.3.1.2.6. Videocámaras

Estas deben ser colocadas en puntos estratégicos para que se pueda monitorear el centro. Los casetes deben ser guardados para su posible análisis.

2.3.1.2.7. Escolta controladora para el acceso de visitantes

Todos los visitantes deben ser acompañados por un empleado responsable. Se consideran visitantes: amigos, proveedores, ingenieros de mantenimiento y auditores externos.

2.3.1.2.8. Puertas dobles

Este equipo es recomendable para lugares de alta seguridad; se trata de dos puertas, donde la segunda sólo se pueda abrir cuando la primera está cerrada.

2.3.1.2.9. Alarmas

Todas las áreas deben estar protegidas contra robo o accesos físicos no autorizados.

Las alarmas contra robo deben ser usadas hasta donde sea posible en forma discreta, de manera que no se atraiga la atención hacia este dispositivo de alta seguridad. Tales medidas no sólo se deben aplicar en el centro de cómputo sino también en áreas adyacentes.

2.3.2. Seguridad en la ubicación y Dimensión del área de sistemas

Se refiere a las precauciones que se deben tomar en cuenta para la instalación física del área que servirá como eje central del procesamiento de la información de la empresa evitando de está manera los accesos no permitidos, otras interrupciones y la falta de espacio físico para la adecuada operación del área.

2.3.2.1. Ubicación del área

Ubicar adecuadamente el área de sistemas es primordial para el desarrollo correcto e ininterrumpido de las actividades de los integrantes del departamento y buen rendimiento de los equipos; este lugar adecuado debe tener las siguientes características:

- Debe estar alejado de áreas de alto tráfico de personas o un lugar cercano a la calle o con un alto número de invitados; esto interfiere con la eficiencia en el trabajo y disminuye la seguridad.

- No debe tener grandes ventanales los cuales permiten la entrada del sol y pueden ser riesgosos para su seguridad.

- Debe estar alejado de lugares sumamente calurosos a los que todo el día les este dando el sol.

2.3.2.2. Dimensión del área

Las dimensiones mínimas del centro de cómputo deben determinarse por la cantidad de componentes del sistema, el espacio requerido para cada unidad, para su mantenimiento y el área de operación. Por ello, las paredes y paneles removibles pueden ser utilizados para facilitar ampliaciones futuras.

En general, aunque los equipos de cómputo se han reducido en tamaño, se debe considerar el incremento en el número de éstos y en equipos periféricos a la hora de planificar la construcción del departamento que será utilizado para el procesamiento de la información.

2.3.3. Seguridad del equipamiento

La información vital de la organización es procesada en los equipos de computación los cuales deben recibir cuidados especiales para prevenir posibles fallas ocasionadas por la electricidad, temperatura o falta de mantenimiento del equipo que puedan provocar interrupciones mientras se estén procesando los datos.

2.3.3.1. Aire acondicionado

El equipo de aire acondicionado es otro de los dispositivos que dependerá del tipo de computadoras que se utilice y del lugar donde está instalado, para lo cual se recomienda verificar con el proveedor la temperatura mínima y máxima, así como la humedad relativa en la que deberán trabajar los equipos. Generalmente la temperatura recomendada está entre 18-19ºC con una humedad entre el 45% - 50%.

Se deben tener algunas precauciones con el aire acondicionado para evitar futuros percances debido a este[9]:

- Las instalaciones del aire acondicionado son una fuente de incendio muy frecuente y deberá de contarse con detectores de humo que indiquen la posible presencia de fuego.

- Se recomienda que la presencia de aire en el área de sistemas sea ligeramente superior a la de las áreas adyacentes, para reducir así la entrada de polvo y suciedad

- Para el área de sistemas debe existir independiente del sistema central de aire acondicionado, dos equipos de aire acondicionado "especiales" de los cuales uno actúe como

---

[9] http://www.rediris.es/cert/doc/unixsec/node7.html

respaldo del otro cuando este no pueda operar correctamente.

La característica de estos equipos no es la común de los aires acondicionados normales ya que estos equipos principalmente acondicionan automáticamente la temperatura, la humedad, controlan el fluido de aire y son silenciosos, evitando de esta forma, daños en las computadoras y demás equipos que conforman el centro de procesamiento.

- En casos de contingencias en las cuales no se cuente con la operatividad del acondicionador de aire principal y a falta del equipo de respaldo; podrían mantenerse disponibles ventiladores de pedestales a fin de refrescar los equipos principales mientras dure la emergencia.

2.3.3.2. Instalación eléctrica y suministros de energía

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta es una de las principales áreas a considerar en la seguridad física.

Los problemas mas frecuentes derivados del entorno de trabajo relacionados con el sistema eléctrico que alimentan nuestros equipos y que amenazan la integridad tanto de nuestro hardware como de los datos que almacena o circulan por él son[10]:

- Cortocircuitos: Son producidos por los cambios de voltaje que recibe un equipo un ejemplo claro es cuando se va súbitamente el fluido eléctrico y regresa de la misma forma pero con mayor intensidad produciendo sobrecargas en el equipo.

- Picos de tensión: Son las subidas de tensión, conocidas como `picos' porque generalmente duran muy poco es decir durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta.

- Cortes de flujo: Son los cortes en el fluido eléctrico que llegan a nuestros equipos.

[10] http://www.rediris.es/cert/doc/unixsec/node7.html

Aunque un simple corte de corriente no suele afectar al hardware, lo más peligroso y que sucede en muchas ocasiones son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

- <u>Daños en los cables</u>: pueden ser producidos por roedores que se comen el plástico de los cables o también por su uso lo que hace que las comunicaciones dejen de ser fiables.

Las medidas más efectivas para proteger los equipos contra estos problemas de corriente eléctrica pueden ser[11]:

- Reguladores
- Sistema de energía no interrumpido (UPS)
- Switch de emergencia
- Protecciones generales

---

[11] Auditoria Informática, Segunda Edición, José Antonio Echenique García, Mc Graw Hill pág: 223.

2.3.3.2.1. Reguladores

Los reguladores son dispositivos eléctricos que reducen el riesgo de tener un accidente por los cambios de corrientes, si se tiene un regulador se debe verificar y controlar que el número de equipos conectados sean acordes con las cargas y especificaciones del regulador, ya que al no seguir las indicaciones puede causar que el regulador no proteja a todos los equipos.

2.3.3.2.2. UPS (Uninterruptable Power Supply/Fuente Ininterrumpida de Energía)

Un UPS consiste en un generador, que hace funcionar a la computadora en caso de haber una falla en el abastecimiento de energía eléctrica.

El UPS provee de energía eléctrica a la computadora por un cierto periodo; dependiendo de lo sofisticado que sea, la corriente eléctrica puede ser de horas o de algunos minutos, de tal forma que permita respaldar la información.

2.3.3.2.3. Switch de emergencia

Los switch de emergencia sirven en algún momento en que tal vez exista la necesidad de apagar la computadora y sus dispositivos periféricos en caso de incendio o si hubiera una evacuación del centro de cómputo. Por este propósito es recomendable tener uno en el área de sistemas y otro cerca pero fuera del área.

Los switch deben ser claramente identificados con un letrero, accesibles e inclusive estar a salvo de gente que no tienen autorización para utilizarlos, además deben estar bien protegidos de una activación accidental.

2.3.3.2.4. Protecciones generales

Algunas recomendaciones adicionales que se deben tomar en cuenta con respecto a las conexiones eléctricas serán:

- Los cables del sistema eléctrico deben estar perfectamente identificados, lo más frecuente es identificarlo por medio de colores (positivo, rojo).

- Deben de existir conexiones independientes para los equipos de cómputo; este cuidado se debe tener en las oficinas donde estén conectadas terminales o microcomputadoras.

- Se debe contar con los planos de instalación eléctrica debidamente actualizados.

- En zonas grandes con cargas eléctricas industriales será necesario un aislamiento adicional para prevenirr interrupciones de energía en el sistema.

- Para reducir los riesgos de incendios por causas eléctricas los cables deberán ser puestos en paneles y canales resistentes al fuego.

- Los cables deben estar adecuadamente aislados y fuera de los lugares de paso del personal.

- La energía del centro de procesamiento y afines debe ser exclusiva y no compartida con otras áreas.

- Como herramienta de emergencia, se debe contar siempre con linternas a pilas.

2.3.3.3. Temperatura y humedad

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%.

En todos los lugares hay que contar con sistemas que renueven el aire periódicamente.

No menos importante es el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio[12].

(12) http://www.segu-info.com.ar/fisica/ergometria.htm

2.3.3.4. Mantenimiento de los equipos

Para tener seguridad de que los equipos de computación operarán de manera adecuada, estos deberán recibir ciertos cuidados.

Dichos cuidados implicarán evitar algunas acciones perjudiciales y realizar periódicamente ciertas medidas simples de mantenimiento.

Estas medidas ayudarán a minimizar el desgaste del equipo y prevenir fallas mayores y de esta forma los equipos ofrezcan un rendimiento óptimo y eficaz a la hora de su funcionamiento.

Hay dos tipos de mantenimiento:

- <u>Mantenimiento Preventivo</u>: Se refiere a la revisión del equipo antes de que se presenten las fallas.
  Este mantenimiento se realiza para prolongar la vida útil del equipo y hacer que permanezca libre de reparaciones.

- Mantenimiento Correctivo: Consiste en la reparación del computador después de alguna falla o mala manipulación del equipo.

Se deben tomar las siguientes consideraciones para el mantenimiento de los equipos:

- Período de mantenimiento: El tiempo dependerá de diversos factores:

    - La cantidad de horas diarias de operación, el tipo de actividad (aplicaciones) que se ejecutan, el ambiente donde se encuentra instalada (si hay polvo, calor, etc.).

    - El estado general (si es un equipo nuevo o muy usado), y el resultado obtenido en el último mantenimiento del equipo.

- Personal Calificado: El mantenimiento debe ser realizado por personal capacitado en el área.

- Registros de mantenimiento: El llevar registros de los mantenimientos realizados ayudarán a prevenir que se repitan estas fallas llevando a cabo las recomendaciones para evitarlos que serán anotadas en dichos registros así como el motivo que causo la falla del equipo.

2.3.3.5. Seguridad de los equipos fuera de las instalaciones

Los equipos por varios motivos como su traslado a otra oficina de la misma empresa o por mantenimiento del mismo salen de la organización corriendo riesgos en su seguridad como el robo del equipo y su información.

Es por estos motivos que se deben tomar las siguientes providencias para mantenerlos seguros:

- Se deben seguir las indicaciones del fabricante para proteger los equipos de daños físicos.

- Los equipos que se trasladen fuera de la organización deben ser cubiertos con un seguro adecuado.

- Se debe llevar un registro de entrada y salida de los equipos en el cual se detallará la persona encargada del mismo, la razón de su salida, así como la hora de ingreso, salida del mismo y otros datos que se crean convenientes para la organización.

- Para el retiro de cualquier equipo se debe contar con una autorización de la gerencia.

2.3.3.6. Seguridad en la reutilización o eliminación de equipos

La información que contienen los equipos o dispositivos de almacenamiento está expuesta a una serie de riesgos como el robo cuando no se cuenta con adecuados controles de seguridad en el momento de eliminarlos o de volver a utilizarlos.

Para cualquiera de estas acciones como son la reutilización y la eliminación de equipos o unidades de almacenamiento se deben tener medidas de seguridad. La eliminación o borrado de la información de este equipo o unidad de almacenamiento es la más adecuada ya que impide que este disponible y asegura que los datos no correrán riesgo como la manipulación de los datos por personas no adecuadas.

Para el caso de que el equipo este dañado se debe realizar una valoración del mismo para lograr determinar si se debería destruirlo o repararlo según sea el caso y así proteger los datos.

2.3.4. Seguridad en contra de incendios y humo

Consiste en las precauciones y medidas a tomar en el caso de presentarse algún incidente provocados por fuego y humo los cuales son una amenaza para la organización debido a que sus consecuencias producen la pérdida de información y daño de los equipos.

2.3.4.1. Incendios

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas. Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

Por este motivo es necesario contar en la organización con salidas de emergencias que deben ser adecuadamente ubicadas y está ubicación será de conocimiento general de la organización

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometida el área de sistemas son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.

- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.

- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.

- No debe estar permitido fumar en las áreas, se debe contar con señales que indiquen tal prohibición.

- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

- El piso y el techo en el recinto del área de sistemas y de almacenamiento de los medios magnéticos deben ser impermeables.

Lastimosamente las previsiones que se toman contra incendios en ocasiones no son lo suficiente para evitarlos así que la organización debe estar preparada para poder combatirlos si se presentan.

Un método muy utilizado en las organizaciones para contrarrestar el fuego cuando este es de pequeñas dimensiones es el uso de extintores y se deben disponer de una suficiente cantidad de ellos; existen precauciones que deben ser revisadas en cuanto al uso de extintores como(13):

- Su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.

- Extintores adecuados: Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.

(13) http://www.monografias.com/trabajos14/datos/datos.shtml

- Correcto uso de extintores: También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.

- Extintor cargado: Es necesario verificar que los extintores se encuentre cargados y esta carga debe ser realizada en un centro de mantenimiento respectivo.

- Probar el extintor: Deben ser probados periódicamente a fin de que estos puedan funcionar en los casos de emergencias.

2.3.4.2. Humo

El área de sistemas y el resto de la organización deben poseer detectores de humo los cuales deben activarse de forma automática al momento de una emanación considerable de humo.

Estos dispositivos deben probarse regularmente para corroborar su funcionamiento.

En caso de ser detectores de incendios con prolongación automática de agua, deben ubicarse en áreas lejos de los equipos y material no recuperable por contacto con agua.

2.3.5. Seguridad contra desastres provocados por agua

Se refiere a la importancia de mantener controlados los riesgos de sufrir pérdidas de información y equipos a causa del agua.

Algunas precauciones que se deben tomar son[14]:

- Ubicación del área de sistemas: En caso de que la organización esté situada en una zona de inundaciones o con problemas de drenaje la mejor opción es situar el área de sistemas donde el riesgo de inundación no sea evidente sin descuidar la seguridad que se debe tener en el acceso a la misma.

[14] http://www.rediris.es/cert/doc/unixsec/node7.html

- Instalación de detectores de agua o inundación, bombas de emergencia: Esto servirá en caso de inundaciones inesperadas.

- Instalación de un falso suelo o situar los equipos a cierta distancia del suelo: Esto evitaría que el agua llegue a tocar a los equipos causando daño en ellos y la pérdida de información

2.3.6. Seguridad de backups o respaldos

Un respaldo o backup es una copia de los datos escrita en cinta u otro medio de almacenamiento duradero.

La protección física de la información almacenada en backups consiste en la protección de los diferentes medios donde residen nuestras copias de seguridad.

Se debe tener presente que si las copias contienen toda la información de la organización hay que protegerlas igual que se protegen los sistemas o los equipos.

De manera rutinaria se debe recordar a los usuarios de computadoras que deben respaldar su trabajo con frecuencia debido a que estas copias de seguridad del sistema son con frecuencia el único mecanismo de recuperación que poseen los administradores para restaurar una máquina que por cualquier motivo ha perdido datos.

Por tanto, una correcta política para realizar, almacenar y, en caso de ser necesario, restaurar los backups es vital en la planificación de seguridad de todo sistema.

El objetivo principal de crear respaldos de la información es la de poder mantener la continuidad del negocio después de algún incidente de seguridad, así también existen otras tareas importantes en la seguridad que tienen los respaldos como(15):

- Proteger la información en caso de que falle el equipo.

- Proteger la información en caso de borrado accidental de archivos.

---

(15) Seguridad y Comercio en el Web, Simson Garfinkel y Gene Spafford, Mc. Graw Hill, 1999, Pag: 267, 268.

- Proteger la información contra irrupciones, ya que los archivos borrados o modificados por un atacante pueden ser restaurados

- Ayudar a determinar la existencia del daño causado por un atacante, ya que es posible detectar cambios en el sistema comparando sus archivos con los almacenados en las cintas de respaldo.

- Sin embargo, los sistemas de respaldo no están exentos de problemas y se deben tomar las precauciones necesarias para su protección

2.3.6.1. Protección de respaldos

Los respaldos deben ser un prerrequisito de cualquier operación de cómputo, segura o no. Pero la información contenida en los respaldos es extremadamente vulnerable.

Cuando se utiliza un medio de almacenamiento cualquiera como respaldo cualquier persona que lo obtenga puede leer la información.

Por esta razón se deben proteger los respaldos por lo menos con tanto cuidado como a las computadoras mismas. Éstas son algunas sugerencias para proteger los respaldos[16]:

- Verificar datos de la cinta de respaldo: Estos datos deben ser correctos para que puedan emplearse para restaurar un sistema en funcionamiento. De otra forma, un respaldo puede dar un falso sentido de seguridad.

- Análisis de los sistemas que respaldan varias computadoras a través de una red: Deben ser analizados pues con frecuencia otorgan al servidor de respaldos control considerable sobre las computadoras que ejecutan clientes de respaldos y si un atacante irrumpe en la computadora que inicia los respaldos, es posible que cualquier sistema respaldado por esta esté

[16] Seguridad Práctica en UNIX e Internet, Segunda Edición, Simson Gar Finkel y Spafford Gene, Mc. Graw Hill, 1999, Pag: 325.

también comprometido.

- Encriptación de las cintas de respaldo: Las cintas de respaldo contienen todos los archivos y se deben proteger con tanto cuidado como las computadoras y sería prudente encriptar las cintas de respaldo para que, en caso de ser robada una de ellas, los datos no puedan comprometerse.

- Ubicación de los respaldos: Deben guardarse los respaldos en locales diferentes donde reside la información primaria evitando así la pérdida si en caso de desastre este hubiese alcanzado todo el edificio.

- Almacenamiento de los respaldos: El almacenamiento de los backups debe realizarse bajo condiciones ambientales óptimas, dependiendo del medio empleado.

  Las cintas de respaldos deberán estar guardadas bajo la vigilancia del administrador del sistema en un lugar seguro como una caja fuerte.

- Etiquetar los respaldos: Es necesario para poder identificar el contenido de las copias de seguridad con abundante información y así recuperar la información más rápido, la etiqueta debe contener la siguiente información:

  - Sistemas de ficheros almacenados.

  - Día y hora de la realización, sistema al que corresponde, etc.

- Entrega de respaldos: Los respaldos no deben ser entregados a servicios de mensajería a los que no se tenga confianza.

- Eliminación de respaldos: Antes de eliminar los respaldos deben ser borradas. Las cintas de respaldo se deben limpiar antes de venderlas, usarlas como cintas de copiado temporal o de deshacerse de ellas de otras formas.

- Reemplazo de respaldos: Debe realizárselo en forma periódica, antes que el medio magnético de soporte se pueda deteriorar.

- Pruebas de los respaldos: Se deben realizar pruebas periódicas de los backups, verificando su funcionalidad, a través de los sistemas, comparando resultados anteriores confiables.

- Registro de Backups: Es obligatorio el uso de un formulario estándar para el registro y control de los backups.

Es posible administrar los riesgos asociados con los respaldos si se tienen adecuadas medidas de control hacia ellos.

2.3.7. Seguridad de otros equipos

En muchas ocasiones los responsables de seguridad de los sistemas tienen muy presente que la información a proteger se encuentra en los equipos, en las copias de seguridad o circulando por la red y por lo tanto toman medidas para salvaguardar estos medios, pero olvidan que esa información también puede encontrarse en lugares menos obvios, como impresoras, faxes, copiadoras, información impresa, entre otros.

Evidentemente, hay que tomar medidas contra estos problemas de seguridad que pueden surgir en cualquier dispositivo por el que pueda salir información de nuestro sistema algunas pueden ser:

- <u>Ubicación de los equipos</u>: Deben estar situados en un lugar de acceso restringido.
  También es conveniente que sea de acceso restringido el lugar donde los usuarios recogen los documentos que lanzan a estos dispositivos.

- <u>Retiro de copias</u>: Se debe elegir a una persona que se encargue del retiro de copias aunque quizás esto puede ser imposible de implementar o por lo menos muy difícil en empresas que tengan un gran número de usuarios.

- Trituradoras de Papel: El empleo de estos dispositivos dificulta muchísimo la reconstrucción y lectura de un documento destruido. A un bajo costo se pueden conseguir uno de estos equipos, que suele ser suficiente para acabar con cantidades moderadas de papel.

- Archivado de Documentos: Es recomendable que los empleados no dejen expuestos los documentos sobre los escritorios y que sean inmediatamente archivados después de su uso para evitar cualquier extravío de documento intencional o accidental.

2.3.8. Seguros

Tener un seguro que cubra la totalidad de la pérdida ocasionada por un incidente es una obligación que debe asumir la organización mediante la contratación de un seguro.

Los seguros de los equipos en algunas ocasiones se dejan en segundo término aunque son de gran importancia, debido al poco conocimiento de los riesgos a los que está expuesta la computadora y por ende la información que en ella se procesa.

En ocasiones estos riesgos no son entendibles para las compañías de seguros, debido a lo nuevo de la herramienta, a la poca experiencia existente sobre desastres y al rápido avance de la tecnología.

Las consideraciones que debe tener la organización acerca de la póliza de seguro que poseen sus equipos son(17):

- Verificar las fechas de vencimiento de las pólizas, pues puede suceder que se tenga la póliza adecuada pero vencida.

- Actualización de la póliza, se debe tener la póliza actualiza con los nuevos equipos adquiridos por la organización.

- Cobertura del seguro, el seguro debe cubrir todo el equipo y su instalación por lo que es probable que una sola póliza no pueda cubrir todo el equipo con las diferentes

(17) Auditoria en Informática, Segunda Edición, José Antonio Echenique García, Mc. Graw Hill, 2001, Pag: 240

características (existe equipo que puede ser transportado, como computadoras personales y otras que no se pueden mover como unidades de disco duro), por lo que tal vez convenga tener dos o más pólizas por separado, cada una con las especificaciones necesarias.

La cobertura del seguro es otro punto importante en consideración ya que de esto depende la recuperación total de la pérdida sufrida por la empresa.

2.3.8.1. Cobertura de la póliza de aseguramiento

La póliza de seguro debe cubrir todos los activos que corran riesgos debido a diferentes incidentes que puedan suceder debido a varias circunstancias como robo, incendio, inundaciones, fallas eléctricas entre otras; se debe considerar también que existen riesgos que son difíciles de evaluara y de asegurar como la negligencia.

Las consideraciones con respecto a la cobertura del seguro pueden ser:

- Los seguros deben estar a precio de compra y no a precio al momento de contratación del seguro.

- El seguro debe cubrir tanto daños causados por factores externos (terremoto, inundación, etc.) como internos (daños ocasionados por negligencia de los empleados, daños debidos al aire acondicionado, etc.)

- También debe cubrir la pérdida de los programas (software), de la información, de los equipos y el costo de recuperación de lo anterior.

- En el caso de los programas se tendrá en cuenta en el momento de asegurarlos el costo de elaboración de determinado equipo, el costo de crearlos nuevamente y su valor comercial.

- En el caso del personal, se pueden tener fianzas contra robo, negligencia, daños causados por el personal, sabotaje, acciones deshonestas, etc.

2.3.8.2. Términos generales de un seguro de equipo de cómputo

A manera de ejemplo y en forma general, un seguro de equipo de computación considera lo siguiente(18):

- Bienes que se puedan amparar: Cualquier tipo de equipo electrónico como: de cómputo, de comunicación, etc.

  Con excepción de los que formen parte de equipo especial en automóviles, camiones, buques, aviones.

- Riesgos cubiertos: La cobertura básica cubre contra todo riesgo de pérdida súbita, accidental e imprevista, con excepción de las exclusiones que se indican en las condiciones generales de la póliza.

  Esta cobertura ampara riesgos como: incendio, rayo, explosión, picos de energía, cortocircuitos, sobretensiones, etc.

---

(18) Auditoria en Informática, Segunda Edición, José Antonio Echenique García, Mc. Graw Hill, 2001, Pag: 241.

- Riesgos excluidos: Pero que pueden ser cubiertos bajo convenio expreso son: terremoto y erupción volcánica; huracán, ciclón y tifón; equipos móviles o portátiles; huelgas y motín; hurto.

- Exclusiones: Las indicadas en las condiciones generales de cada seguro.

- Suma asegurada: En todos los casos se tiene que reportar como suma asegurada el valor de reposición de los equipos a asegurar (a valor nuevo sin descontar depreciación).

- Primas, cuotas y deducibles: Dependen del tipo de equipo.

- Indemnización en caso de siniestro: Las pérdidas parciales se indemnizan a valor de reposición (valor nuevo) y las pérdidas totales a valor real (valor nuevo menos depreciación).

2.4. Seguridad Lógica

La seguridad lógica consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Los objetivos de la seguridad lógica buscan:

- Restringir el acceso a los programas y archivos.

- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

- Que la información recibida sea la misma que ha sido transmitida.

- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.4.1. Seguridad en los accesos

Se refiere a los controles que pueden implementarse para proteger el sistema operativo de la red, los sistemas de aplicación y demás software de la utilización o modificaciones no autorizadas.

Para mantener la integridad de la información, restringiendo la cantidad de usuarios y procesos con acceso permitido y para resguardar la información confidencial de accesos no autorizados.

Los requisitos mínimos de seguridad en cualquier sistema son:

- Identificación y autentificación.
- Roles.
- Transacciones.
- Limitaciones a los servicios.
- Modalidad de Acceso.
- Ubicación y horario.

2.4.1.1. Identificación y autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas.

Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

- Identificación.- Se define así al momento en que el usuario se da a conocer en el sistema.

- Autenticación.- Es la verificación que realiza el sistema sobre esta identificación.

La medida más utilizada que permite la autenticación de la identidad del usuario es algo que solamente el individuo conoce como es una clave secreta de acceso o password.

2.4.1.1.1. Palabras claves o password

Las palabras claves o password se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones.

Son la barrera más común en contra de accesos no autorizados a un sistema y prácticamente son la única barrera.

Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo, es por eso que hay que poner especial atención en el tema de la elección de las palabras claves que servirán de identificación para el usuario que accede al sistema de datos de una organización.

2.4.1.1.1.1. Pautas de elección de claves

La elección de la clave es muy importante ya que será la identificación que tendrá el usuario al ingresar al sistema de la organización. Para escogerla se debe tener en cuenta los siguientes consejos[19]:

- <u>No utilizar contraseñas que sean palabras o nombres</u>. En la mayoría de los casos los usuarios son muy predecibles al escoger palabras que con frecuencia son aquellas que significan o tienen un nivel de importancia en su vida como: el propio nombre del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado.

---

[19] http://www.segu-info.com.ar/logica/seguridadlogica.htm

- No usar contraseñas completamente numéricas con algún significado. Por lo general las personas escogen datos como teléfono, cedula, fecha de nacimiento, placa del automóvil, etc, que son más fáciles de recordar para ellos.

- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

- Deben ser largas. Mínimo de 8 caracteres y máximo 10.

- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

- Deben ser fáciles de recordar para no verse obligado a escribirlas. Es decir palabras que no olvidarán y serán difíciles de descifrar para cualquier extraño. Algunos ejemplos son:

    - Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3.

- Usar una combinación de las primeras letras de alguna frase fácil de recordar: (A) (r)ío (R)evuelto (G)anancia (d)e (P)escadores por lo tanto la clave quedaría ArRGdP.

- Añadir un número a la combinación de las letras de la frase escogida para mayor seguridad: Usando la clave anterior añadimos los números quedando A9r7R5G3d1P.

- Realizar reemplazos de letras por signos o números: (E)n (S)eguridad (M)ás (V)ale (P)revenir (q)ue (C)urar entonces si reemplazamos la E por el 3 y la S por el 5 y tomamos las primeras letras de las otras palabras la clave quedaría 35MVPqC.

2.4.1.1.1.2. Reglas para proteger una clave

La protección de la contraseña recae tanto sobre el administrador del sistema como sobre el usuario. Al comprometer una cuenta se puede estar comprometiendo todo el sistema.

Algunos consejos a seguir[20]:

- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente.

- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Root, System, Test, Demo, Guest, etc.

- Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.

- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.

---

[20] http://www.segu-info.com.ar/logica/seguridadlogica.htm

- No teclear la contraseña si hay alguien mirando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es...".

- No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente (por lo menos 5).

Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas.

Entre ellas podemos citar las siguientes:

- Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas:

    - Obligar a reescribir el nombre de usuario (lo más común).

- Bloquear el acceso durante un tiempo.

- Enviar un mensaje al administrador y/o mantener un registro especial.

- Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).

- Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.

- Envejecimiento y expiración de contraseñas. Se lleva un control de cuándo pueden y/o deben cambiar sus passwords los usuarios.

  Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.

- <u>Ataque preventivo</u>. Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

2.4.1.1.1.3. Protección contra la intercepción de claves

La única forma de prevenirse contra la intercepción de claves es no utilizar nombres de usuario en texto llano y claves de acceso reutilizables.

En la actualidad, existen dos opciones comunes:

- <u>Utilizar un sistema de claves de acceso no reutilizables</u>: Esto se lleva a cabo entregando al usuario un listado con cientos de claves de acceso y cada vez que utilizan una de ellas, la tachan y utilizan la siguiente.

- <u>Utilizar un sistema basado en encriptación</u>: Evita el envió de la clave de acceso en forma llana a través de la red.

  La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada.

2.4.1.2. Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.
En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios[21].

2.4.1.3. Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada[22].

---

(21) http://www.segu-info.com.ar/logica/seguridadlogica.htm

(22) http://www.segu-info.com.ar/logica/seguridadlogica.htm

2.4.1.4. Limitaciones a los Servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario(23).

2.4.1.5. Modalidad de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser(24):

- Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.

(23) http://www.segu-info.com.ar/logica/seguridadlogica.htm

(24) http://www.segu-info.com.ar/logica/seguridadlogica.htm

- Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.

- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.

- Borrado: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos).

  El borrado es considerado una forma de modificación.

- Todas las anteriores.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- Creación: permite al usuario crear nuevos archivos, registros o campos.

- Búsqueda: permite listar los archivos de un directorio determinado.

2.4.1.6. Ubicación y Horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.
En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

2.4.1.7. Separación de las instalaciones de desarrollo y producción

La separación de las instalaciones para desarrollo y producción es importante porque pueden causar serios problemas como cambios no deseados en los archivos o en el entorno del sistema o fallas del sistema. Así también deben estar separadas las funciones de desarrollo y producción para reducir el riesgo de cambios accidentales o del acceso no autorizado al software de producción y a los datos de la organización.

Para su seguridad debería tomarse en cuenta lo siguiente:

- El software de producción y desarrollo deberían si es posible funcionar en procesadores diferentes, o en dominios o directorios distintos.

- Las tareas de desarrollo y de prueba deberían separarse tanto como sea posible.

- Se deberían usar diferentes claves de usuario en los sistemas de producción y desarrollo, para reducir el riesgo de confusión.

2.5. Seguridad en Redes

Las redes en las empresas son los medios que permiten la comunicación de diversos equipos y usuarios es así que es prioridad en la empresa mantener su seguridad debido a la información que por ellas se transmite como son los datos de clientes, servicios contratados, reportes financieros y administrativos, estrategias de mercado, etc.,

La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles y que son tan costosos como los ataques intencionados.

Dentro de la organización existen redes internas o intranet y las redes externas o extranet que deben ser protegidas de acuerdo a las amenazas a las que cada una está expuesta, estableciendo mecanismos de seguridad contra los distintos riesgos que pudieran atacarlas.

El mantener una red segura fortalece la confianza de los clientes en la organización y mejora su imagen corporativa,

2.5.1. Seguridad en la red interna o intranet

La red interna o intranet está formada por el conjunto de computadoras interconectadas a través de un servidor con la finalidad de compartir información y recursos de forma eficiente y rápida dentro de la organización.

El riesgo al que está frecuentemente expuesta esta red es el que viene del uso inadecuado del sistema por parte de los propios usuarios.

Ya sea por mala fe o descuido un usuario con demasiados privilegios puede destruir información.

Las medidas de seguridad que requiere la intranet para disminuir el riesgo existente por parte de los usuarios que son quienes hacen uso constante de la red son la encripción y las contraseñas para validar usuarios.

Estas medidas lógicas de seguridad son gestionadas por el administrador de la red y son explicadas con más detalle en este mismo capítulo dentro de la sección 2.4 que trata el tema de seguridad lógica.

2.5.2. Seguridad en la red externa o extranet

La red externa más grande que existe es internet y en la actualidad es desde donde se producen la gran mayoría de ataques por parte de personas que tienen el propósito de destruir o robar datos empresariales causando pérdidas de dinero. La seguridad en internet es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios de esta red y las organizaciones que los rodean. La seguridad es una protección contra el comportamiento inesperado.

2.5.2.1. Peligros en la red externa

Internet es una red de dos sentidos. Así como hace posible que los servidores de internet divulguen información a millones de usuarios, permite a otros vándalos irrumpir en las mismas computadoras donde se ejecutan los servidores de internet. Hay dos grandes tipos de peligros potenciales que pueden comprometer nuestra información desde una red externa[25]:

- **Ataques Indiscriminados.** Suelen ser los más frecuentes y también los menos dañinos. Dentro de esta categoría podemos incluir los troyanos y los virus. Cuyos ataques pueden ser contrarestados por los antivirus.

- **Ataques a medida.** Mucho menos comunes que los anteriores y también más peligrosos son los ataques que generalmente llevan a cabo los hackers. En estos casos las victimas más frecuentes casi siempre son las grandes corporaciones.

---

[25] Criptografía y Seguridad en Computadoras, Segunda Edición, Manuel José Lucena López, Universidad de Jaen, Septiembre 1999, Pag: 137, 138.

2.5.2.2. Medidas de seguridad en Internet

Las líneas de defensa contra intrusos en internet y que más son implementados por las organizaciones para proteger sus datos son el firewall y los antivirus

2.5.2.2.1. Firewall o puerta de seguridad

Los firewalls son parte de la estrategia de seguridad de una organización debido a que manejan el acceso entre dos redes la red interna y la red externa y si no existiera el firewall todas las computadoras de la red estarían expuestas a ataques desde el exterior (internet), quizás uno de los elementos más conocidos a la hora de establecer seguridad, sea este.

Aunque debe ser uno de los sistemas a los que más se debe prestar atención ya que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada máquina interna.

El objetivo del firewall es:

- Controlar todo el tráfico desde dentro hacia fuera de la organización, y viceversa, y cualquier dato, archivos entre otros debe pasar a través de él para que pueda tener acceso el usuario de la red.

- Sólo el tráfico autorizado, definido por la política local de seguridad en el firewall se le permite el acceso a la red de la organización.

El firewall sólo sirve de defensa perimetral de las redes, no defiende de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

2.5.2.2.1.1. Limitaciones del firewall

El firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataques, pero el firewall también tiene sus limitaciones[26]:

---

(26) http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

- Vulnerabilidades que no se corrigen y que coincidentemente o no, son descubiertas por intrusos. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar.

- El firewall no es contra humanos. Es decir que si un intruso logra entrar a la organización y descubrir passwords o las vulnerabilidades del Firewall y difunde esta información, el Firewall no se dará cuenta.

- Tampoco provee herramientas contra la filtración de software o archivos infectados con virus. Aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Estás limitaciones deben ser tomadas en cuenta por la organización ya que su información está expuesta a intrusos sino cuenta con las debidas seguridades.

2.5.2.2.2. Antivirus

Los virus son el mayor riesgo de seguridad para una red, debido a que afectan a toda la información dañando los archivos que se guardan en las computadoras, impidiendo que los usuarios trabajen normalmente.

La medida básica de seguridad que se debe tomar en estos casos son los antivirus. Estos antivirus son aplicaciones o programas dedicados a detectar y eliminar virus informáticos.

2.5.2.2.2.1. Tácticas antivíricas

Las tácticas antivíricas son nada más que maneras o formas en que los usuarios pueden preparase y afrontar situaciones como la infección de su equipo por la causa de un virus. Estas técnicas son[27]:

- Preparación y prevención

[27] http://www.monografias.com/trabajos6/sein/sein.sht

- Detección de virus

- Contención y recuperación

A continuación explicaremos cada uno de estas técnicas.

2.5.2.2.2.1.1. Preparación y prevención

Los usuarios pueden prepararse frente a una infección viral creando regularmente copias de seguridad del software original legítimo y de los archivos, para poder recuperar el sistema informático en caso necesario. Puede copiarse en un CD el software del sistema operativo y proteger el disco contra escritura, para que ningún virus pueda sobrescribir el disco. Las infecciones virales pueden prevenirse obteniendo los programas de fuentes legítimas, empleando una computadora en cuarentena para probar los nuevos programas y protegiendo contra escritura los CD's siempre que sea posible.

2.5.2.2.2.1.2. Detección de virus

Para detectar la presencia de un virus pueden emplearse varios tipos de programas de antivirus. Los programas de antivirus pueden reconocer las características del código informático de un virus y buscar estas características en los archivos del computador. Como los nuevos virus tienen que ser analizados cuando aparecen, los programas de virus deben ser actualizados periódicamente para resultar eficaces.

2.5.2.2.2.1.3. Contención y recuperación

Una vez detectada una infección viral, ésta puede contenerse aislando inmediatamente los computadores de la red, deteniendo el intercambio de archivos y empleando sólo discos protegidos contra escritura.

Para que un sistema informático se recupere de una infección viral, primero hay que eliminar el virus.

Algunos programas antivirus intentan eliminar los virus detectados, pero a veces los resultados no son satisfactorios.

Se obtienen resultados más fiables desconectando la computadora infectada, arrancándola de nuevo desde un disco flexible protegido contra escritura, borrando los archivos infectados y sustituyéndolos por copias de seguridad de archivos legítimos y borrando los virus que pueda haber en el sector de arranque inicial.

2.6. Seguridad en los Recursos Humanos

Las personas son necesarias para que trabajen en las computadoras pero también es cierto que la mayor amenaza para los sistemas de seguridad de una empresa es la deshonestidad y negligencia de sus propios empleados. Los gerentes deben poner mucha atención al personal que contratan para puestos con acceso a los sistemas computarizados de información y de datos delicados ya que alguien totalmente negligente puede causar tanto daño como alguien que sea deshonesto por naturaleza.

Para mantener la seguridad en los recursos humanos que trabajarán y trabajan en la organización es necesario considerar lo siguiente:

- Investigar sus antecedentes.
- Establecer acuerdos de confidencialidad.
- Fijar los términos y condiciones de la relación laboral.
- Capacitación continua y concientización.
- Segregación de funciones.
- Despidos y renuncias.

2.6.1. Investigación de antecedentes

Al contratar a empleados nuevos se debe investigar sus antecedentes. Pidiendo a los candidatos que llenen una solicitud y luego se deben verificar todas las referencias que ha dado el candidato para conocer su pasado, incluyendo las razones por las que cambia de trabajo.

Es importante verificar las fechas de contratación y separación buscando pistas que puedan dar indicios de hechos que el aspirante no haya mencionado. También se requiere verificar el historial académico y las distinciones.

Un candidato que miente en su solicitud de empleo no ha establecido una buena base para confiar en él.

A veces es prudente investigar más a fondo la historia y la personalidad de los candidatos. Puede requerirse[28]:

- Contratar a una agencia de investigaciones para verificar el historial.

- Obtener una copia de los antecedentes penales del individuo.

- Revisar la historia de crédito del candidato buscando deudas personales cuantiosas y la imposibilidad de pagarlas. Estos problemas deben discutirse, si se presentan, con el candidato.

- Usar un detector de mentiras (si es legal).

---

[28] Seguridad Práctica en UNIX e Internet, Segunda Edición, Simson Gar Finkel y Spafford Gene, Mc. Graw Hill, 1999, Pag: 335.

- Exigir una fianza al candidato si se le emplea.

No se recomienda aplicar estas medidas en general para contratar a todos los empleados. Pero sí debe examinarse cuidadosamente a quienes se les aplicará preferentemente a los que serán contratados para trabajos de confianza o que requieran acceso privilegiado, incluyendo al personal de mantenimiento y limpieza.

También se considera apropiado avisar a los candidatos que se realizarán estas revisiones para obtener su consentimiento. Esta cortesía facilitará las investigaciones y le advertirá al candidato que las precauciones de seguridad se toman en serio.

2.6.2. Acuerdos de confidencialidad

Estos acuerdos de confidencialidad o no divulgación sirven para notificar que información es secreta o confidencial. Los empleados deberán firmar, normalmente, dicha cláusula como parte de sus términos o condiciones iniciales de trabajo.

La organización debería requerir la firma de un acuerdo de confidencialidad con el personal temporal y los usuarios que son terceras partes no cubiertos por un contrato de trabajo (que contiene cláusulas de confidencialidad) antes de su acceso a los recursos de tratamiento de información.

Las cláusulas de confidencialidad deberían revisarse cuando cambien los términos del empleo o contrato, especialmente cuando los empleados dejen la organización o sus contratos terminen

2.6.3. Términos y condiciones de la relación laboral

Los términos y condiciones de la relación laboral deberían indicar la responsabilidad de los empleados en cuanto a la seguridad de la información. Donde sea apropiado, dicha responsabilidad debería continuar durante un periodo definido tras la finalización del contrato.

Debería incluirse qué hacer si el empleado incumple los requisitos de seguridad.

Deberían aclararse e incluirse en los términos y las condiciones de empleo las responsabilidades y derechos legales, por ejemplo, respecto a las leyes de propiedad intelectual o de protección de datos. También debería incluirse la responsabilidad por la clasificación y gestión de los datos del empleador.

Los términos y las condiciones del contrato deberían establecer, cuando proceda, que dichas responsabilidades se extienden fuera del ámbito de la organización y de las horas normales de trabajo.

2.6.4. Capacitación continua y concientización

Los usuarios deben recibir periódicamente información actualizada sobre la seguridad y el uso apropiado de las computadoras. Esta capacitación continua es una oportunidad de explicar las buenas costumbres, recordarles a los usuarios las amenazas y las consecuencias de las fallas, y proporcionar un foro para discutir las preguntas y preocupaciones del personal.

Los colaboradores de los administradores de sistemas deben tener la oportunidad de capacitarse continuamente.

Esto incluye asistir a reuniones profesionales y seminarios, suscribirse a revistas técnicas y gremiales, y comprar libros de referencia y otros materiales.

Deben tener tiempo para leer y usar este material y recibir incentivos para dominarlo.

Junto con la capacitación continua puede considerarse un programa de concientización continua.

Esto incluye la colocación de avisos acerca de las buenas costumbres, usar mensajes diarios con consejos y recordatorios, realizar un “día de concientización” cada datos o tres meses y llevar a cabo otros eventos que eviten que la seguridad caiga en el olvido.

Los planes deben, claro está, tomar en cuenta el tamaño y la naturaleza de la organización, los niveles de riesgo y el tamaño y tipo de la población de los usuarios.

Se debe pensar en el costo de las actividades de concientización y presupuestarlas[29].

2.6.5. Segregación de funciones

Se refiere a la separación cuidadosa de las funciones de cada empleado de forma tal que los que deben vigilar el uso inapropiado no puedan hacer uso indebido de los recursos. Para esto se debe determinar las autorizaciones de cada función, evaluando su nivel de riesgo para la organización y de esta forma evitar que puedan suceder alteraciones en los procesos, perpetración de fraudes o accesos a información confidencial.

Para el manejo de la seguridad de la información es necesario separar la función de seguridad y la de monitoreo ya que esto puede conducir a que se facilite la violación de las políticas de seguridad y la realización de actos prohibidos sin que nadie se de cuenta del problema.

---

[29] Seguridad Práctica en UNIX e Internet, Segunda Edición, Simson Gar Finkel y Spafford Gene, Mc. Graw Hill, 1999, Pag: 337.

2.6.6. Despidos y renuncias

La salida de un empleado es un punto crítico de riesgo para la organización.

En casos de problemas laborales y despidos, un empleado modelo hasta la fecha, puede convertirse en una seria amenaza, en estos casos hay que definir una sucesión de acciones para manejar la partida. Este procedimiento debe incluir el dar de baja a los empleados.

En muchas ocasiones, Recursos Humanos se encarga de realizar los trámites legales de la baja, mientras que el departamento de informática se ocupa de dar de baja sus accesos (en el momento en que perciben su ausencia). Este escenario acaba degenerando en problemas tales como que los accesos de los ex empleados siguen vigentes durante meses, o que tras la marcha del empleado no es posible recuperar cierta información vital que poseía.

Para evitar todo esto, se debe comunicar de las bajas tan pronto como se conozca de ellas, Recursos Humanos debe comunicar las bajas de personal a Seguridad y en la comunicación se debe indicar el nombre, la fecha efectiva de la baja, su clasificación y cualquier medida o control especial que sea necesario realizar.

2.7 Seguridad en Contrataciones externas o Outsourcing

Outsourcing o contratación externa consiste en el uso de recursos exteriores a la empresa para realizar actividades tradicionalmente ejecutadas por personal y recursos internos.

Es una estrategia de administración por medio de la cual una empresa delega la ejecución de ciertas actividades a empresas especializadas, pero el outsourcing representa riesgos en la seguridad de una organización.

2.7.1. Riesgos del outsourcing

Los riesgos involucrados en el proceso de Outsourcing pasan de ser riesgos operacionales a riesgos estratégicos(30).

(30) http://www.monografias.com/trabajos56/mpt/mpt.shtml

- <u>Riesgos operacionales</u>: Estos riesgos afectan más la eficacia de la empresa.

- <u>Riesgos estratégicos</u>: Afectan la dirección de la misma, su cultura, la información compartida, entre otras.

Los principales riesgos de Outsourcing son:

- No negociar el contrato adecuado.

- No adecuada selección del contratista.

- Puede quedar la empresa a mitad de camino si falla el contratista.

- Incrementa el nivel de dependencia de entes externos.

- Inexistente control sobre el personal del contratista.

- Incremento en el costo de la negociación y monitoreo del contrato.

- Falta de concienciación sobre seguridad de la información.

Al delegar un servicio a un proveedor externo las empresas están permitiendo que personas ajenas a la organización tengan la oportunidad de cometer actos ilícitos que pueden poner en peligro la información que se maneja dentro de la organización y otros activos de la empresa si no se cuenta con un control adecuado sobre las actividades de este personal.

Uno de los riesgos más importantes del Outsourcing es que el proveedor seleccionado no tenga las capacidades para cumplir con los objetivos y estándares que la empresa requiere del servicio que están brindando.

2.7.2. Requisitos de seguridad en el outsourcing

La empresa que solicita el outsourcing deberá tomar las providencias (procedimientos, recursos físicos y/o humanos, etc.) de que pueda disponer para asegurar la confidencialidad, integridad de su información a fin que ningún tercero tenga facilidad de acceso a la misma.

Ciertos procedimientos de seguridad que se deben tomar en cuenta al momento de contratar un outsourcing son:

- Realizar una evaluación y análisis de riesgos: Con el fin de determinar las implicaciones de seguridad y los controles que serán requeridos para proteger los activos de información del acceso de terceros; estos podrían ser.

  - Procedimientos para proteger los activos de la organización, incluida la información y el software.

  - Procedimientos para determinar si ha ocurrido algún incremento del riesgo de los activos como una pérdida o modificación de datos.

  - Restricciones en la copia y divulgación de la información.

  - Descripción de cada servicio que esté disponible.

  - Detalle de las respectivas obligaciones de las partes en el contrato.

- Responsabilidades sobre la instalación y mantenimiento del hardware y del software.

- Controles sobre el acceso de terceros a la organización.

* <u>Acuerdo y definición de los requerimientos y controles de seguridad en el contrato</u>: Estos deberán contener qué y cómo serán garantizados los requerimientos de seguridad.

Estas medidas de seguridad se tomarán en cuenta con el objeto de garantizar que los recursos y servicios provistos por terceros no impliquen una amenaza a la seguridad de la organización.

Se va ha considerar tocar este punto en vista que la empresa en la cual se ha desarrollado el caso práctico incluido en este trabajo, tiene un servicio del área de informática como es el de mantenimiento de los equipos a cargo de una empresa ajena a la organización.

2.8 Plan de contingencias

El plan de contingencias tiene como finalidad proveer a la organización de requerimientos para su recuperación ante desastres. En su elaboración deben intervenir los niveles ejecutivos de la organización, el personal usuario y el técnico de los procesos.

2.8.1. Contenido del plan de contingencias

El plan de contingencia deberá tomar en cuenta que debe ser eficaz y eficiente para lograr reestablecer las operaciones de la empresa. Este plan debe incluir:

La naturaleza, la extensión y la complejidad de las actividades de la organización.

- El grado de riesgo al que la organización está expuesta.
- El tamaño de las instalaciones de la organización (centro de cómputo y número de usuarios).
- La evaluación de los procesos críticos.

- La formulación de las medidas de seguridad necesarias dependiendo del nivel de seguridad requerido.

- La justificación del costo de implantar las medidas de seguridad.

2.8.2. Etapas del plan de contingencia

Entre las etapas del proyecto del plan de contingencias están:

- <u>Análisis del impacto en la organización.-</u> En esta etapa se identifican los procesos críticos o esenciales y sus repercusiones en caso de no estar en funcionamiento estos procesos.

- <u>Selección de la estrategia</u>.- Una vez definido el grado de riesgo, se elabora una lista de los sistemas con las medidas preventivas que se deben tomar, así como las correctivas en caso de desastre, señalándose a cada función su prioridad.

- Preparación del plan.- La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia. La estructura debe considerar facilitar su actualización

- Prueba.- Para la prueba del plan se seleccionará el personal que realice las actividades clave de éste. El grupo de recuperación en caso de emergencia debe estar integrado por personal de Sistemas. Cada miembro tendrá una tarea y se le asignará una persona de respaldo.

- Mantenimiento y reevaluación de los planes.- Este plan se debe mantener con ayuda de revisiones y actualizaciones regulares para asegurar la continuidad de su eficacia.

2.9 Definiciones conceptuales

Acción de contingencia.- Acción a realizar en caso de un incidente de seguridad.

Amenaza.- Cualquier evento que pueda provocar daño en los Sistemas de información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo.

Antivirus.- Dicho de un programa que detecta la presencia de virus y puede neutralizar sus efectos.

Análisis de riesgo.- Uso sistemático de la información para identificar las fuentes y estimar el riesgo.

Backup.- Copias de seguridad de los discos duros.

Base de Datos.- Cualquier conjunto de datos organizados para su almacenamiento en la memoria de un ordenador o computadora, diseñado para facilitar su mantenimiento y acceso de una forma estándar. Los datos suelen aparecer en forma de texto, números o gráficos. Hay cuatro modelos principales de bases de datos: el modelo jerárquico, el modelo en red, el modelo relacional (el más extendido hoy en día; los datos se almacenan en tablas a los que se accede mediante consultas escritas en SQL) y el modelo de bases de datos deductivas. Otra línea de investigación en este campo son las bases de datos orientadas a objeto, o de objetos persistentes.

Controles.- Comprende los métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos.

Copias de Seguridad.- Copia de un programa informático, de un disco o de archivo de datos, realizada para archivar su contenido o para proteger archivos valiosos contra su pérdida en caso de que la copia activa se dañe o quede destruida. Una copia de seguridad puede considerarse como una medida de seguridad contra la pérdida de datos producida por algún virus o por otro tipo de incidencia. Ciertos programas de aplicación realizan automáticamente copias de seguridad de archivos de datos, manteniendo en disco tanto la versión actual como la precedente.

Además, es una buena medida hacer copias de seguridad de programas o de datos valiosos de difícil reconstrucción.

Defensa.- Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo. Debe realizarse una valoración cuantitativa de su coste. Muchas veces se la conoce como medida de seguridad o prevención.

Encriptación.- Conjunto de técnicas que intentan hacer inaccesible la información a personas no autorizadas. Por lo general, la encriptación se basa en una clave, sin la cual la información no puede ser descifrada. Se puede hablar de dos sistemas de cifrado: sistemas simétricos, en los que se utiliza la misma clave para cifrar y descifrar el mensaje, y sistemas asimétricos, en los que se utiliza una clave para cifrar el mensaje y otra distinta para descifrarlo.

Evaluación del riesgo.- Evaluación de amenazas a la información, impactos sobre ésta y vulnerabilidades de ella y de los medios usados para su procesamiento, y de su probable ocurrencia.

Factores de riesgos.- Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad.

Firewall.- Cortafuegos, en seguridad informática, dispositivo que impide el acceso no autorizado a la red de área local de una organización; en inglés se denomina firewall. Puede estar implementado en hardware, software o una combinación de ambos.

El cortafuego puede residir en el servidor que actúa como gateway de la red de área local o en un sistema dedicado emplazado entre la red local e Internet, de manera que la red privada nunca accede a Internet directamente. Realiza el seguimiento de todos los archivos que entran o salen en la red de la organización para poder detectar el origen de virus o de intentos de acceso no autorizado.

El cortafuego se considera una primera línea de defensa en la protección de la información; para mayor seguridad se deben utilizar, por ejemplo, programas específicos de control de acceso, antivirus o copias de seguridad.

Gobierno de TI.- Es una estructura de procesos para dirigir y controlar a la organización con el fin de lograr sus objetivos mientras se equilibran los riesgos.

Hardware.- Equipo utilizado para el funcionamiento de una computadora. El hardware se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento.

Impacto.- Es la medición y valoración del daño que podría producir a la empresa un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles.

Incidente de seguridad.- Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza.

Internet.- Es una interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente, es decir, cada ordenador de la red puede conectarse a cualquier otro ordenador de la red. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También existen sistemas de redes más pequeños llamados intranets, generalmente para el uso de una única organización, que obedecen a la misma filosofía de interconexión.

Passwords.- También llamados User ID o Claves de Acceso son secuencias confidenciales de caracteres que permiten que los usuarios autorizados puedan acceder a un ordenador. Para ser eficaces, las claves de acceso deben resultar difíciles de adivinar.

Recurso de recuperación.- Recurso necesario para la recuperación de las operaciones en caso de desastre.

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

Redes de comunicación.- Posibilidad de compartir con carácter universal la información entre grupos de computadoras y sus usuarios; un componente vital de la era de la información.

Riesgo.- Proximidad o posibilidad de un daño, peligro, etc. Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Riesgo residual.- Nivel restante de riesgo después de que se han tomado medidas de procesamiento.

Software.- Conjunto de programas de computadoras. Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado. Las dos categorías primarias de software son los sistemas operativos (software del sistema), que controlan los trabajos del ordenador o computadora, y el software de aplicación, que dirige las distintas tareas para las que se utilizan las computadoras.

Seguridad.- Cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

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

Seguridad de la información.- Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Valoración del riesgo.- Proceso global de análisis y evaluación del riesgo.

Virus (informática).- Son programas, generalmente destructivos, que se introducen en el ordenador (al leer un disco o acceder a una red informática) y pueden provocar pérdida de la información (programas y datos) almacenada en el disco duro. Existen programas antivirus que los reconocen y son capaces de “inmunizar” o eliminar el virus del ordenador. Existen otros programas informáticos nocivos similares a los virus, pero que no cumplen ambos requisitos de reproducirse y eludir su detección. Estos programas se dividen en tres categorías: caballos de Troya, bombas lógicas y gusanos.

Vulnerabilidad.- Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

CAPÍTULO 3

1. NORMAS Y/O ESTANDARES INTERNACIONALS

Todo procedimiento informático debe estar apoyado en estándares y/o normas referentes a tecnología de información para que brinden la seguridad que la organización necesita.

Por este motivo el presente capítulo trata en forma resumida las normas y/ o estándares internacionales que guarden relación con la seguridad de información y que servirán de apoyo para la realización del caso práctico que presenta este trabajo de tesis en el siguiente capítulo.

3.1 COSO

El denominado informe COSO sobre control interno, publicado en Estados Unidos en 1992, surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno al control interno.

3.1.1 Definición y objetivos

La definición de COSO del control interno hace énfasis en que el control interno es un proceso, o un medio para llegar a un fin, y no un fin en sí mismo.

El Control Interno es un proceso integrado a los procesos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.

- Confiabilidad de la información financiera.

- Cumplimiento de las leyes, reglamentos y políticas.

El proceso se efectúa por medio de individuos, no solamente a partir de manuales de políticas, documentos y formas.

3.1.2 Fundamentos de Control Interno

El Control Interno comprende el plan de organización y la totalidad de los métodos, sistemas y procedimientos, que en forma ordenada, se adoptan en una organización, para asegurar la protección de todos sus recursos, la obtención de información correcta, segura y oportuna, la promoción de economía, eficiencia y efectividad operacional y la adhesión del personal a los objetivos y políticas debidamente predefinido por la dirección.

3.1.3 Componentes

El informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión que son:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control

- Información y comunicación

- Supervisión y seguimiento del sistema de control

Para un mejor control de las seguridades implementadas en la organización es que se toman en cuentan estos componentes para el desarrollo del caso práctico que se presenta en este trabajo.

3.1.3.1 Ambiente de control

Este componente se refiere al establecimiento de un entorno que estimule e influencie las actividades del personal con respecto al control de sus actividades.

Los principales factores del ambiente de control son:

- La filosofía y estilo de la dirección y la gerencia.

- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.

- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.

- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.

- El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

El ambiente de control reinante será tan bueno, regular o malo como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos hará, en ese mismo orden, a la fortaleza o debilidad del ambiente que generan y consecuentemente al tono de la organización.

Manejar un buen ambiente de control es imprescindible para disminuir los peligros a los que está expuesta la información por la falta de conocimiento de los empleados acerca de planes, reglamentos y otras políticas existentes en la organización, así como su falta de valores éticos.

Todos estos factores serán tomados en cuenta en el momento de analizar a los recursos humanos en el desarrollo del caso práctico

3.1.3.2 Evaluación de riesgos

El control interno ha sido pensado esencialmente para mitigar los riesgos que afectan las actividades de las organizaciones o transferirlos mediante el outsourcing de los servicios externos de tecnología de información.

La evaluación de riesgos se refiere a la identificación y análisis de riesgos relevantes para el logro de los objetivos y la base para determinar la forma en que tales riesgos deben ser manejados. Asimismo se refiere a los mecanismos necesarios para identificar y manejar riesgos específicos asociados con los cambios, tanto los que influyen en el entorno de la organización como en el interior de la misma.

Para llevar acabo este análisis es indispensable primeramente el establecimiento de objetivos tanto a nivel global de la organización como al de las actividades relevantes y una vez identificados, el análisis de los riesgos incluirá:

- Una estimación de su importancia / trascendencia.

- Una evaluación de la probabilidad / frecuencia.

- Una definición del modo en que habrán de manejarse.

Dado que las condiciones en que las entidades se desenvuelven suelen sufrir variaciones, se necesitan mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio.

Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión de los cambios merece efectuarse independientemente, dada su gran importancia y las posibilidades de que los mismos pasen inadvertidos para quienes están inmersos en las rutinas de los procesos.

Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean:

- Cambios en el entorno.

- Redefinición de la política institucional.

- Reorganizaciones o reestructuraciones internas.

- Ingreso de empleados nuevos, o rotación de los existentes.

- Nuevos sistemas, procedimientos y tecnologías.

- Aceleración del crecimiento.

- Nuevos productos, actividades o funciones.

Los mecanismos para prever, identificar y administrar los cambios deben estar orientados hacia el futuro, de manera de anticipar los más significativos a través de sistemas de alarma complementados con planes para un abordaje adecuado de las variaciones.

Este tipo de análisis es el que llevaremos a cabo para evaluar los riesgos que se presentan en la organización en la cual se realizó el trabajo práctico.

3.1.3.3 Actividades de control

Las actividades de control son aquellas que realiza la gerencia y demás personal de la organización para cumplir diariamente con actividades asignadas.

Estas actividades están relacionadas (contenidas) con las políticas, sistemas y procedimientos principalmente. Ejemplo de estas actividades son aprobación, autorización, verificación, conciliación, inspección, revisión de indicadores de rendimiento, también la salvaguarda de los recursos, la segregación de funciones, la supervisión y la capacitación adecuada.

Las actividades de control tienen distintas características. Pueden ser:

- Manuales o computarizadas
- Gerenciales u operacionales
- General o específicas.
- Preventivas o detectivas.

Sin embargo, lo trascendente es que sin importar su categoría o tipo, todas ellas estén apuntando hacia los riesgos (reales o potenciales) en beneficio de la organización, su misión y objetivos, así como a la protección de los recursos.

Para el desarrollo de nuestro trabajo se tomarán en cuenta que actividades de control son puestas en práctica en la organización donde se lo realizó.

3.1.3.4 Información y comunicación

Consecuentemente la información pertinente debe ser identificada, capturada, procesada y comunicada al personal dentro del tiempo indicado, de forma tal que le permita cumplir con sus responsabilidades.

Los sistemas producen reportes conteniendo información operacional, financiera y de cumplimiento que hace posible conducir y controlar la organización.

Todo el personal debe recibir un claro mensaje de la alta gerencia de sus responsabilidades sobre el control así como la forma en que las actividades individuales se relacionan con el trabajo de otros.

Asimismo, debe contarse con medios para comunicar información relevante hacia los mandos superiores, así como a entidades externas.

A continuación comento brevemente los elementos que integran a este componente y que serán tomados en cuenta para nuestro análisis y desarrollo del proyecto:

3.1.3.4.1 Información

La información tanto generada internamente como aquella que se refiere a eventos acontecidos en el exterior, es también parte esencial de la toma de decisiones así como del seguimiento de las operaciones.

La información cumple distintos propósitos a diferentes niveles de la organización.

Sin la información correcta sería imposible tomar decisiones que ayuden a la organización en su mejor desempeño, es po eso que será un punto importante para nuestro análisis.

3.1.3.4.1.1 Sistemas integrados a la estructura

No hay duda que los sistemas están integrados o entrelazados con las operaciones.

Sin embargo se observa una tendencia a que éstos deben apoyar de manera contundente la implantación de estrategias.

Los sistemas de información, como un elemento de control, estrechamente ligados a los procesos de planeación estratégicas son un factor clave de éxito en muchas organizaciones.

Debido a que el sistema de información influye sobre la capacidad de la dirección para tomar decisiones de gestión y control, la calidad de este resulta de gran trascendencia y se deben considerar los aspectos de contenido, oportunidad, actualidad, exactitud y accesibilidad del mismo para tener resultados correctos como se lo verá en el caso práctico.

3.1.3.4.1.2 Sistemas integrados a las operaciones

En este sentido es evidente cómo los sistemas son medios efectivos para la realización de las actividades de la empresa.

Desde luego el grado de complejidad varía según el caso, y se observa que cada día están más integrados con las estructuras o sistemas de la organización.

La información vital de la organización es manejada en el sistema, el cual debe ser considerado un punto relevante que tiene que estar protegido de cualquier amenaza. En nuestra práctica se definen algunos métodos de seguridad para protegerlos.

3.1.3.4.1.3 La calidad de la información

La información es tan trascendente que constituye un activo, un medio y hasta una ventaja competitiva en todas las organizaciones importantes, ya que está asociada a la capacidad gerencial de las empresas.

La información, para actuar como un medio efectivo de control, requiere de las siguientes características: relevancia del contenido, oportunidad, actualización, exactitud y accesibilidad, principalmente. Para lograr esto se debe invertir en una cantidad importante de recursos.

De la calidad de la información dependerá las decisiones que se tomen en la organización es por eso importante mantener su integridad como lo veremos reflejado en el caso práctico.

3.1.3.4.2 Comunicación

Al respecto también es claro que deben existir adecuados canales para que el personal conozca sus responsabilidades sobre el control de sus actividades.

Estos canales deben comunicar los aspectos relevantes del sistema de información indispensable para los gerentes, así como los hechos críticos para el personal encargado de realizar las operaciones críticas. También los canales de comunicación entre la gerencia y el consejo de administración o los comités son de vital importancia.

En relación con los canales de comunicación con el exterior, éstos son el medio a través del cual se obtiene o proporciona información relativa clientes, proveedores, contratistas, entre otros.

Así mismo son necesarios para proporcionar información a las entidades reguladoras sobre las operaciones de la empresa e inclusive sobre el funcionamiento de su sistema de control.

La comunicación es importante dentro de una organización para facilitar la relación con los integrantes de la misma con la finalidad de mantener un control que disminuya los riesgos por la falta de la misma.

Es así que constituye una parte importante para el desarrollo de nuestro trabajo.

3.1.3.5 Supervisión y seguimiento del sistema de control

En general los sistemas de control están diseñados para operar en determinadas circunstancias, claro está que para ello se tomaron en consideración los riesgos y las limitaciones inherentes al control; sin embargo, las condiciones evolucionan debido tanto a factores externos como internos colocando con ello que los controles pierdan su eficiencia.

Como resultado de todo esto, la gerencia debe llevar a cabo la revisión y evaluación sistemática de los componentes y elementos que forman parte de los sistemas.

Esto no significa que tengan que revisarse todos los componentes y elementos, como tampoco que deba hacerse al mismo tiempo.

Esto dependerá de las condiciones específicas de cada organización, de los distintos niveles de riesgos existentes y del grado de efectividad mostrado por los distintos componentes y elementos de control.

La evaluación debe conducir a la identificación de los controles débiles, insuficientes o necesarios, para promover con el apoyo decidido de la gerencia, su reforzamiento e implantación.

Esta evaluación puede llevarse a cabo de tres formas: durante la realización de las actividades de supervisión diaria en distintos niveles de la organización; de manera independiente por personal que no es responsable directo de la ejecución de las actividades (incluidas las de control) o mediante la combinación de las dos formas anteriores.

Se puede concluir que es fundamental realizar evaluaciones de los controles que se llevan acabo en la organización para verificar que estos están cumpliendo su objetivo que es el de disminuir los riesgos a los que se expone la información de la organización.

Esta misma evaluación es la que realizaremos en nuestro trabajo con el objetivo de medir la funcionalidad de los controles de seguridad que en la empresa se hayan implantado.

3.2 COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas)

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI.

Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos.

COBIT está basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

3.2.1 Misión

COBIT investiga, desarrolla, publica y promueve un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores.

3.2.2 Usuarios

Los usuarios de cobit son aquellos quienes desean mejorar y garantizar la seguridad de sus sistemas bajo un estricto método control de tecnología de información como lo es COBIT:

- La gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.

- Los usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.

- Los auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

- Los responsables de TI: para identificar los controles que requieren en sus áreas.

También puede ser utilizado dentro de las empresas por el responsable de un proceso de negocio en su responsabilidad de controlar los aspectos de información del proceso, y por todos aquellos con responsabilidades en el campo de la TI en las empresas.

3.2.3 Características de COBIT

- Orientado al negocio.

- Alineado con estándares y regulaciones “de facto”.

- Basado en una revisión crítica y analítica de las tareas y actividades en TI.

- Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

3.2.4 Principios de COBIT

El concepto fundamental del marco referencial COBIT se refiere a que el enfoque del control en TI (Tecnología de información) se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la tecnología de información que deben ser administrados por procesos de TI.

Así como podemos observarlo en esta figura 3.1 que nos presenta los principios de COBIT.

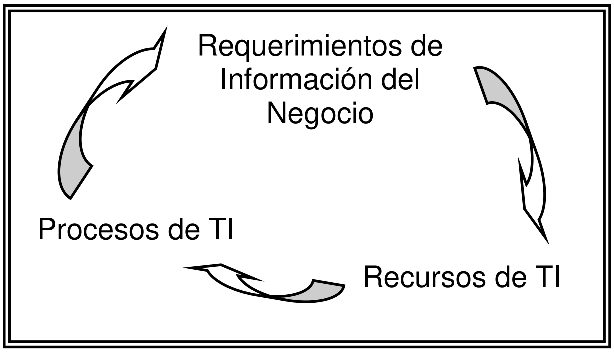

FIGURA 3.1 Principios de COBIT

3.2.4.1 Requerimientos de la información del negocio

Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios**:**

- <u>Requerimientos de Calidad</u>: Calidad, Costo y Entrega.

- Requerimientos Fiduciarios: Se refiere a la efectividad, eficiencia, confiabilidad y cumplimiento.
  - Efectividad: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.
  - Eficiencia: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).
  - Confiabilidad: proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.
  - Cumplimiento: de las leyes, regulaciones y compromisos contractuales con los cuales está comprometida la empresa.
- Requerimientos de Seguridad: Confidencialidad, Integridad y Disponibilidad.

- Confidencialidad: Protección de la información sensible contra divulgación no autorizada

- Integridad: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.

- Disponibilidad: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.

3.2.4.2 Recursos de TI

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

- Datos: Todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.

- <u>Aplicaciones</u>: entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.

- <u>Tecnología</u>: incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

- <u>Instalaciones</u>: Incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

- <u>Recurso Humano</u>: Por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

3.2.4.3 Procesos de TI

La estructura de COBIT se define a partir de una premisa simple y pragmática:

“Los recursos de las Tecnologías de la Información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos”. COBIT se divide en tres niveles como la figura 3. 2 nos presenta:

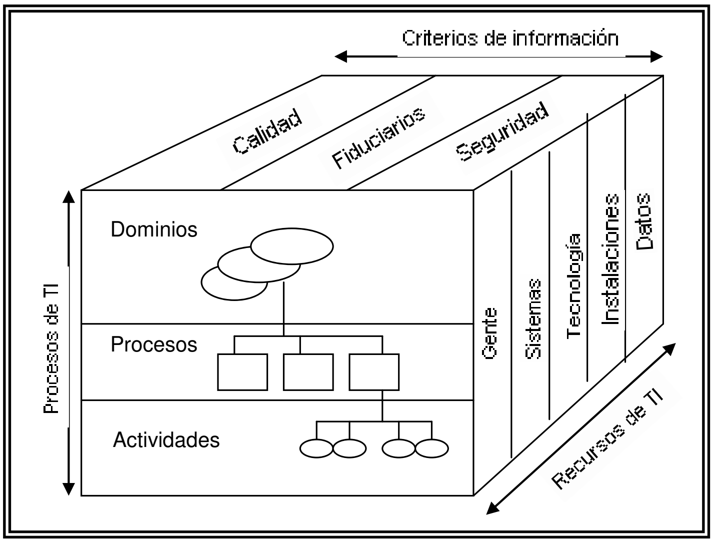

FIGURA 3.2 Niveles de COBIT

- **Dominios**: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.

- **Procesos:** Conjuntos o series de actividades unidas con delimitación o cortes de control.

- **Actividades:** Acciones requeridas para lograr un resultado medible.

Se definen 34 objetivos de controles generales, uno para cada uno de los procesos de las TI. Estos procesos están agrupados en cuatro grandes dominios que son:

- Planeación y Organización
- Adquisición e Implementación
- Prestación y Soporte
- Monitoreo

De estos sólo tomaremos en consideración los procesos que guarden relación con el tema de seguridad de información que es el objetivo de análisis de nuestro trabajo, los cuales son:

- Planeación y organización
    - Definición de un plan estratégico.

- Evaluación de riesgos.

- Adquisición e implementación.

  - Adquisición y mantenimiento de la infraestructura tecnológica.

  - Desarrollo y mantenimiento de procedimientos.

- Entrega de servicios y soporte.

  - Administración de servicios prestados por terceros.

  - Garantizar la seguridad de sistemas.

  - Educación y entrenamiento de usuarios.

  - Apoyo y asistencia a los clientes de TI.

  - Administración de problemas e incidentes.

  - Administración de las instalaciones.

3.2.4.3.1 Planeación y organización

Se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio.

Los siguientes procesos que integran este dominio de COBIT serán considerados en el análisis de nuestro trabajo práctico.

3.2.4.3.1.1 Definición de un plan estratégico

Con este plan se desea lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio, para asegurar sus logros futuros.

Su realización se concreta a través un proceso de planeación estratégica emprendido en intervalos regulares dando lugar a planes a largo plazo, los que deberán ser traducidos periódicamente en planes operacionales estableciendo metas claras y concretas a corto plazo, teniendo en cuenta:

- La definición de objetivos de negocio y necesidades de TI, la alta gerencia será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas generales de la organización.

- El inventario de soluciones tecnológicas e infraestructura actual, se deberá evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

- Los cambios organizacionales, se deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la TI.

- Estudios de factibilidad oportunos, para que se puedan obtener resultados efectivos.

3.2.4.3.1.2 Evaluación de riesgos

Es necesaria para asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI.

Para llevarla acabo se logra la participación de la propia organización en la identificación de riesgos de TI y en el análisis de impacto, tomando medidas seguridad para mitigar los riesgos y para realizarlo se toma en consideración:

- Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI. Estos riesgos pueden ser tecnológicos, de seguridad, entre otros y una vez identificados se puede determinar la manera en la que estos deben ser manejados a un nivel aceptable.

- Definición de alcances, limites de los riesgos y la metodología para las evaluaciones de los riesgos.

- Actualización de evaluación de riesgos

- Metodología de evaluación de riesgos

- Medición de riesgos cualitativos y/o cuantitativos

- Definición de un plan de acción contra los riesgos. Esto servirá para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

- Aceptación de riesgos. Dependerá de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

3.2.4.3.2 Adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio.

Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes. Para el análisis del trabajo que se desarrollará en el próximo capítulo se a considerado los procedimientos que se detallan a continuación.

3.2.4.3.2.1 Adquisición y mantenimiento de la infraestructura tecnológica

El objetivo principal de este proceso es el de proporcionar a la empresa plataformas apropiadas para soportar las aplicaciones que en el negocio se manejen.

Para el desarrollo de nuestro proyecto se evaluará el mantenimiento hardware y la seguridad, tomando en consideración:

- Mantenimiento preventivo del hardware. Cuyo objetivo será el de reducir la frecuencia y el impacto de fallas de rendimiento.

- Seguridad del software de sistema, instalación y mantenimiento. Será evaluado con la finalidad de no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

3.2.4.3.2.2 Desarrollo y mantenimiento de procedimientos

Asegurar el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas es el objetivo de toda organización, y una forma de mantener su seguridad.

Para esto se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:

- Manuales de procedimientos de usuarios y controles. Para el mejor desempeño y control de los usuarios estos deben estar actualizados.

- Manuales de Operaciones y controles. Deben estar permanentemente actualizados.

- Materiales de entrenamiento. Estos deben ser enfocados al uso del sistema en la práctica diaria.

Para fines del análisis y desarrollo del caso práctico se realizará la constatación de estos manuales como medida de seguridad.

3.2.4.3.3 Entrega de servicios y soporte

Este dominio hace referencia a la entrega de los servicios requeridos, que abarcan desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad.

Con el fin de proveer servicios, se deben establecer los procesos de soporte necesarios y los adecuados controles de las aplicaciones para asegurar el procesamiento de los datos, se ha seleccionado ciertos procesos de este dominio de COBIT que guardan relación con nuestro trabajo práctico y que podrán ayudarnos para su estudio y su elaboración.

3.2.4.3.4 Administración de servicios prestados por terceros

Es necesario asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos de la organización.

Por este motivo se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización se toma en consideración:

- Acuerdos de servicios con terceras partes. Estos acuerdos se llevan a cabo a través de contratos entre la organización y el proveedor de la administración de instalaciones este basado en niveles de procesamiento requeridos, seguridad, monitoreo y requerimientos de contingencia, así como en otras estipulaciones según sea apropiado.

- Acuerdos de confidencialidad. Deberán estar estipulados y acordados en los contratos que se realicen para cada servicio prestado por un tercero.

- Requerimientos legales regulatorios. Se definen con el objetivo de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.

- Monitoreo. Con el fin de asegurar el cumplimiento de los contratos se lleva un registro de la entrega de servicio.

Otro punto que se tomará en cuenta al momento de realizar el caso práctico es este proceso, ya que se deben tener medidas de seguridad con los servicios de outsourcing.

3.2.4.3.4.1 Garantizar la seguridad de sistemas

Para salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, se deben realizar controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados para su seguridad se toma en consideración:

- Perfiles e identificación de usuarios. Se realiza estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión y suspensión de cuentas de usuario.

- Prevención y detección de virus. Los virus son controlados estableciendo adecuadas medidas de control preventivas, detectivas y correctivas.

- Utilización de Firewalls. Son necesarios si existe una conexión con Internet u otras redes públicas en la organización.

Este proceso será considerado para la realización de nuestro proyecto. Por el motivo de ser medidas de protección a los sistemas informáticos.

3.2.4.3.4.2 Educación y entrenamiento de usuarios

Tiene como fin asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades que tienen.

Para mantener la seguridad en las actividades de los usuarios se emplean técnicas de concientización que se ejecutan proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

Es importante que una organización se asegure que los integrantes de ella manejen los sistemas de información correctamente de tal manera que disminuyan los riesgos que de ellos puedan surgir.

Emplearemos este proceso para el desarrollo de nuestro trabajo.

3.2.4.3.4.3 Apoyo y asistencia a los clientes de TI

Este dominio tiene como objetivo es asegurar que cualquier problema experimentado por los usuarios sea atendido apropiadamente y para su realización se proporciona soporte y asesoría de primera línea considerando:

- Consultas de usuarios y respuesta a problemas. Se efectúa estableciendo un soporte de ayuda para cualquier problema.

- Monitoreo de consultas y despacho. Es el registro de todas las consultas, procedimientos de solución y fecha en que se soluciono el problema.

Llevar un adecuado control de las fallas que presenta el sistema o los equipos y las soluciones que se les dan a las mismas es fundamental considerar para nuestro trabajo.

3.2.4.3.4.4 Administración de problemas e incidentes

Es primordial asegurar que los problemas e incidentes sean resueltos y que sus causas sean investigadas para prevenir que vuelvan a suceder.

Una solución eficiente es implementar un sistema de manejo de problemas, que se lo efectúa con el propósito de que se registre y dé seguimiento a todos los incidentes.

Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado.

Los problemas deben ser resueltos y llevar un control de la solución que se le a dado es la mejor manera de evitar que se vuelva a presentar ya que se podrían corregir las fallas que lo originaron con este fundamento es que se trabajará el caso práctico.

3.2.4.3.4.5 Administración de las instalaciones

Es objetivo de toda organización proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales (fuego, polvo, calor excesivos) o fallas humanas lo cual se hace posible con la instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

Mantener la seguridad física en la organización es un punto que contiene nuestro trabajo y es así que este proceso formará parte de su desarrollo.

3.3 Norma ISO 17799

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada.

El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

- **Confidencialidad**. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

- **Integridad**. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.

- **Disponibilidad**. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

La norma ISO 17799 establece <u>diez dominios de control</u> que cubren por completo la gestión de la seguridad de la información:

1. Política de seguridad.

2. Aspectos organizativos para la seguridad.

3. Clasificación y control de activos.

4. Seguridad ligada al personal.

5. Seguridad física y del entorno.

6. Gestión de comunicaciones y operaciones.

7. Control de accesos.

8. Desarrollo y mantenimiento de sistemas.

9. Gestión de continuidad del negocio.

10. Conformidad con la legislación.

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

3.3.1 Política de seguridad

Objetivo.-

- Dirigir y dar soporte a la gestión de la seguridad de la información.

La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.

La política se constituye en la base de todo el sistema de seguridad de la información. Y la alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

3.3.2 Aspectos organizativos para la seguridad

Objetivo.-

1. Gestionar la seguridad de la información dentro de la organización.

2. Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.

3. Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma.

Dicha estructura debe poseer un enfoque multidisciplinar: los problemas de seguridad no son exclusivamente técnicos.

3.3.3 Clasificación y control de activos

Objetivo.-

1. Mantener una protección adecuada sobre los activos de la organización.

2. Asegurar un nivel de protección adecuado a los activos de información.

Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

3.3.4 Seguridad ligada al personal

Objetivo.-

1. Reducir los riesgos de errores humanos, robos o mal uso de las instalaciones y los servicios.

2. Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad.

3. Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

4. Las implicaciones del factor humano en la seguridad de la información son muy elevadas.
5. Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.

6. Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc.

7. Procesos de notificación de incidencias claros, ágiles y conocidos por todos.

3.3.5 Seguridad física y del entorno

Objetivo.-

1. Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

2. Evitar pérdidas, daños de los activos así como la interrupción de las actividades de la organización.

3. Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

Las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

3.3.6 Gestión de comunicaciones y de operaciones

Objetivo.-

1. Asegurar la operación correcta y segura de los recursos de tratamiento de información.

2. Minimizar el riesgo de fallos en los sistemas.

3. Proteger la integridad del software y de la información.
4. Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

5. Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

6. Evitar daños a los activos e interrupciones de actividades de la organización.

7. Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas de información la empresa con el fin de que la información este disponible y sea confiable para la organización..

3.3.7 Control de accesos

Objetivo.-

1. Controlar los accesos a la información.

2. Evitar accesos no autorizados a los sistemas.

3. Evitar el acceso de usuarios no autorizados.

4. Protección de los servicios en red.

5. Evitar accesos no autorizados a ordenadores.

6. Evitar el acceso no autorizado a la información contenida en los sistemas.

7. Detectar actividades no autorizadas.

Estableciéndose controles de acceso adecuados se puede proteger los sistemas más críticos de la organización.

3.3.8 Desarrollo y mantenimiento de sistemas

Objetivo.-

1. Asegurar que la seguridad está incluida dentro de los sistemas de información.

2. Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

3. Proteger la confidencialidad, autenticidad e integridad de la información.

4. Asegurar que los proyectos de TI y las actividades complementarias son llevadas a cabo de una forma segura.

5. Mantener la seguridad del software y la información de la aplicación del sistema.

Debe contemplarse la seguridad de la información en el proceso de desarrollo o mejoramiento de un sistema.

3.3.9 Gestión de continuidad del negocio

Objetivo.-

1. Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.

Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.

Los planes de contingencia deben ser probados y revisados periódicamente.

Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre y poder continuar con las operaciones de la empresa a pesar de las dificultades presentadas.

3.3.10 Conformidad con la legislación

Objetivo.-

1. Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.

2. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.

3. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

Se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos (Ley de comercio electrónico), integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.

Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

3.4 Norma ISO 27001

El estándar ISO/IEC 27001 es un nuevo estándar oficial, publicada la primera versión el 15 de octubre de 2005, su título completo en realidad es “BS 7799-2:2005 (ISO/IEC 27001:2005)**“,** ya que es una versión actual del ISO-17799.

Actualmente es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

Esta norma propone orientar los aspectos netamente organizativos.

Su propósito es “Organizar la seguridad de la información”, por ello propone toda una secuencia de acciones destinados al establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System/Dirección de la seguridad de sistemas de información).

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en:

- ISMS (Information Security Management System/Administración de la seguridad de los sistemas de información).

- Responsabilidades de la Administración.

- Auditoría Interna del ISMS.

- Administración de las revisiones del ISMS.

- Mejoras del ISMS.

Estos puntos estarán presentes durante la elaboración y estudio de nuestro trabajo práctico.

3.4.1 ISMS (Information Security Management System/Dirección de la seguridad de los sistemas de información)

Indica que la organización, establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado ISMS en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos y todos los documentos requeridos por el ISMS serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

1. Aprobar documentos y prioridades o clasificación de empleo del documento.

2. Revisiones, actualizaciones y re-aprobaciones de documentos.

3. Asegurar que los cambios y las revisiones de documentos sean identificados.
4. Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.

5. Asegurar que los documentos permanezcan legibles y fácilmente identificables.

6. Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.

7. Asegurar que los documentos de origen externo sean identificados.

8. Asegurar el control de la distribución de documentos.

9. Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

3.4.2 Responsabilidades de la administración

Esta norma establece que la administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:

1. Establecimiento de la política del ISMS.

2. Asegurar el establecimiento de los objetivos y planes del ISMS.

3. Establecer roles y responsabilidades para la seguridad de la información.

4. Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.

5. Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el ISMS.

6. Decidir los criterios de aceptación de riesgos y los niveles del mismo.

7. Asegurar que las auditorias internas del ISMS, sean conducidas y a su vez conduzcan a la administración para la revisión del ISMS.

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el ISMS sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

3.4.3 Auditoria interna del ISMS

La organización realizará <u>auditorias internas al ISMS a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar</u>

acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoria, los informes resultantes y el mantenimiento de los registros serán definidos en un procedimiento.

3.4.4 Administración de las revisiones del ISMS

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el ISMS incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, como se mencionó en el punto anterior serán claramente documentados y los mismos darán origen a esta actividad.

3.4.5 Mejora del ISMS

La organización deberá mejorar continuamente la eficiencia del ISMS a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorias, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

CAPÍTULO 4

4. CASO PRÁCTICO

En el presente capítulo se llevará a cabo la elaboración del plan de seguridad informática realizado a raíz de los resultados que de la evaluación de riesgos llevada a cabo en la empresa la cual por ética profesional nos reservaremos su nombre, el de los integrantes del área de sistemas y recursos humanos; usaremos el nombre ficticio de “AGROPEC S.A.” para identificarla y datos ficticios para sus integrantes.

4.1 Descripción de la empresa

AGROPEC S.A., cuenta con una casa matriz y una sucursal en la ciudad de Guayaquil y otra oficina en Quito.

Fue fundada el 26 de enero de 1966. Su objetivo es proveer productos y servicios de calidad en forma ágil y oportuna que contribuyan a aumentar la productividad de la industria y del sector agrícola ecuatoriano.

AGROPEC S.A. se encuentra estructurada operativamente por dos divisiones que son: "Agroquímicos y Lubricantes" e "Industrial Agrícola y Marina" cada una es administrada independientemente tanto, física como administrativa y financiera.

Para el desarrollo de sus operaciones Agropec S.A. cuenta con 163 empleados, distribuidos en la siguiente forma:

- División Agroquímicos y Lubricantes: 68 empleados

- División Agrícola y Marina: 95 empleados

AGROPEC S.A. es una de las principales empresas importadoras para el Ecuador en sus líneas de negocios, el factor esencial de su crecimiento son los productos que distribuye como bienes de capital para la industria tales como equipos de generación eléctrica, motores industriales y marinos, bombas de agua, tractores, filtros, baterías, repuestos e insumos agrícolas todos de más alta calidad y bajo la representación de corporaciones de prestigio mundial como: Detroit Diesel Corporation, A. C. Delco, G. M. Kohler Co., Dow Agrosciences, F. M. C., BASF, etc., cuya credibilidad y calidad de los productos garantiza el éxito de Agropec S.A..

Su estrategia de negocio está basada en el monitoreo y control del producto desde la entrega al cliente hasta su uso en el campo y la industria.

4.2 Motivos para diseñar un plan estratégico de seguridad de información

Entre los principales justificativos o motivos para desarrollar este plan estratégico de seguridad informática encontramos los siguientes:

- Interés de los Gerencia en conocer la situación informática de la empresa determinando las vulnerabilidades existentes en lo relativo a controles de seguridad.

- Preocupación de los Gerencia en proteger sus sistemas frente a intrusos y visitantes no deseados que puedan atentar contra sus actividades.

- Deseo de los Gerencia de establecer un esquema de seguridad y control en informática.

- Interés de los Gerencia en asegurar que se cubra y proteja los recursos con mayores riesgos y exposiciones existentes en el medio informático del negocio.

- Voluntad de los Gerencia de fortalecer la compañía a nivel de seguridad para lograr el avance y optimizar sus recursos.

- Interés de los Gerencia de asegurar el uso eficiente de los recursos informáticos, orientándolos al logro de los objetivos y las estrategias de la organización.

- Preocupación de los Gerencia en disminuir el tiempo de producción perdido y consumo de recursos en horas de recuperación de la actividad normal de la empresa para garantizar la continuidad de los servicios frente algún contingente.

4.3 Objetivos

Los objetivos que se plantean para este plan de seguridad de información son:

4.3.1 Objetivo general

Diseñar un plan estratégico de seguridad de información para una empresa comercial.

4.3.2 Objetivos específicos

- Diseñar un modelo de seguridad orientado al cumplimiento de normas, procedimientos y estándares informáticos con el objetivo de crear una cultura de seguridad en la organización.

- Mejorar las seguridades existentes requeridas para la salvaguarda de la integridad de la información procesada en cuanto a totalidad y exactitud.

4.4 Alcance

El diseño de políticas de seguridad informática planteadas a partir de los resultados del análisis de riesgo cuyos factores de riesgo son el resultado de las evaluaciones a las seguridades físicas, lógicas, redes, recursos humanos y outsourcing de la entidad y fundamentadas en las normas y/o estándares de seguridad informática mencionadas en el capítulo 3.

Estas políticas serán puestas en práctica por la empresa mediante la ejecución del diseño del plan estratégico de seguridad que será desarrollado para ser aplicado de forma anual.

El diseño de este plan estratégico trata de cubrir los objetivos que la empresa está en capacidad de llevar a cabo para disminuir los riesgos a los que está expuesta.

Este plan de seguridad servirá como una guía aplicable a cualquier otra empresa y podrá ser implementado en toda la organización pero deberá ser dirigido por el Jefe de Seguridad y a falta de este el Jefe de Sistemas; el cual se hará responsable de que dichas políticas de seguridad sean cumplidas a cabalidad por todos los integrantes de la compañía.

4.5 Equipo de Trabajo

Este trabajo será realizado por dos personas, quién está redactando María Gabriela Hernández Pinto dirigida por su Directora de Tesis la Ing. Alice Naranjo.

4.6 Descripción del entorno informático

La empresa cuenta con un área destinada para el funcionamiento del departamento de sistemas que está integrado actualmente por el jefe y asistente de sistemas; los cuales tienen las siguientes funciones dentro del área.

Jefe de sistemas:

- Administrar los recursos del área.
- Control y mantenimiento de la red y programas que dan servicio a la empresa.
- Gestión de las adquisiciones de equipos.
- Control del mantenimiento a los equipos.

- Implementación de nuevas aplicaciones para mejorar el sistema.

- Elaboración de un plan tecnológico.

<u>Asistente de sistemas</u>:

- Dar soporte técnico a los usuarios.

- Realizar los inventarios de los equipos en conjunto con personal de contabilidad.

- Chequear las conexiones de datos con las oficinas regionales.

- Realizar correcciones de datos por errores de usuarios.

- Ciertas tareas de programación.

La función del departamento de sistemas es la de estructurar sus servicios y proyectos con base en los requerimientos específicos del negocio, apoyándose en la tecnología de vanguardia disponible y que está a su alcance pero se debe acotar que el área de sistemas no cuenta con asesoramiento en materia de seguridad informática, no han realizado evaluaciones a la seguridad informática y por lo tanto no existen políticas formales de seguridad.

Los objetivos del área de sistemas como el departamento encargado de resguardar la información esencial del negocio son:

- Mejorar la plataforma tecnológica con el fin de optimizar los procesos operativos de la empresa.

- Mantener la información disponible y generar nueva información estadística en base a la necesidad de la gerencia.

- Mediante el uso de la tecnología minimizar los costos operativos y de los servicios.

- Mantener el buen funcionamiento de los equipos de la red de computación y los programas.

Las actividades que lleva a cabo el área de sistemas dentro de la organización son las siguientes:

- Control de Inventario.

- Desarrollo de nuevas opciones en el sistema.
- Soporte a los usuarios.
- Mantenimiento de la red.
- Mantenimiento de la base de datos.
- Mantenimiento de la conexión a internet.
- Control del consumo telefónico.
- Control del uso de las impresoras.
- Control de nuevas adquisiciones tecnológicas por ejemplo protectores electrónicos.
- Correcciones en la base de datos como eliminaciones, cambio de fechas a movimientos, previa autorización del jefe de área y gerencia.
- Esquemas de seguridad mencionados anteriormente.

Existe un servicio de informática que es ofrecido por un tercero, se mantiene un contrato de outsourcing con INFOEXPRESS, quienes son los encargados de ofrecer el servicio de mantenimiento a los equipos dentro de la organización.

Los equipos con que cuenta la organización para el desarrollo de las actividades de la empresa son lo suficientemente aptos para los requerimientos de la compañía, tanto en capacidad de procesamiento como en su almacenamiento.

4.6.1 Arquitectura informática

4.6.1.1 Entorno de red de computadoras

La organización dispone de veinte y nueve equipos integrados a la red dentro de los cuales están los servidores de producción, desarrollo e internet y demás estaciones de trabajo.

La empresa cuenta con una red LAN con conexión ethernet 10/100 base T con una topología de red estrella, el medio de transmisión que utilizan para comunicarse con las sucursales del centro y Quito es vía modem.

Su cableado es estructurado, con cables del tipo UTP categoría 5 y su proveedor de servicio de internet es Telconet.

4.6.1.2 Equipos disponibles

En toda la organización se cuenta con veinte y nueve equipos de cómputo distribuidos en todos los ocho departamentos que conforman la empresa.

Dentro del área de sistemas encontramos cuatro servidores los cuales están bajo la responsabilidad del jefe de sistemas, con distintas funciones identificadas a continuación:

- Base de Datos
- Firewall (propiedad de TELCONET)
- IAC (propiedad de TELCONET)

- Acceso de datos para la sucursal de Quito (propiedad de TELCONET).

Además cuentan con tres computadoras para uso de los integrantes del área, pero solo dos de ellos están en funcionamiento los cuales están a cargo del jefe y asistente de sistemas el tercer computador está destinado para el auxiliar de sistemas puesto que está vacante actualmente; también se encuentran de los equipos de red y comunicación un switch, un hub y dos modems.

4.6.1.3 Sistema Operativo

El sistema operativo instalado en los servidores de producción es Windows NT 4.0 Server pero el resto de computadoras posee diferentes versiones de Windows (95, 98, ME, XP) de acuerdo a las capacidades de cada equipo.

4.6.1.4 Software de Sistemas y Utilitarios

4.6.1.4.1 Lenguajes de Programación

En el área de sistemas se manejan dos lenguajes de programación:

- SQL Server versión 6.5 para los procesos en la Base de Datos.

- Power Builder versión 5.04 para hacer las interfases en caso de mejoras de las aplicaciones.

4.6.1.4.2 Sistema de aplicación

La empresa cuenta con un sistema administrativo financiero llamado Spyral cuyos módulos son:

- Facturación y Cuentas por Cobrar

- Tesorería
- Inventario

- Contabilidad

- Control de Bodegas

- Reportes Estadísticos
- Seguridad

4.6.1.4.3 Software Básico y Utilitarios

La organización cuenta con los siguientes software básico y utilitarios como apoyo para el desarrollo de sus actividades:

- Sistemas Operativos:
    - Windows 95, 98, ME, XP, NT
    - LINUX
- Utilitarios:
    - Office 97
    - Outlook Express

- Mira scan

- Epson scan

- Microsoft SQL Server 6.5

- Acrobat reader

- CCT (software de control de consumo telefónico)

- Nero

- Antivirus: AVG, Norton 2005, Antivid

4.7 Identificación de los riesgos

Una vez establecidos los objetivos y el alcance de este trabajo, se desarrollaron cuestionaros para evaluar las seguridades existentes (**Ver Anexo 5 al 20**) los cuales fueron respondidos por los dos miembros del área de sistemas y solo uno de ellos por el jefe de recursos humanos que es a quién le correspondía debido a su fin.

De las respuestas obtenidas con las evaluaciones a las seguridades informáticas se pudo obtener las vulnerabilidades que originan los factores de riesgo (**Ver Anexo 21**) a los que la empresa esta expuesta. Estos factores de riesgo para el propósito de su análisis reflejan un criterio (**Ver Anexo 22**) formado a consecuencia de las evidencias encontradas a raíz de los cuestionarios.

4.8 Análisis de riesgos

Para efectuar el análisis de riesgos se llevaron a cabo los siguientes pasos:

- Ponderación de los factores de riesgo.
- Valoración de los riesgos.

- Matriz Descriptiva de Factores y Valoración asociada a los recursos informáticos.

- Matriz Ponderada de Factores y Valoración asociada a los recursos informáticos.

- Matriz Categorizada

4.8.1 Ponderación de los factores de riesgo

Una vez identificados los factores de riesgo con la ayuda de los integrantes del área de sistemas se procedió a la ponderación en términos porcentuales de los mismos (**Ver Anexo 23**) dando a cada uno de ellos su valor de importancia dentro de la organización:

- Sistema de Control.
- Nivel de sensibilidad.
- Complejidad.
- Materialidad.
- Imagen.
- Tiempo de realización de Auditorías previas.
- Respuesta ante fallas (Planes de contingencia).

Todos estos factores de riesgos serán valorados de acuerdo a los criterios por los cuales fueron escogidos.

4.8.2 Valoración de los riesgos

Una vez que los riesgos han sido identificados procedemos a valorarlos (**Ver Anexo 24**), definiendo una escala de riesgos (Alto, Medio Alto, Medio Bajo y Bajo), dicha escala será asignada de acuerdo al nivel de riesgo que representa ese factor basado en los criterios por el cual fue escogido como riesgo para la organización.

4.8.3 Matriz Descriptiva de Factores y Valoración asociada a los recursos informáticos.

Mediante la ayuda de una matriz denominada “Descriptiva” (**Ver Anexo 25**) se confrontan los recursos informáticos de la empresa con los factores de riesgo determinados mediante las evaluaciones a las seguridades. El puntaje que se le asigna a cada recurso informático al ser valorado con cada factor de riesgo es dado bajo el criterio especificado en la valoración de los factores de riesgo.

4.8.4 Matriz Ponderada de Factores y Valoración asociada a los recursos informáticos.

Para realizar está matriz definida como “Matriz Ponderada” (**Ver Anexo 26**) nos ayudamos de la matriz creada anteriormente que es la Matriz Descriptiva y le incluimos la ponderación de los factores de riesgo. Pero a diferencia de la anterior matriz en esta calculamos un total de la siguiente manera:

i. Multiplicamos la valoración de cada recurso informático por su correspondiente ponderación del factor de riesgo.

ii. Finalmente sumamos cada multiplicación obteniendo un total para cada recurso informático.

Obteniendo este resultado determinamos el grado de prioridad en el que estos riesgos deben ser mitigados por la organización, considerando al de mayor puntaje como el más importante.

4.8.5 Matriz Categorizada

Finalmente para determinar que recursos informáticos tienen una prioridad de riesgo alto, medio y bajo realizamos está matriz (**Ver Anexo 26**). Guiándonos con los siguientes pasos:

1. Ordenamos la columna total de mayor a menor.

2. Determinamos un rango que nos ayudará a encontrar un tamaño de intervalo para definir nuestra escala de riesgo.

3. Establecemos la escala de riesgo, definiendo intervalos para cada categoría de riesgo y para una mejor presentación e identificación se le añadió un color a cada riesgo.

4.9 Políticas de Seguridad Informática

Luego de haber concluido el análisis de riesgo a la organización procedimos a diseñar las políticas de seguridad informática (**Ver Anexo 27**) de acuerdo a la empresa y sus recursos para cumplir con las directrices allí expuestas.

El objetivo de esta política es la de establecer un marco para la implantación de seguridad y control que abarque a todas las áreas de la organización.

Está política cubrirá las siguientes secciones de seguridad:

- Seguridad física
- Seguridad en el Outsourcing
- Seguridad lógica
- Seguridad en redes
- Seguridad en los recursos humanos

- Planificación de seguridad informática

- Planificación de contingencia y recuperación de desastres.

4.10 Plan Estratégico de seguridad informática

El plan estratégico de seguridad informática es la culminación de este trabajo, una vez que realizamos el análisis de riesgo y a raíz de estos resultados diseñamos las políticas de seguridad informática que es la forma de mantener controlados los riesgos, procedemos a la elaboración del plan (**Ver Anexo 28**). Pero hay que dejar en claro que está parte es desarrollada por la empresa ya que solo ella sabrá en que tiempo podrá poner en práctica las políticas de seguridad antes mencionadas.

El plan cubrirá 8 objetivos:

1. Elaborar Políticas de seguridad informática.

2. Implementar seguridades físicas.

3. Mejorar la seguridad lógica.

4. Establecer seguridades en redes.

5. Fortalecer la seguridad en los Recursos Humanos.

6. Implantar medidas de seguridad en el outsourcing.

7. Implementar estrategias de continuidad.

8. Revisar el cumplimiento de las políticas de seguridad informática.

Estos objetivos serán realizados por la empresa dentro del período de un año. Cada objetivo está formada por los puntos que la empresa desea implementar, además de incluir a los cargos responsables de llevarlos a cabo, alcance y fecha de realización de cada objetivo en la organización.

CONCLUSIONES

Orientadas a las Empresas

1. Las herramientas de tecnología evolucionan con el pasar del tiempo volviéndose inseguras en la medida que su utilización no sea la más adecuada en la organización, convirtiéndose así en objeto de amenazas.

2. Hoy en día en toda empresa es una necesidad más frecuente utilizar esquemas de seguridad fuertes, que permitan una mayor confiabilidad de la información utilizada para la toma de decisiones.

3. La incomprensión de la Gerencia que conlleva a la falta de apoyo económico a la gestión de informática para implantar medidas de seguridad, provoca que la entidad tenga una exposición mayor a los riesgos.

4. La seguridad de la información es una responsabilidad compartida de todos los niveles de la organización, que requiere del apoyo de todos ellos pero debe estar dirigida por un plan y con la adecuada coordinación.

Orientadas al Tema de Tesis

5. El avance de la tecnología y del conocimiento de los seres humanos ya sean usadas con buena o mala intensión, vuelven más vulnerable a la información exponiéndola a diversas amenazas tanto internas como externas y volviéndola poco confiable.

6. La evaluación de seguridad informática realizada a la empresa AGROPEC S.A. dio a conocer a todo el recurso humano que en ella laboran los riesgos a los que está expuesta la información y que directa o indirectamente ellos colaboran para que estos aumenten.

7. La elaboración de este trabajo de tesis, contribuyo a que la empresa AGROPEC S.A. tome conciencia de cuan importante es que la información sea confiable, integra y disponible para la organización ya que vieron que si cualquiera de estas características sufriera alteraciones conllevaría a resultados nefastos para la entidad.

Orientadas a los Estudiantes

8. El fin de este trabajo es el de contribuir sirviendo como una guía para todos aquellos que deseen emprender el reto que es mantener

razonablemente segura la información y me refiero de esa manera porque no existe la seguridad total.

9. Con este trabajo se desea fomentar una cultura de seguridad en todos aquellos que lo consulten y deseen ponerlo en práctica.

RECOMENDACIONES

Orientadas a las Empresas

1. Definir políticas de seguridad clara. No solo por los riesgos derivados de los equipos de computación o de los servicios que brinda el área de sistemas, sino también por las pérdidas de productividad que puede generar un incidente de seguridad

2. Se recomienda establecer en las organizaciones la administración de seguridad informática, es decir involucrar a todos los Jefes de áreas en la administración de la seguridad con el debido apoyo total del Departamento de Sistemas

3. Fomentar la conciencia del empleado para garantizar que no haya fuga de información.

4. Realizar Auditorias a la seguridad informática de sus empresas para tener un conocimiento de sus vulnerabilidades y que procedimientos seguir para minimizar los riesgos.

5. Invertir en la capacitación del empleado en medidas de seguridad informática.

6. Proporcionar al área de sistemas en lo posible los recursos necesarios para mantener la seguridad informática en la empresa.

Orientadas al Tema de Tesis

7. Dentro del Departamento de sistemas debe existir alguien o un grupo de personas cuyas funciones sean las de administrar la seguridad informática en la empresa.

8. Se debe reubicar el Departamento de Sistemas teniendo en cuenta que el área no esté próxima a corredores de alto tráfico de personas.

9. La empresa AGROPEC S.A. deberá realizar un análisis de riesgo cada cierto tiempo. Este periodo de tiempo deberá establecerse según el impacto de riesgo en el que se encuentre la organización.

10. El personal encargado de la seguridad deberá monitorear constantemente los factores de riesgos existentes en la organización.

11. Deberán crearse Políticas de seguridad en base a los resultados del análisis de riesgo. Estas políticas serán claras para el correcto entendimiento y de conocimiento de todo el personal.

12. Implantar las políticas de seguridad recomendadas en este trabajo.

13. Diseñar un plan estratégico de seguridad siguiendo la guía que este trabajo propone.

14. La Gerencia de la empresa AGROPEC S.A. deberá sancionar al personal que viole la política de seguridad.

15. Actualizar el Plan de Seguridad de Información con cada evaluación de riesgo de la empresa.

16. Las personas que están involucradas en el plan estratégico de seguridad deben estar realmente comprometidas con la ejecución del mismo.

17. La Gerencia debe brindar apoyo completo para la implementación de este plan estratégico de seguridad informática.

Orientadas a los Estudiantes

18. Debido a que la tecnología de información avanza y con ellos incrementan los riesgos hacia la información, debemos estar en constante capacitación para tener conocimiento de que medidas emplear para afrontar esos riesgos.