NIVERSIDAD ISRAEL

FACULTAD DE SISTEMAS INFORMÁTICOS

SOLUCIONES TECNOLÓGICAS EN SEGURIDADES DE LA INFORMACIÓN PARA PROCESOS ADMINISTRATIVOS PARA DIFERENTES ORGANIZACIONES

Estudiante:

Tcnlgo. Diego Eduardo Lucero Alvarado

Tutor:

Ing. Pablo Tamayo

Cuenca - Ecuador

Diciembre 2011

UNIVERSIDAD ISRAEL
FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORIA

El documento de tesis con título **"Soluciones Tecnológicas en seguridades de la información para procesos administrativos para diferentes organizaciones"**, ha sido desarrollado por Diego Eduardo Lucero Alvarado con C.C.: No. 010470157-8 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de esta tesis sin previa autorización.

_____

Diego Eduardo Lucero Alvarado

UNIVERSIDAD ISRAEL
FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Pablo Tamayo, certifico que el señor Diego Eduardo Lucero Alvarado con C.C. No. 010470157-8, realizó la presente tesis con el título **"Soluciones Tecnológicas en seguridades de la información para procesos administrativos para diferentes organizaciones"**, y que es autor intelectual del mismo, que es original, auténtico y personal.

_____

Ing. Pablo Tamayo

UNIVERSIDAD ISRAEL
FACULTAD DE SISTEMAS INFORMATICOS

ACTA DE CESION DE DERECHOS

Yo, Diego Eduardo Lucero Alvarado, declaro conocer y aceptar la disposición de la Normativa de la Universidad Israel que en su parte pertinente textualmente dice: “Forma parte del Patrimonio de la Universidad la propiedad intelectual de las investigaciones, trabajo científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

Cuenca, diciembre 01 del 2011.

_____

CERTIFICA:

Que el presente trabajo de investigación “Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos para diferentes organizaciones”, realizado por el Sr. Diego Eduardo Lucero Alvarado, egresado de la Facultad de Sistemas Informáticos, se ajusta a los requerimientos técnico-metodológicos y legales establecidos por la Universidad Tecnológica Israel, por lo que se autoriza su presentación.

Cuenca, 01 de diciembre del 2011.

Ing. Pablo Tamayo

DIRECTOR DE TESIS

AGRADECIMIENTO

Mi más sincero agradecimiento y de todo corazón, a la Universidad Israel, que en sus catedráticos fueron quienes permitieron que pueda desarrollarme en el ámbito estudiantil, y en especial al Ing. Pablo Tamayo, persona quien estuvo siempre presente con sus conocimientos y experiencia tutelándome en el transcurso y desarrollo de este presente trabajo, que me ha brindado su amistad y se ha convertido en un digno ejemplo a seguir tanto profesional como personalmente por todos sus conocimientos adquiridos y más aún por su don de gente.

DEDICATORIA

La presente Tesis de Grado la dedico a Dios, quien me ha brindado la oportunidad para poder desarrollarme intelectual y profesionalmente en el área técnica que es de mi agrado, a mis padres y mi familia quienes me han apoyado en todo y han confiado en mí y a mi compañera de toda la vida, Doris, quien ha estado siempre a mi lado dándome fuerzas, apoyo incondicional e impulsándome cada día para poder cumplir con un objetivo más en mi vida, por este motivo este trabajo final tiene presente en cada párrafo un poquito de cada uno de ellos.

RESUMEN

El desarrollo de Soluciones Tecnológicas en seguridades de la información, para procesos administrativos para diferentes organizaciones, permite definir políticas y procedimientos de seguridad informática tanto para los equipos, aplicaciones y sistemas informáticos que posee la organización o empresa, además de proveer de reglamentos internos para el buen uso de las mismas y de los servicios que se brinda, con el fin de permitir el desenvolvimiento normal de las actividades y el buen funcionamiento de la empresa.

La administración o gerencia de la organización, debe estar cien por ciento segura de que se debe implementar estas medidas en la misma, con el fin de cumplir con los objetivos para el normal funcionamiento y brindar el servicio que los clientes externos esperan.

No olvidemos, que en un principio las personas van a estar en contra de estas políticas pero debemos asegurarnos que se deben implementar y que cuando estén realizadas se ejerzan.

Las políticas informáticas que se desarrollan en la organización, son de gran utilidad en la misma, ya que permiten utilizar los servicios y herramientas informáticas que se posee de forma adecuada con el fin de que los usuarios o funcionarios de la empresa, puedan obtener los beneficios para los cuales se adquirieron.

El buen uso de estas herramientas informáticas o de los servicios que presta la organización, deben difundirse a todas las personas involucradas con el fin de que conozcan como utilizarlos y las consecuencias que conllevan el mal uso de las mismas, las sanciones o responsabilidades que se determinan en la empresa son de carácter obligatorio y deben cumplirse de tal forma que se siente un precedente para quienes no lo hagan correctamente.

SUMMARY

The development of technological solutions in information security for administrative processes for different organizations to define security policies and procedures for both computer h

ardware, software and computer systems owned by the organization or company, in addition to providing internal regulations for the good use of them and the services being provided in order to allow the normal development of activities and the functioning of the company.

The administration or management of the organization, must be a hundred percent sure that these measures should be implemented in the same, in order to meet the objectives for the operation and provide the service they expect external customers.

Do not forget, that at first people will be against these policies but we must ensure to be implemented and that they are made are exercised.

Computer policies are developed in the organization, are useful herein, as they allow to use the services and tools that have properly so that users or employees of the company to reap the benefits for which they were acquired.

The proper use of these tools or services that the organization should be disseminated to all concerned to know how to use it and the consequences that involve the misuse of the same, penalties or liabilities are determined in the

company are mandatory and must be met so that a precedent for those who do not properly.

ÍNDICE DE CONTENIDOS

DESARROLLO

LISTA DE FIGURAS

LISTA DE TABLAS

CAPÍTULO I

1. Tema de investigación

Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos para diferentes organizaciones.

2. Planteamiento del problema

2.1 Antecedentes

La implementación de medidas de seguridad en servidores de bases de datos y de aplicaciones web, así como definir directrices para el uso de sus servicios informáticos, es un proceso Técnico-Administrativo, que debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Las prácticas informáticas administrativas permiten mantener en buen uso los equipos y sistemas informáticos de una empresa, en virtud de que la mayoría de las actividades que realizamos son hechas en base al uso de un computador y del empleo de las tecnologías de la información, así como de las redes de datos y el internet.

La Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos, se basa en la forma de usar adecuadamente los equipos informáticos, los sistemas y los diferentes recursos que la empresa provee a sus empleados, con el fin de concientizar a los miembros de la organización la

importancia de la información y los servicios que brinda la empresa y determinar responsables en el mal uso de los mismos.

Se han realizado investigaciones sobre seguridad informática, revelando que existe un aumento de actividades ilícitas por parte de personas que a través ataques cibernéticos engañan otras ya sea mediante la publicación de sitios web maliciosos, falsificaciones de empresas legítimas, campañas de spam, etc.

Es así que empresas especialistas en seguridad informática, investigan y determinan los países que alojan el mayor número de amenazas, situando a Estados Unidos, Francia, Rusia, Alemania entre otros, como los principales alojamientos de malware.

Como consecuencia de la falta o reducidas medidas de seguridad informática, tenemos actualmente las incursiones por parte de un grupo de hackers denominados “Anonymous”, en varias entidades gubernamentales de nuestro país, quienes han alterado sus páginas web, incluyendo videos en oposición al Presidente de la República.

Motivos como estos, determinan que algunas entidades públicas de otros países implementen programas estatales de políticas informáticas, como ejemplo citaremos al municipio del estado de Guanajuato, que presentó una “Política Informática” elaborado por un comité técnico, para el período de administración 2004-2006, disponiendo su vigencia desde su aprobación.

2.2 Diagnóstico o planteamiento de la problemática general

2.2.1 Causa - Efectos

Causas

- Pocas son las empresas que tienen establecido un programa de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, con lo cual se logra proteger de los diferentes tipos de ataques informáticos, reduciendo las vulnerabilidades a las seguridades que poseen.
- Los administradores de red o los responsables de los centros de cómputo, en varios casos posen conocimientos limitados sobre las diferentes formas de aplicar la Seguridad de la Información en los procesos.
- Adicionalmente a estas condiciones en muchos de los casos, existe también mala actitud por parte de los empleados de la organización, quienes no entienden que todas estas medidas de ser tomadas van en beneficio de ellos y de sus equipos informáticos, así como de su información, que es el centro de todas sus actividades.

Efectos

- La falta de un programa de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, conllevará a la empresa a presentar vulnerabilidades en diferentes formas, además de desproteger la información y de no establecer

responsabilidades a sus empleados, por la mala aplicación y mala utilización de los recursos provistos para el desarrollo de sus actividades diarias o normales.

- El desconocimiento de la aplicación de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, por parte de los responsables o administradores del centro de cómputo o la red, respectivamente, expondrá los activos de la empresa (información) a los ataques propiciados por parte de hackers o personas mal intencionadas, que deseen causar daños en algunos casos irreparables.
- Si no se cambia la mala actitud de algunos empleados de la empresa, para adaptarse a estas políticas y proteger de cierta forma la información que utilizan, así como la optimización de los recursos que presta la empresa para su funcionamiento, no servirá de nada la aplicación o puesta en marcha del programa de seguridad informática administrativa.

2.2.2 Pronóstico y control del pronóstico

Pronóstico

Se espera entregar a las organizaciones los resultados de la investigación sobre Seguridades de la Información para procesos administrativos, con el fin de proteger los activos de la misma (información), así como de determinar responsabilidades a empleados y administradores del área de sistemas.

Los resultados de esta Solución Tecnológica en Seguridades de la Información para procesos administrativos permitirá cumplir con las metas de la organización, es por este motivo que la empresa deberá invertir dinero y tiempo.

Control del pronóstico

Luego de realizada y aprobada la solución Tecnológica en Seguridades de la Información en la organización, se debe considerar evaluar la aplicación de las políticas de seguridad informática, posiblemente 2 veces al año, con el fin de verificar y ver si se dan cumplimiento éstas además de que se apliquen de la forma correcta, cabe recordar que si existen cambios administrativos puntuales que modifiquen las políticas de seguridad deberían darse a conocer las variaciones de éstas a los empleados, incluirse o modificarlas y socializarlas con los empleados .

2.3 Formulación de la problemática específica

2.3.1 Problema principal

¿El uso de las Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos, proveerá seguridad de acceso a los servidores y confidencialidad, integridad y disponibilidad de la información, así como determinar responsabilidades y aplicar sanciones por el mal de los servicios informáticos?

2.3.2 Problemas secundarios

¿La falta de seguridad en los servidores y de políticas y procedimientos informáticos afectará a las organizaciones en el acceso a su información y en los respaldos respectivos?

¿El correo electrónico institucional y el servicio de internet organizacional, es utilizado de forma correcta de acuerdo a cada rol personal?

¿Se puede determinar responsabilidades y aplicar sanciones a quienes utilicen la información y los servicios informáticos institucionales inadecuadamente?

2.4 Objetivos

2.4.1 Objetivo general

Presentar Soluciones tecnológicas mediante matrices específicas orientadas a la seguridad de la Información en servidores de bases de datos y servidores de aplicaciones web, que intervienen en los procesos administrativos para proporcionar políticas y procedimientos de respaldo en medios físicos; y, el correcto uso de los servicios informáticos institucionales con el fin de permitir su implementación en organizaciones gubernamentales.

2.4.2 Objetivos específicos

- Proporcionar matrices para la seguridad en servidores de bases de datos y de aplicaciones web y establecer políticas y procedimientos para realizar respaldos de su información medios físicos.

- Diseñar formularios para identificar los servicios informáticos que provee la organización.
- Establecer el uso correcto del correo electrónico institucional y el servicio de internet corporativo, según las actividades o roles de cada usuario a través de lineamientos o normas definidas.
- Establecer responsabilidades y sanciones a quienes utilicen la información de los sistemas y usen los servicios informáticos institucionales de forma inadecuada.
- Presentar “Políticas de seguridad para servidores de bases de datos y servidores web, para la realización de backups y el uso correcto de los servicios institucionales, que provee la organización, así como establecer responsabilidades y sanciones por su mal uso”.

2.5 Justificación

2.5.1 Teórica

Las Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, se basa en políticas y normas que se deben implementar y seguir, proporcionan las reglas que dicen cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Toda política debe de tener un propósito y procedimiento específico que especifique por qué fue creada y qué beneficios espera la organización. La responsabilidad de una política o procedimiento, define quién se hará responsable por la implementación, así como el

responsable de aplicarla de manera adecuada. Las políticas de información definen qué información es confidencial y cual es de dominio público.

Las políticas de seguridad definen los requerimientos técnicos para la seguridad en un sistema de cómputo y de redes, indica la manera en que un administrador de redes o sistema debe de configurar un sistema respecto a la seguridad que requiere la empresa.

Las políticas de uso de las computadoras extienden la ley en lo que respecta a quién puede utilizar los sistemas de cómputo y cómo pueden ser utilizados.

Las políticas de uso de Internet y correo electrónico se incluyen con frecuencia en la política más general del uso de las computadoras, sin embargo, en ocasiones se plantea en una política aparte, debido a la naturaleza específica del uso de Internet.

2.5.2 Metodológica

El desarrollo de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, se basa en la investigación, de diferentes informaciones encontradas en el amplio mundo del internet como por ejemplo “La Política de Informática” del Municipio del Estado de Guanajuato [1], así como del “Reglamento que norma el uso de herramientas informáticas y equipos de cómputo” de la Prefectura del Azuay [2], aprobado en Sesión Ordinaria del día 17 de julio del 2009, en la ciudad de Cuenca.

[1] Política Informática
[2] Reglamento que norma el uso de herramientas informáticas y equipos de cómputo.

Debemos tener presente que según la Constitución de la República del Ecuador [3] en la sección tercera, Comunicación e Información, establece:

Art. 16. - Todas las personas, en forma individual o colectiva, tienen derecho a:

> Literal 2: "El acceso universal a las tecnologías de información y comunicación."

Art. 18. - Todas las personas, en forma individual o colectiva, tienen derecho a:

> Literal 2: "Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información"

Adicionalmente deberíamos tener en claro que una política de seguridad es un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico.

2.5.3 Práctica

El desarrollo de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en organizaciones, contendrá lo referente y

[3] Constitución Política de la República del Ecuador

relativo al uso de las herramientas informáticas, seguridad de la información y al uso de políticas de seguridad en la empresa, para prevenir los posibles ataques y fugas de información “crítica”.

De aquí que la implantación de estas políticas, colaborará a mejorar el uso y el rendimiento de los equipos informáticos y de los servicios que provee la organización a los empleados y por ende a los clientes de la misma.

Permite administrar y mantener el control correcto de responsabilidades de los empleados en el uso de los equipos informáticos y sus accesos necesarios según sus funciones, como debería ser.

2.6 Marco de referencia

2.6.1 Marco teórico

Política.-

"Es el proceso orientado ideológicamente hacia la toma de decisiones para la consecución de los objetivos de un grupo." **(1)**

Política de seguridad.-

"Es el proceso orientado ideológicamente hacia la toma de decisiones para la consecución de los objetivos de un grupo, que está exento de peligro, daño o riesgo".

“Una política de seguridad es un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con

el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico.” [4]

Política de Procedimiento.-

"Es el proceso orientado ideológicamente hacia la toma de decisiones para la consecución de los objetivos de un grupo, con el fin de ejecutar algunas cosas a través de una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta"

Seguridad.-

"Es aquello que está exento de peligro, daño o riesgo". [5]

"Es aquello que está exento de peligro, daño o riesgo al ejecutar algunas cosas mediante una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta"

Procedimiento de Seguridad.-

"Es la acción de proceder o el método de ejecutar algunas cosas mediante una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta, a través de un proceso orientado ideológicamente hacia la toma de decisiones para la consecución de los objetivos de un grupo."

[4] Concepto de seguridad
[5] Concepto de Seguridad

"Es la acción de proceder o el método de ejecutar algunas cosas mediante una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta, exento de peligro, daño o riesgo"

"Es la acción de proceder o el método de ejecutar algunas cosas. Se trata de una serie común de pasos definidos, que permiten realizar un trabajo de forma correcta"

2.6.2 Marco espacial

Las Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos para organizaciones, podrá desarrollarse en empresas gubernamentales donde se requiera determinar las responsabilidades y propiciar el acceso correcto a los servidores así como el buen uso de los servicios informáticos que se posee.

2.6.3 Marco temporal

El presente tema de investigación será llevado a cabo en el transcurso de 2 meses y medio, aproximadamente, en donde se definirán todas y cada una de las acciones a realizar para poder cumplir con los objetivos propuestos.

2.7 Metodología y cronograma

Se ha realizado el análisis de documentos referentes a la seguridad informática, en donde se detallan las políticas y los procedimientos que se deben llevar a cabo para poder poner en práctica las medidas necesarias que debe poseer una organización, con el de fin de evitar fugas de información y el mal uso de los servicios informáticos que provee la empresa a los empleados.

El método utilizado es el cualitativo en base a la realidad de varias organizaciones, en donde se puede evidenciar la falta de políticas de seguridad.

Se debe conocer internamente la estructura de la organización en donde se va a desarrollar el proyecto de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos con el fin de conocer las medidas de seguridad informática si es que poseen alguna.

CRONOGRAMA DE ACTIVIDADES							
	ACTIVIDADES	DURACION					
		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 5	SEMANA 6
1	*Introducción *Proporcionar matrices para la seguridad en servidores de bases de datos y de aplicaciones web y establecer políticas y procedimientos para realizar backups de su información medios físicos.						
2	*Establecer el uso correcto del correo electrónico institucional y el servicio de internet corporativo, según las actividades o roles de cada usuario a través de lineamientos o normas definidas.						
3	*Establecer responsabilidades y sanciones a quienes utilicen la información de los sistemas y usen los servicios informáticos institucionales de forma inadecuada.						

INTRODUCCIÓN

Hoy en día las organizaciones dependen casi en un cien por ciento de sus redes informáticas y equipos informáticos, por lo tanto su seguridad es muy importante, razón por la cual un problema por pequeño que sea puede llegar a complicar la continuidad de sus actividades normales.

En ocasiones la falta de medidas de seguridad informática es un problema que crece y cada vez son más el número de ataques informáticos que buscan vulnerar las debilidades existentes en los equipos y aplicaciones, sin olvidar que en muchos casos los errores se producen en el interior de la organización por mala práctica o mal uso de los usuarios.

La estructura de la red de datos es una de las dificultades para detectar y corregir los problemas de seguridad, razón por la cual los recursos de red y sistemas informáticos han sido y son objeto de ataques por personas que poseen conocimientos avanzados en informática, conocidos o denominados como “hackers” o “crakers”.

Es por esta razón que el uso de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos en diferentes organizaciones, permitirán proveer confidencialidad, integridad y disponibilidad de la información, de sus respaldos y determinar las responsabilidades y aplicar sanciones por el mal uso de los equipos y herramientas informáticas a quienes incurran en estos tipos de delitos.

Gracias al análisis de documentos, en donde se detallan la forma y el proceso de estructuración de las políticas y procedimientos informáticos nos sirven para orientarnos de tal forma que podamos definir y en lo posterior se pueda implementar estas medidas que irán en beneficio de la organización, con el fin de salvaguardar los activos más preciados de la misma, que es la información que posee.

Con esta premisa se propone mejorar la práctica de las actividades de los administradores de la red y sus equipos servidores, del respaldo y almacenamiento de la información y de su administración; y al mismo tiempo, alertar sobre la importancia crítica de la seguridad informática.

Consideremos que un adecuado trato de este problema es de vital importancia, debido a que las amenazas son cada vez mayores, exponiendo la información generada en la organización a personas que utilizan ésta en beneficio personal o grupal, con el fin de provocar daños en la empresa y obtener dividendos monetarios en muchos casos.

Por esta razón que se debe considerar algunos temas, que permitirán mejorar la seguridad informática y minimizar las vulnerabilidades informáticas dentro la organización, entre estas tenemos:

- Definir las políticas y procedimientos de seguridad informática.
- Respaldos de información y el correcto uso de las herramientas informáticas de la organización.
- Control y seguimiento de accesos a servidores e información.

- Establecer responsabilidades y sanciones por el mal uso de los servicios informáticos que provee la organización para el uso de sus usuarios.

CAPÍTULO II

MARCO DE REFERENCIA

2.1 PROPORCIONAR MATRICES PARA LA SEGURIDAD EN SERVIDORES DE BASES DE DATOS Y SERVIDORES WEB ASÍ COMO ESTABLECER POLÍTICAS Y PROCEDIMIENTOS PARA REALIZAR BACKUPS DE SU INFORMACIÓN EN MEDIOS FÍSICOS.

2.1.1 ¿Qué es una política de seguridad informática?

Una política de seguridad informática es el lazo de comunicación entre la sección o departamento de Tecnologías de la Información y Comunicaciones (TIC), con los usuarios y el área administrativa o gerencial; es decir, es un canal entre los usuarios, los recursos y los servicios informáticos que posee la organización. Debemos recordar que una política de seguridad informática no debería ser un concepto técnico informático, ni legal, es más bien una descripción de lo que queremos proteger y el por qué de la misma, con el objetivo de persuadir a los usuarios de la forma correcta de actuar sobre los recursos, servicios y requerimientos de la organización. [6]

[6] Manual de seguridad en redes ARCET

2.1.2 Elementos que forman una política de seguridad informática.

Una política de seguridad informática o también denominada “PSI” sirve para realizar acciones o medidas en relación a la seguridad informática, por lo tanto se requiere de una decisión absoluta por parte de administración de la organización, para que cada uno de los miembros y en forma conjunta puedan realizar el levantamiento de una posible política de lo que se considera importante y necesario para los fines organizacionales.

Una PSI o política de seguridad informática debe considerar contener estos elementos:

- Conocimiento sobre los recursos, los sistemas y sobre el personal al cual se aplicará la política.
- Objetivos de la política y descripción detallada de los elementos involucrados en su definición.
- Determinación de responsabilidades para los servicios y recursos informáticos, así como para los usuarios con respecto a la información a la que tienen acceso.
- Determinación de infracciones y de las consecuencias del no cumplimiento de la política.

Toda política debe proveer explicaciones comprensibles del por qué deben llevarse a cabo y comunicar por qué son importantes para el desempeño de la organización, de esta manera las PSI (política de seguridad informática) deben

mantener un lenguaje libre de tecnicismos y términos legales que impidan su comprensión clara.

La política debe especificar quién será la persona encargada de verificar que ésta se cumpla, las medidas de corrección, acciones y sanciones que se puedan imponer, además deben seguir un proceso de actualización periódica sujeto a los cambios administrativos relevantes de la organización.

2.1.3 Parámetros para establecer políticas de seguridad informática.

Algunas características de las PSI (política de seguridad informática) y aspectos generales recomendados para su enunciación.

- Considérese en lo posterior efectuar el análisis de riesgo informático con el fin de perfeccionar las PSI (políticas de seguridad informática) de la organización.
- Involucre a las áreas que intervienen en el uso de los recursos y servicios informáticos, pues ellos tienen experiencia con lo cual podrán establecer el alcance y determinar las sanciones necesarias.
- Comunique al personal involucrado en la PSI (política de seguridad informática), los beneficios y riesgos de no ejecutar la misma.
- Desarrolle un proceso de monitoreo periódico de las directrices en la organización, con el fin de poder realizar actualizaciones oportunas a las mismas.

2.1.4 ¿Por qué las políticas de seguridad informática, generalmente no consiguen implantarse?

Muchas veces, las organizaciones realizan grandes esfuerzos para definir sus directrices de seguridad y concretarlas en documentos que orienten las acciones de las mismas. En algunos casos resulta una trabajo duro convencer a la alta gerencia la necesidad de buenas políticas y prácticas de seguridad informática.

Es así que los encargados de la seguridad deben asegurarse de que las personas entiendan los asuntos importantes de la seguridad, conozcan sus alcances y estén de acuerdo con las decisiones tomadas en relación a estos asuntos.

En consecuencia para que las PSI (política de seguridad informática) puedan funcionar en el interior de una organización deben integrarse a las estrategias del negocio, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones de la organización, sus elementos culturales y comportamientos que lleven a reconocer las pautas de seguridad necesarias y suficientes para asegurar confiabilidad en las operaciones diarias.

2.1.5 Las políticas de seguridad informática son base de la administración integral.

Las políticas de seguridad informática conforman el conjunto de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus

sistemas, constituyen un proceso continuo y retroalimentado, de los métodos de acceso a la información, el monitoreo de cumplimiento y la renovación, aceptación de las directrices y estrategia de implantación, que lleven a una formulación de directivas institucionales que logren aceptación general.

Las políticas solas no establecen una garantía para la seguridad de la organización, sino que responden a los intereses y necesidades del negocio, para administrar sus recursos y proporcionar factores que permitan proveer confiabilidad en la organización.

La seguridad tiene varios estratos:

- El marco jurídico adecuado.
- Medidas técnico-administrativas (políticas y procedimientos)

Debe existir una definición de funciones y una separación de tareas, no tiene sentido que una misma persona autorice, implante, y revise después los resultados.

2.1.6 ¿Qué es un procedimiento de seguridad informática?

Procedimiento de seguridad informática es la forma o metodología de realizar acciones definidas con el fin de llegar a cumplir un objetivo o realizar una tarea específica, que se hay determinado como una política o directriz de la organización. Este procedimiento debe estar incluido en el reglamento o manual de la empresa y debe ser llevado a cabo con todas las especificaciones brindadas.

2.1.7 Riesgos de seguridad informática

"Son la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios en la organización."[7]

Independiente de la seguridad se puede considerar que el mayor riesgo, aún teniendo un entorno seguro, es que las PSI (políticas de seguridad informática) en general no resguarden las necesidades o no estén alineadas con sus finalidades organizacionales.

Hablando de la seguridad propiamente dicha los riesgos pueden ser múltiples, lo primero es conocerlos y lo segundo tomar las decisiones respectivas.

En consecuencia las amenazas pueden llegar a afectar los datos en los programas, en los equipos, en la red y algunas veces simultáneamente entre ellos.

2.1.8 Niveles de seguridad en la información

2.1.8.1 Confidencialidad

"Consiste en proteger la información contra la lectura no autorizada explícitamente. Incluye no sólo la protección de la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial."[8]

[7] Análisis de Riesgos de Seguridad de la Información.
[8] Manual de seguridad en redes ARCET

2.1.8.2 Integridad

Es proteger la información contra la modificación sin el permiso del dueño, no solo la almacenada directamente en los sistemas informáticos sino que también se deben considerar otros tipos de modificaciones.

2.1.8.3 Autenticidad

Se refiere a garantizar que quien dice ser "X" es realmente "X". En la mayoría de organizaciones se usan nombres de usuarios y contraseñas para el acceso a la información, estos controles nos sirve principalmente para verificar que la persona que dice ser es la misma.

2.1.8.4 No repudio

“Ni el origen ni el destino en un mensaje deben poder negar la transmisión. Quien envía el mensaje puede probar que en efecto el mensaje fue enviado y viceversa.”[9]

2.1.9 Disposición de los recursos de la información

2.1.9.1 Consistencia

Se trata de asegurar que el sistema siempre funcione de la forma esperada de tal manera que los usuarios no encuentren cambios inesperados.

[9] Manual de seguridad en redes ARCET

2.1.9.2 Control de acceso a recursos.

Consiste en controlar quién utiliza el sistema o los recursos que ofrece la organización y cómo lo hace.

2.1.10 Respaldo de Información en medios físicos de almacenamiento

El responsable del área de informática conjuntamente con los propietarios de la información determinarán los requerimientos para resguardar los datos en función de su criticidad, en base a ello se definirá y documentará un diseño de resguardo de la información.

Además dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de la información. Los sistemas de resguardo deberán probarse asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades del organismo.

“Un sistema de respaldo debe contar con ciertas características como son:

- **Continuo**

  “El respaldo de datos debe ser completamente automático, continuo y transparente, sin intervenir en las tareas que se encuentra realizando el usuario”.

- **Seguro**

  En su mayoría el software de respaldo incluye cifrado de datos el cual debe ser hecho localmente en el equipo antes del envío de la información.

- **Remoto**

  Los datos deben quedar alojados en dependencias alejadas de la empresa.

- **Mantención de versiones anteriores de los datos**

  "Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos."[10]

Podemos mencionar que existe también software especializado para realizar respaldos de información tanto en equipos servidores como en clientes, estos programas permiten automatizar el proceso de backups, pero debemos tener presente que tienen un costo representativo y que depende mucho del tamaño de la organización en base al número de servidores y al número de usuarios.

Como software especializado podemos mencionar:

1. Tivoli software[11]: es un producto de IBM que permite los datos de la organización de fallos y errores, mediante una administración que permite cumplir con regulaciones y planes de recuperación de desastres.

[10] Seguridad informática
[11] Actualización de Backups, Tivoli Software http://www.redsis.com/soluciones-especializadas/automatizacion-de-backupas

Trabaja con diferentes sistemas operativos y presenta una consola de administración basada en la web.

Permite administrar y almacenar:

- Backup
- Archivado
- Bases de datos y aplicaciones
- Administración de espacios
- Retención de datos
- Planificación de recuperación de desastres

2. Data Protection Manager 2010 (DPM): Es un software para backup y recuperación de datos de aplicaciones y servidores Microsoft, a través de la utilización de discos integrados y medios de cinta.

Para el uso de cualquiera de estos softwares, debemos considerar que su costo es elevado y se requiere de un equipo de buenas características técnicas para su implementación.

2.1.11 Seguridad Lógica en servidores de bases de datos.

El principal objetivo es proteger la base de datos de ataques maliciosos ya sean internos o externos, pero no olvidemos que gran parte de los errores en cuanto a la seguridad se producen por la falta de procedimientos para asegurar su integridad.

Se debe considerar poseer un DBA (Data Base Administrator) para la administración del servidor de base de datos, pero recordemos que por más

seguridad que éste provea no hay nada que hacer ante los errores cometidos por los usuarios, sin embargo no olvidemos que generalmente el administrador se encontrará más preocupado por el correcto funcionamiento del servicio de la base de datos que por la seguridad de la misma.

Es entonces cuando el DBA encargado generalmente de establecer usuarios, crear, borrar y modificar objetos según los requerimientos deberá conceder permisos a otros usuarios sobre los objetos creados.

Consideremos que un factor de importancia en la seguridad de la base de datos es el control de la información, que suele perderse por distintos errores ya sean de hardware, software o por fallas cometidas por los usuarios por lo que se recomienda tener un respaldo de toda la información.

2.1.11.1 Intrusión desde diferentes lugares

Existen ataques externos que son detectados y controlados por el firewall, pero también existen ataques internos en donde se le permite al usuario acceder libremente a la base de datos sin ningún tipo de protección suponiendo que no actuará con malas intenciones sobre la información.

2.1.11.2 Tipos de ataques

Activos.- Causan cambios en la red o sistema que están atacando, afectan la disponibilidad, integridad y autenticidad de los datos.

Pasivos.- Tratan obtener información del sistema, afectan la confidencialidad.

- Sniffing: Escucha la información monitoreando la red.

- Man in the middle (MITM): Intercepta la autenticación y la reenvía al servidor.
- Replay Atack: Intercepta la autenticación y la utiliza en lo posterior.

Internos.- Generalmente causado por un “informante” que tiene acceso a más recursos que los esperados.

Externos.- Ataques originados fuera del perímetro de seguridad.

2.1.12 Seguridad

2.1.12.1 Identificación y autentificación

- Contraseña.
- Identificación por hardware.

2.1.13 Seguridad Lógica en servidores Web.

En la actualidad la mayoría de servidores Web poseen una gran cantidad de problemas de seguridad relacionada a su acceso a través del protocolo HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) y HTTPS HyperText Transfer Protocol Secure (Protocolo de Transferencia de HiperTexto Seguro), es decir éstas se han convertido en objetivos muy atractivos para los intrusos que desean acceder a su información confidencial, ya que estos están expuestos 24 horas, 7 días a la semana los 365 días del año. Debemos considerar algunos aspectos que se pueden afectar la seguridad en relación al protocolo HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto):

- **Seguridad en el servidor.-** Se debe garantizar que la información del servidor sea la correcta, que esté disponible y pueda ser accedida por las personas permitidas.
- **Seguridad en la red.-** Se debe garantizar que la información que es enviada desde el servidor hacia el cliente y viceversa no sean modificadas por terceras personas.
- **Seguridad en el cliente.-** Se debe garantizar que las páginas que se descargan desde el servidor, no perjudiquen la seguridad del equipo del cliente.

Sea cual sea el servidor web, se debe minimizar el número de usuarios en la máquina y número de servicios que ofrece, adicionalmente no debemos olvidar que este equipo debe ser dedicado únicamente a esta tarea.

2.1.14 Conformar el Comité de Seguridad Informático

El comité de seguridad estará formado por un grupo de personas que serán responsables de las actividades referentes a la creación y aprobación de nuevas normas de seguridad en la información de la organización.

Estas personas deberán poseer los conocimientos tanto técnicos como legales para aplicar al momento de definir las directrices en la elaboración de las políticas y procedimientos de seguridad informática.

El comité será el encargado realizar los análisis previos a los procesos y la revisión de la situación actual en la organización, con el fin de tener una idea

clara de cómo está la empresa antes de la elaboración de sus políticas de seguridad informática.

El comité deberá apoyarse en las personas que intervienen en los procesos e interpretar sus conocimientos, así como el de guiar a éstos de tal forma que se puedan crear políticas funcionales, que permitan optimizar todos los recursos de la organización.

En las reuniones se definen los criterios de seguridad adoptados en cada área y el esfuerzo común necesario para que la seguridad alcance un nivel más elevado.

2.2 ESTABLECER EL USO CORRECTO DEL CORREO ELECTRÓNICO INSTITUCIONAL Y EL SERVICIO DE INTERNET CORPORATIVO, SEGÚN LAS ACTIVIDADES O ROLES DE CADA USUARIO A TRAVÉS DE LINEAMIENTOS O NORMAS DEFINIDAS.

2.2.1 ¿Qué es el correo electrónico?

El correo electrónico o denominado e-mail es una forma o medio para comunicarse con amigos, familia, compañeros de trabajo, etc; por lo que se ha convertido en uno de los servicios más utilizados que provee el internet.

Existen innumerables ventajas del uso del correo electrónico, entre estas tenemos: es inmediato (se recibe al poco tiempo de haber sido enviado), fácil de enviar (desde cualquier lugar), económico y dinámico ya que permite recibirlo aún no estando en el lugar donde se usa habitualmente.

2.2.2 ¿Qué es una cuenta de correo electrónico?

Una cuenta de correo electrónico es como nuestra dirección física para recibir el correo convencional; es decir, es como si tuviéramos un buzón de correo tradicional. Para comprender mejor podemos analizar una dirección de correo, por ejemplo prueba_de_email@yahoo.com.

Las direcciones de correo electrónicos están formados por dos partes separadas por el símbolo @ “arroba”, la primera indica nuestro nombre “nombre de usuario”, para el ejemplo superior (prueba_de_email) y la segunda parte es el dominio “yahoo.com”, que indica cuál es el servidor de correo al cual pertenece mi cuenta.

Un usuario puede tener varias cuentas y destinar cada una a un asunto particular, de igual forma varios usuarios puede compartir un mismo computador para acceder a distintas cuentas de correo.

La diferencia entre el correo tradicional y el correo electrónico está en el primero en conocer obligatoriamente la dirección física del remitente mientras que en el segundo hay que conocer la dirección de correo electrónico.

2.2.3 Tipos de cuentas de correo electrónico

Hay dos tipos de cuentas de correo electrónico: el correo web y el correo POP. El correo Web, no necesita configuración especial, se puede acceder desde cualquier computador, es menos propenso a los virus ya que se almacena en un servidor y sólo cuando descarguemos algún archivo adjunto estaremos vulnerables al ataque de algún virus.

El correo POP, no necesita estar conectado para redactar los mensajes, es más rápido y se descarga desde el servidor a nuestro computador, es decir aún después de estar desconectados del internet podemos leerlo, es de mayor facilidad de infección de virus.

El correo web es personal o gratuito ya sea este hotmail, yahoo, gmail, entre otros, y lo puede poseer cualquier persona, su ventaja es que puede consultarse desde cualquier computador.

El correo POP, se puede acceder mediante una aplicación denominada cliente de correo, en Windows la aplicación más conocida es Outlook y desde Microsoft Office el denominado Microsoft Outlook, que es la más común que utilizamos en las organizaciones en donde laboramos.

El correo institucional depende de nuestra organización; es decir, si la organización a la cual pertenecemos económicamente puede adquirir un dominio, entonces nosotros podremos tener cuenta de correo corporativa. La misma servirá para procesos empresariales y permitirá identificar el nombre de nuestra organización, en la mayoría de casos aquí utilizamos el denominado Microsoft Office Outlook, en donde se configura la cuenta de correo corporativa.

2.2.4 Protocolos que intervienen en una aplicación de correo electrónico

- **Protocolo SMTP**

  SMTP (Simple Mail Transfer Protocol), es el protocolo de entrega de mensajes entre servidores y envío entre usuario y servidor.

- **Protocolo POP**

POP (Post Office Protocol), Protocolo de Oficina de Correos, el servidor POP almacena el correo electrónico en buzones hasta que el programa del cliente lo recupere, una vez allí el cliente revisa sus mensajes, los descarga, los borra, los puede enviar, etc.

2.2.5 Seguridad del correo electrónico

El responsable del área Tecnologías de la Información y Comunicaciones definirá y documentará normas y procedimientos claros con respecto al uso del correo electrónico institucional y su seguridad, que incluyan algunos de los siguientes aspectos:

a) Protección contra ataques y virus.

   Virus.- Es un programa o código ejecutable, tiene la habilidad de reproducirse, los virus informáticos tienen la facilidad de diseminarse rápidamente y muchas veces son difíciles de erradicar.

b) Protección de archivos adjuntos al correo electrónico. En virtud de que en el correo electrónico se puede enviar cualquier tipo de archivo adjunto, el administrador deberá contar con el software antivirus adecuado y actualizado para el cliente, el mismo que analizará el adjunto antes de permitir abrirlo.

c) Aspectos operativos (tamaño máximo para envío y recepción, cantidad de destinatarios, tamaño máximo de almacenamiento para el buzón del usuario, etc.). Esta configuración estará definida por el administrador del correo en el servidor en donde se detallan todas estas características.

d) Potestad para auditar los mensajes de los servidores de la organización. El administrador estará en la capacidad de poder auditar o revisar los mensajes de datos siempre y cuando exista una solicitud del tipo legal, manteniendo siempre como primordial la confidencialidad de los mismos.

2.2.6 Uso administrativo del correo electrónico

Entender que el correo electrónico es una herramienta más de trabajo que debe ser utilizado conforme su uso destinado, y que autoriza al nivel gerencial a implementar sistemas o normas de control para la protección y el buen uso de sus recursos.

Sin embargo, no deberá interferir en la dignidad y derecho a la intimidad del empleado, por lo que la organización deberá informar a sus empleados el uso que se espera hagan del correo electrónico; y, bajo qué condiciones los mensajes pueden ser objeto de control.

2.2.7 Riesgos de Seguridad en el correo electrónico

Se implementarán controles para reducir los riesgos de seguridad en el correo electrónico, considerando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados.
b) La posible intercepción y acceso a los mensajes en los medios que intervienen en la distribución de los mismos.

c) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la red.
d) Aspectos legales como prueba de origen, envío, entrega y recepción.
e) El uso inadecuado del personal de la organización.

2.2.8 Uso del servicio de internet

El acceso al servicio de internet será utilizado con el propósito para el cual fue provisto por el responsable del área Tecnologías de la Información y Comunicaciones quien definirá los procedimientos necesarios para solicitar y aprobar los accesos al mismo.

Los accesos serán autorizados por el responsable del área Tecnologías de la Información y Comunicaciones, así mismo se definirán las directrices de utilización para los usuarios.

Se valorará la utilidad de poseer un registro de accesos por usuarios, con el objeto verificar los accesos efectuados para futuros análisis, este control será comunicado a los usuarios de acuerdo a lo establecido. Para ello, el responsable del área Tecnologías de la Información y Comunicaciones analizará las medidas a ser implementadas para efectivizar este control, como son la instalación de “firewalls” (cortafuegos) software o hardware que permite o niega los accesos a los equipos de una red a través de los puertos TCP, “proxies” (equipo servidor que permite el acceso a internet desde el interior de mi red de área local LAN), etc.

Debemos recordar que en la actualidad existe software para administrar el servicio de internet, y para contralar el ancho de banda, pero este es de un costo elevado, por lo que si la organización está dispuesta a realizar el gasto debería considerar al mismo para una mejor administración.

Bandwidth Splitter (controlador de ancho de banda), es un programa para *Forefront TMG* que permite limitar el ancho de banda por usuario y por hosts, así como por grupos. Admite configurar cuotas máximas en megas para el tráfico de internet, por periodos y monitorear las conexiones por usuario, además de generar reportes detallados de uso, ya sea por regla, por IP o por cliente, etc.

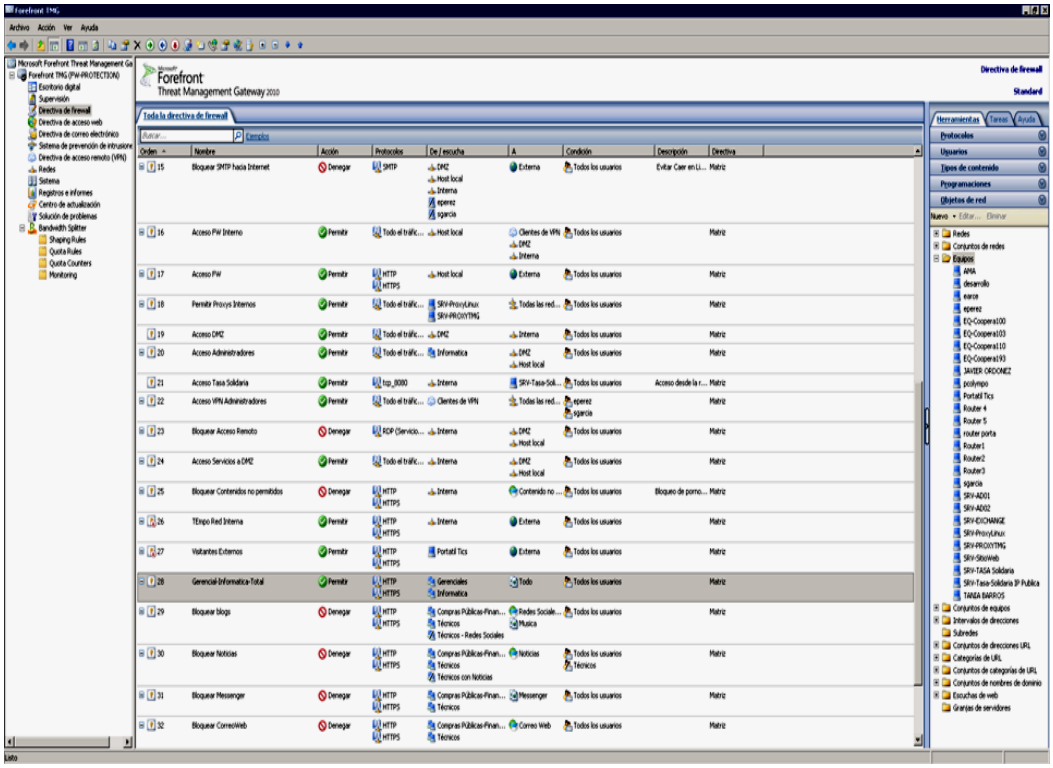

Gráfico # 1

2.3 ESTABLECER RESPONSABILIDADES Y SANCIONES A QUIENES UTILICEN LA INFORMACIÓN DE LOS SISTEMAS Y USEN LOS SERVICIOS INFORMÁTICOS INSTITUCIONALES DE FORMA INADECUADA.

2.3.1 Delito informático

El delito informático o denominado crimen electrónico, es el término general para las operaciones ilícitas realizadas a través del internet que tienen como objetivo destruir o dañar computadores, medios electrónicos y redes. Sin embargo, las categorías de un delito informático son complejas y pueden incluir delitos tradicionales como: fraude, robo, chantaje, falsificación y la malversación de fondos públicos utilizando redes y equipos informáticos.

Existen actividades ilícitas que se realizan de forma electrónica y van ligadas a infringir o dañar partes del ámbito informático como ingreso e interceptado ilegal a sistemas y redes, daños en la información (borrado, dañado, alteración, etc), robo de bancos, ataques de hackers, violación de derechos de autor y de información confidencial.

El delito informático puede ser dividido en dos grupos:

1. Crímenes con el objetivo de causar daños a las redes de datos, por ejemplo: gusanos, archivos maliciosos, spam, ataques masivos a servidores y generación de virus.

2. Crímenes a través de computadores y del internet, por ejemplo, espionaje, fraude, robo, etc.

Citemos a una persona quien roba información de sitios webs o causa daños a redes y servidores, estas actividades pueden ser virtuales, pero el daño aunque es real no tiene consecuencias físicas. Un computador puede ser la evidencia y aunque no haya sido directamente utilizado para cometer el crimen, es un excelente aparato que guarda los registros, esta propiedad ha provocado que los datos codificados del computador tengan un valor de evidencia en el campo legal.

En varios países existe policía especializada en la investigación de estos tipos de delitos informáticos que al ser cometidos a través del internet, su esclarecimiento se ve dificultado ya que dependiendo de cada país las leyes no son aplicadas o simplemente no existen.

2.3.2 Fraude

El fraude informático es inducir a otra persona a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

1. Afectar el ingreso de datos de forma ilegal, esto significa que el criminal conoce y posee un alto nivel de técnica, generalmente es común en empleados de la empresa que conocen las redes de información y pueden ingresar a ella para alterar los datos así como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.

2. Alterar, destruir y robar datos, este es un evento que puede ser difícil de detectar en las redes de la organización si no se poseen medidas de seguridad.

3. Utilizar de forma inadecuada los sistemas y alterar o reescribir códigos con propósitos fraudulentos, aquí se requieren de un alto nivel de conocimiento.

Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

2.3.3 Hostigamiento

El hostigamiento o acoso se dirige de manera específica a un individuo o grupo de individuos con comentarios de rogativos a causa de su género, raza, religión, nacionalidad, orientación sexual, etc, ocurre generalmente en canales de conversación, grupos o con el envío de correos electrónicos destinados en exclusiva a ofender. Todo comentario que sea derogatorio u ofensivo es considerado como hostigamiento o acoso.

2.3.4 Terrorismo virtual

Desde años atrás el terrorismo virtual se ha convertido en uno de los novedosos delitos criminales informáticos los cuales deciden atacar masivamente el sistema de servidores de una empresa, organización, centro de estudios, oficinas oficiales, etc. La difusión de noticias falsas en internet (por ejemplo decir que va a explotar una bomba en un edificio estatal), es

considerado terrorismo informático y es procesable dependiendo las leyes de cada país.

2.3.5 Sujetos activos y pasivos

Muchas de las personas que cometen delitos informáticos poseen ciertas condiciones específicas como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", esta categoría requiere que:

- El sujeto activo del delito sea una persona de cierto estatus socioeconómico;
- Su comisión no pueda explicarse por falta de medios económicos, poca educación, poca inteligencia, ni por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos puede ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información generalmente conectados a otros equipos o sistemas externos.

2.3.6 Determinación de responsabilidades de usuario y sanciones

2.3.6.1 Responsabilidades

Responsabilidad, es la acción de realizar algo y medir sus consecuencias si no se efectúa correctamente, además se debe estar consciente de las causas directas o indirectas que se provocan sobre una persona u organización el no actuar con la responsabilidad debida, que puede afectar a una norma jurídica o moral en la sociedad.

2.3.6.2 Sanciones

Sanción es la consecuencia de una conducta que constituye una infracción a una ley o reglamento, dependiendo la ley que ha sido vulnerada será la sanción.

- Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la sección de Tecnologías de la Información y Comunicaciones.
- Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta.
- Corresponderá al responsable del área de Tecnologías de la Información y Comunicaciones hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones informáticas de la institución.
- Todas las acciones en las que se comprometa la seguridad de la red y que no estén previstas en las políticas de seguridad informática, deberán

ser revisadas por la sección de Tecnologías de la Información y Comunicaciones para dictar una resolución sujetándose al estado de derecho.

CAPÍTULO III

METODOLOGÍA

3.1 Políticas y procedimientos de seguridad informáticas.

Debemos considerar que una política de seguridad informática o denominada "PSI", debe estar ligada de manera directa entre los funcionarios, la administración o gerencia de la organización, los recursos y los servicios informáticos que se provee en la empresa.

Debe estar detallada de la forma más sencilla y simple para su comprensión, ya que no todas las personas de la organización están en la capacidad de entender términos técnicos o legales, es decir debería estar compuesta por lenguaje común.

Toda política de seguridad informática contempla algunos elementos para su desarrollo, sin embargo esta no podría realizar su función si no existe la decisión firme por parte del área administrativa o gerencial.

Para definir la política de seguridad informática, se debe conocer realmente cómo funcionan los recursos y los servicios informáticos que posee la organización, además de identificar el objetivo de la política, determinar

responsables del uso de los recursos y determinar sanciones a la no aplicación de la PSI.

Además debemos definir un responsable de verificar que se cumpla la política de seguridad informática, que se den las medidas y se apliquen las sanciones de ser necesarias, también la PSI debe permitir que se pueda modificar o adaptar según los cambios conforme las diferentes variaciones de la organización.

En la creación de una PSI debemos involucrar a las áreas y personas que están inmersas en el uso de los servicios o recursos informáticos, que intervienen en esta política; también se debe comunicar los beneficios que obtendrá la organización al aplicar la misma.

Para que las políticas de seguridad informáticas sirvan a la organización deberían estar ligadas con los objetivos de la empresa, así como el de crear una conciencia de uso y aplicación de las mismas.

Estas políticas deben estar compuestas por un marco jurídico y por las medidas administrativas que permitan actualizar y renovar las mismas considerando el proceso de retroalimentación en la organización.

La política de seguridad informática está ligada directamente a un procedimiento de seguridad que permitirá definir y establecer la forma y metodología para poder utilizar la misma.

Metodología:

1. Debe existir un compromiso por parte de la alta gerencia o administración de la organización, sabiendo que las políticas y procedimientos de seguridad informática están directamente ligadas con los objetivos de la organización. Sin este compromiso cualquier medida que se intente tomar no tendrá los resultados esperados. El administrador o gerente debe estar consciente que la seguridad informática es tan primordial como cualquier otro servicio para la organización.

   Debe realizarse una carta compromiso, en el que se defina la aceptación para la elaboración de las políticas y procedimientos para la seguridad informática en el que se establezca la aplicabilidad en la organización.
2. Se debe conformar el comité o equipo de seguridad informática, integrado por personal que tengan los conocimientos tanto técnicos como legales en el área administrativa y de informática y que sepan o conozcan de los procesos y los servicios informáticos que presta la organización a sus empleados. Además se debería designar una persona que se haga responsable de hacer cumplir las medidas y aplicar las sanciones necesarias que den en favor de la seguridad informática en la organización.
3. Elaboración o definición de procesos para la seguridad informática en los servidores de bases de datos y servidores web de la organización, sobre los respaldos de información de éstos en medios

físicos de almacenamiento, para su futura utilización, no olvidemos que los mismos que servirán para su análisis posterior en donde se definan las matrices que permitirán realizar un reglamento de políticas y procedimientos informáticos para la seguridad en la administración.

4. Análisis de la situación actual de la seguridad en los servidores de bases de datos y servidores web de la organización, así como de los métodos o formas de respaldos de su información si es existen, todo esto permitirá realizar un estudio posterior que permitirá el desarrollo de los procesos que irán en beneficio de la organización.

   Cuando se han definido ya los procesos de seguridad informática en los servidores de bases de datos y servidores web, y sus respaldos de información respectivos, se debe considerar el análisis de la situación actual de la organización, en base a lo que se requiere establecer como política de seguridad informática.

ANÁLISIS DE LA SITUACIÓN ACTUAL CON RESPECTO A LA SEGURIDAD DE SERVIDORES Y POLÍTICAS INFORMÁTICAS, RESPALDOS Y SERVICIOS INFORMÁTICOS EN LA ORGANIZACIÓN

	CUESTIONARIO	SI	NO	NO SABE
1.-	**EQUIPOS**			
	Existen servidores de bases de datos y servidores web en su organización?			

	Existe un servidor de correo electrónico en la organización?			
	Existe un equipo servidor para el servicio de internet en su organización?			
	Existen firewall en su organización?			
2.-	**ADMINISTRACION**			
	Existe un comité de seguridad informática en la empresa?			
	Existen políticas de seguridad informática para los servidores de bases de datos y para sus respaldos de información en su organización?			
	Conoce Ud.,si su información está protegida al acceso de terceras personas sin su autorización?			
	Conoce Ud.,si su información no es alterada o modificada y es realmente íntegra?			
	Existen políticas para administrar sus contraseñas o claves?			
	Existen políticas para el uso del correo electrónico institucional?			
	Existen políticas para confidencialidad en su información en la organización?			
	Existen políticas para el uso del internet corporativo?			
	Existen políticas para formar grupos y proveer el servicio de internet en la organización?			
	Conoce Ud.,si existen sanciones por el mal uso de el correo electrónico y el servicio de internet, dentro de la organización?			

3.-	RESPALDOS			
	Con qué frecuencia se realizan los respaldos de información de los servidores de bases de datos y servidores web en su organización?			
	Sabe que tipo de respaldo se realiza en los servidores de bases de datos y servidores web en su organización? Completa……. Diferencial…….			
	Si existen respaldos de las bases de datos, conoce Ud. Si exiten formas o medios para etiquetar, comprobar y restauar los mismos?			
	Existen registros donde se definen los respaldos a las bases de datos?			
	Los respaldos en medios físicos de almacenamiento, se resguardan en algún lugar externo a la organización?			
	Se realizan copias de seguridad de sus servidores, tanto en S.O., como en aplicaciones?			
4.-	**SEGURIDAD**			
	Existen autenticación de usuarios en los servidores y aplicaciones?			
	Existen técnicas de cifrado de datos?			
	Hay personas responsables, para auditar las bases de datos?			
	Se realizan actualizaciones de los S.O de los servidores?			

5.-	SERVICIOS INSTITUCIONALES			
	Su organización provee de servicio de correo electrónico institucional?			
	Usted posee correo electrónico institucional para envíos externos?			
	Su organización provee de servicio internet corporativo?			
	Usted necesita servicio de internet para realizar su trabajo en la organización?			
6.-	SOFTWARE			
	Existe software para realizar copias de seguridad de bases de datos en la organización?			
	Existe software para monitorear y administrar el servicio de internet en la organización?			
	Existe software para controlar el ancho de banda de internet en la organización?			
	Existe software antivirus en la organización?			

Tabla # 1

5. Planificación y elaboración de las políticas de seguridad en los servidores de bases de datos y servidores web de la organización, así como las políticas de respaldos de información de los mismos en medios físicos de almacenamiento.

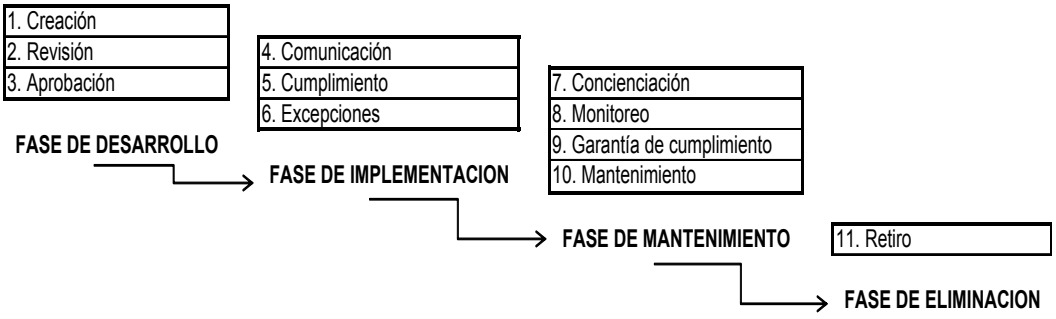

Gráfico #2

6. Revisión y aprobación de las políticas y procedimientos de seguridad informática en la organización.
7. Socialización de las políticas y procedimientos de seguridad informática en la organización a los usuarios y funcionarios que utilizan los equipos y servicios que presta la empresa u organización.
8. Aplicación de las políticas y procedimientos de seguridad informática, para los servidores de bases de datos y servidores web, así como para sus respectivos respaldos, además del uso del correo electrónico e internet.

Conclusión

La definición de políticas y procedimientos de seguridad informática en la organización dependen de muchos factores y están relacionadas directamente con los recursos y servicios informáticos que provee o disponen las mismas, con las áreas organizacionales, con los funcionarios involucrados en el uso de éstos, y desarrollada con una definición que no sea técnicamente estructurada de la política conjuntamente con un marco legal que pueda ser interpretado por

las personas comunes de la organización, además debe establecer responsabilidades y sanciones a quienes no cumplan con ésta, y deben dar a conocer los beneficios para los cuales se crearon, mismos que deberán contemplar y estar estrechamente ligados con los objetivos de la organización.

Para la elaboración de las políticas de seguridad informática se debería conformar un grupo de personas o denominado Comité Técnico, mismo que deberá poseer la capacidad y conocimientos tanto técnicos como legales, así como en el uso de los recursos informáticos, de esta manera se podrán definir de una forma clara y comprensiva las políticas paras las personas a quienes se van a aplicar las mismas, logrando de esta manera hacer conciencia en los usuarios para el uso y aplicación de las mismas.

3.2 Riesgos de seguridad informática

Es la estimación a que suceda una amenaza o se materialice, lo que se trata es de generar un entorno seguro y libre de riesgos, con respecto a la seguridad informática, con el fin de que se protejan la información, programas, equipos de red, etc.

Metodología:

1. Identificar las amenazas
2. Identificar el riesgo
3. Determinar políticas y especificar medidas adecuadas para eliminar riesgos y amenazas de seguridad informática

Conclusión

Los riesgos de seguridad informática, siempre estarán presentes en toda organización, sin embargo debemos tratar de minimizar que éstos ocurran y determinar medidas de seguridad en beneficio de la misma, para precautelar la información y los equipos.

3.3 Niveles de seguridad y disponibilidad de los recursos.

Toda política y procedimiento de seguridad informática debe considerar que la información que posee la organización es de gran importancia para la misma; es decir, es considerada un activo y que tiene que asegurarse su protección al acceso no autorizado, mantenerse de forma íntegra y sin modificación sin la autorización del propietario de la misma, debe permitir verificar la autenticidad de quien accede a los equipos así como a la información y permitir que se pueda probar el origen y destino de quien envía o recibe la información, además de mantenerse a la disposición de cualquier persona cuando sea requerida administrativamente o en algunas ocasiones requerida en el campo legal por diferentes motivos.

También debe mantener consistencia, es decir que no tengan cambios inesperados, sin el previo consentimiento del propietario o administrador de los sistemas; así como, controlar quien utiliza los recursos informáticos y la función o aplicación que se le da en base a las necesidades o requerimientos de cada uno de los usuarios o funcionarios de la organización.

Metodología:

1. Proteger la lectura, escritura y acceso a la información mediante la prohibición de recursos compartidos que sean innecesarios tanto en los servidores de bases de datos como en los servidores web, logrando de esta manera proteger la información de personas no autorizadas o ajenas a su acceso, mismas que podrían causar diferentes tipos de daños o malas interpretaciones que pueden perjudicar a la organización, funcionarios o niveles jerárquicos superiores en cualquier fase de su vida.
2. Comprobar que los sistemas o aplicaciones no permitan modificar la información que existe en ellas, sin la debida autorización del propietario de la misma o sin el consentimiento del administrador del sistema y sin el respaldo de la alta gerencia, que prioritariamente debería mantener la información de forma segura, tanto en su beneficio como en el de sus empleados o funcionarios.
3. Comprobar que los sistemas de la organización realicen una correcta verificación y validación de usuario y contraseña, misma que servirá antes de mostrar la información solicitada, logrando de esta manera asegurarse que quien solicita la información es quien dice ser, no olvidemos que habrán personas que quieran realizar actividades ilícitas accediendo a la información privada de ciertos usuarios, con el objetivo de perjudicar a la organización o a la persona propietaria de la información.

4. Solicitar que cada uno de los accesos que generen cambios o no a las bases de datos y al servidor web se almacenen en un archivo en donde se pueda verificar los mismos, en el momento que se requiera y cuando se lo necesite. Este archivo debería estar respaldado en algún lugar físico de los servidores y en lo posible en medios externos con el fin de poder realizar una auditoría de ser necesaria.

Conclusión

Se debe considerar que la información de los sistemas de la organización y sus bases de datos deben estar protegidas de cambios o modificaciones y accesos no permitidos, a personas internas o externas a la misma, para lograr cumplir con este objetivo deberíamos proveer a los usuarios contraseñas y sistemas verificados que provean la certeza de que lo que hacen con su información es personal y sólo podrán acceder a la misma quienes ellos autoricen y quienes tengan los permisos para verla o modificarla de acuerdo a sus privilegios según sus perfiles en la organización. Estos perfiles deberán definirse manteniendo un criterio según la criticidad de la información y según el volumen de la misma, así como quien decida el autor o propietario brindarle los permisos necesarios para su acceso o lectura.

3.4 Respaldo de información en medios físicos de almacenamiento.

Se deberá establecer una persona responsable de realizar los respaldos de información de la organización, esta persona debe ser quien tenga acceso a los servidores y sistemas y que pueda realizar dichos respaldos o copias de seguridad. En la actualidad existen diferentes formas para realizar los

respaldos de información, mismos que se deben utilizar en base a las características de la organización; es decir, dependerán mucho de los equipos y sistemas que se posee la misma, en base a estos antecedentes se debe considerar las formas o métodos de respaldo.

Metodología:

1. Definir las bases de datos que se deben respaldar en base a su criticidad para la organización; es decir, dependerán mucho de los objetivos que persigue en la empresa y de cuales son más importantes para el desarrollo normal de las actividades, en función de las áreas que forman a la misma.
2. Establecer un esquema de etiquetación de los respaldos de información, para poder identificarlos de forma sencilla a cada uno de ellos y utilizarlos correctamente cuando sea necesario o sea requerido por alguna situación.
3. Establecer una técnica de reemplazo para los medios de almacenamiento considerando la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor y de acuerdo a su estructura física, además de asegurarse que su destrucción sea correcta en aquellos que poseen daños por alguna situación o hayan terminado su vida útil, según sea el caso.
4. Llevar un registro detallado de los respaldos la información y de su forma de recuperación, que permitirá a cualquier persona que conozca y sepa de informática y pertenezca a la Coordinación de

Tecnologías de la Información y Comunicaciones y tenga la autorización necesaria poder realizar una restauración de la base de datos.

5. Guardar en una ubicación interna y externa a la organización las copias de información, en diferentes medios de almacenamiento conjuntamente con los registros necesarios para su recuperación, en los cuales se detallaran el tipo de respaldo y la forma de utilizarlos.
6. Comprobar periódicamente que los medios de respaldo estén en buenas condiciones y que los backups, puedan ser utilizados sin ningún problema al momento de subir las bases de datos.
7. Verificar las formas de restauración para garantizar la recuperación de los respaldos, de esta manera se podremos normalizar las operaciones y el desenvolvimiento de la organización será el esperado en el caso de ser necesario.
8. Además de los respaldos de las bases de datos se podría realizar de la misma manera las copias de seguridad de todo el servidor (sistema operativo y aplicaciones), que podemos utilizar en cualquier momento cuando ocurra un problema de software a nivel de S.O.
9. Si existe la disponibilidad económica por parte de la organización se podría adquirir un software especializado para la obtención de backups de información, mismo que permite automatizar esta tarea o actividad.

Conclusión

Los respaldos de información en la organización, son de mucha importancia en la misma, ya que de éstos depende su operatividad y normalización de las actividades para brindar servicio a los usuarios o clientes tanto internos como externos, en el caso de sufrir daños en sus bases de datos o servidores web por diferentes situaciones o circunstancias.

Se debe tener en cuenta que existen diferentes formas de respaldos y que se deben guardar los mismos en medios físicos tanto interna como externamente a la organización, así como llevar registros de cada uno de ellos y conocer el tiempo de vida útil de los medios físicos para poder utilizarlos de manera adecuada, también debemos tenerlos al alcance de ser necesario y cuando se los requiera conocer la forma de restauración con el fin de no perjudicar o interferir en las actividades normales de la organización.

3.5 Seguridad lógica en servidores de Base de Datos

La seguridad en los servidores de bases de datos en la actualidad se considera muy útil, en virtud de que a la par de la información lo que se debe proteger es al equipo servidor de los ataques tanto internos como externos, recordemos que la mayoría de daños o problemas que ocurren con frecuencia sobre los servidores de bases de datos son realizados indirectamente por los usuarios de la organización, que realizan actividades o tareas en algunos casos sin conocer que es lo que hacen, este problema se da en virtud de que el administrador de la base de datos no les provee de los permisos o accesos necesarios en base a un análisis y creación de un perfil de usuario, es decir pueden modificar,

borrar o eliminar datos y piensan que los equipos son inteligentes y deben corregir los errores que ellos cometen.

Además no debemos olvidar que también pueden ocurrir daños sobre los servidores de bases de datos originados por problemas de hardware o software, problemas comunes en algunas ocasiones en nuestro medio.

Metodología:

1. Analizar e identificar los tipos de cuentas y perfiles de usuarios (operadores y administrador), esta información permitirá brindar los accesos requeridos a las personas indicadas y con los conocimientos necesarios para el desarrollo normal de las funciones en la organización.
2. Autorizar a los usuarios el acceso a la información necesaria para el desarrollo de su trabajo normal y diario en la organización, con el fin de que cada persona sea responsable de sus acciones y que éstas no interfieran en las actividades comunes que realizan en la organización.
3. Utilizar técnicas de cifrado para la protección de datos, con el fin de que sea difícil encontrar los valores reales que puedan servir a personas ajenas a la organización, con el fin de causar daño en la misma.
4. Determinar una persona responsable para realizar el control de auditorías de accesos a la base de datos, cuando sea necesario y lo requiera la organización administrativamente o legalmente.

5. Realizar actualizaciones del S.O. y parches correspondientes.
6. Definición de contraseñas seguras para acceso al servidor de bases de datos, con el fin de que sea difícil para una persona ajena a la organización detectar las contraseñas y causar daños en el mismo o en su información.
7. Mantener una copia de las contraseñas almacenadas en una bóveda o caja fuerte.

3.5.1 Normas para proteger las contraseñas o claves.

La protección de la contraseña es de responsabilidad tanto del administrador como del usuario, en virtud de que el sistema está al alcance de cualquier persona que introduzca una contraseña insegura.

Deberíamos proponer al usuario que el cambio de contraseña sea lo más frecuente posible y no la divulguemos a terceras personas, ya que de esta forma precautelamos la información y los sistemas.

1. No permitir cuentas sin contraseña.
2. No compartir las contraseñas con otras personas.
3. No escribir las contraseñas en lugares de acceso para otras personas.
4. No enviar contraseñas por e-mail.
5. Cambiar la contraseña periódicamente.
6. La contraseña debería ser alfanumérica y poseer caracteres especiales (mínimo 6 caracteres).

Conclusión

La seguridad lógica servidores de bases de datos, es primordial en virtud de que la información es un activo que no tiene precio, y debemos precautelarla de todas las maneras posibles, ya sea mediante permisos definidos por grupos o categorías, cifrado de información, contraseñas seguras y actualizaciones de S.O., todas estas características permitirán al administrador del departamento de Tecnologías de la Información y Comunicaciones estar preparado y seguro de que quienes acceden al servidor lo hacen de la forma correcta y según lo requerido para el desenvolvimiento normal de sus tareas o funciones.

3.6 Seguridad lógica en servidores web

La seguridad de la información de los servidores web en una organización, es de mayor responsabilidad ya que éstos están expuestos a los ataques de intrusos principalmente desde fuera de la organización. Consideremos que nuestro servidor está con las puertas abiertas al exterior a través de los protocolos HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) y HTTPS HyperText Transfer Protocol Secure (Protocolo de Transferencia de HiperTexto Seguro), mismos que permiten el envío y recepción de información para el servidor y el cliente. Estos puertos son generalmente usados en estos tipos de servidores y deben ser configurados correctamente ya que pueden dejar expuestos no solo al servidor, a la base de datos, o a la aplicación sino también a nuestra red en la organización y por ende a nuestros equipos clientes con la información que posee cada uno de ellos.

Recordemos que la información de nuestra organización es de suma importancia no solo a nivel empresarial sino que también va a existir información personal que será de gran valor para quien la recopiló o generó, así como para la empresa, que es en donde se desarrolló.

Metodología:

1. Activar la opción de firewall de nuestro sistema operativo.
2. Verificar la integridad de S.O y sus aplicaciones.
3. Deshabilitar servicios y cuentas de usuario que no sean utilizadas para brindar el servicio para el cual fue destinado el servidor.
4. Instalar y mantener actualizado el antivirus necesario o pertinente para una protección mayor del equipo.
5. Utilizar contraseñas seguras para el acceso al servidor y sus aplicaciones web.
6. Encriptar la información del usuario y su contraseña.
7. Publicar la información estrictamente necesaria para la aplicación y de ser necesario el envío y recepción de datos, hacerlo de la manera más segura a través de web services probados.

Conclusión

La seguridad lógica en servidores web, hoy en día con todos los avances tecnológicos, es uno de los puntos claves dentro de una organización para permitir el desenvolvimiento normal de sus actividades y asegurar la confidencialidad, integridad y disponibilidad en la información.

Recordemos que toda información que sea publicada o enviada en un servidor web, debe ser controlada y asegurada que es la correcta y que no fue alterada en el proceso de envío y recepción, además consideremos que si permitimos el acceso a través de un servidor web a nuestra red, podemos ocasionar problemas aún más graves en los equipos clientes y en la información de los mismos.

Para concluir, mencionemos algunas recomendaciones que pueden servir para concientizar a los usuarios sobre la seguridad informática en la organización:

- Realizar y desarrollar ejemplos relacionados con fallas de seguridad con todos los usuarios de la organización, con el fin de concientizar sobre el uso correcto de medidas de seguridad para precautelar nuestros activos que son muy preciados.
- Mencionar que las fallas de seguridad en los equipos provocan daño no solo a nuestros objetivos organizacionales sino que también a la información personal, con lo cual interfieren en el normal desenvolvimiento de las actividades diarias, tanto personales como institucionales y que perjudican a la imagen de la empresa para los clientes internos como externos.
- Consolidar las políticas de seguridad informática con el proceso de toma de decisiones de la gerencia o administración y los principios de integridad, confidencialidad y disponibilidad de la información, con el objetivo de brindar a las personas dependientes de la misma la seguridad de que su información está resguardada y que podemos

disponer de ella cuando sea necesario o cuando lo requiera cualquier otra persona.

- Demostrar la importancia de la seguridad informática en la organización, no solo para su propio beneficio sino también para beneficio personal, en virtud de que estaremos seguros de nuestra información no está siendo modificada o alterada y que podernos recurrir a ella en cualquier momento y cualquier situación.

3.7 Correo electrónico institucional, cuentas, tipos, seguridad y riesgos

Correo electrónico o conocido como e-mail, es una forma para comunicarse con las personas que necesitamos, ya sea por situaciones de trabajo o personales, su información es enviada de forma inmediata y el destinatario puede utilizarla rápidamente.

Para utilizar el correo electrónico debemos poseer una cuenta de correo, la misma que equivale a nuestra dirección física para enviar o recibir una carta de la forma tradicional.

La cuenta de correo electrónica está formada de tres partes, la una, de un nombre, la segunda del signo arroba "@" y la tercera del dominio (nombre de la empresa). Una persona puede tener varias cuentas de correo electrónicas y acceder a ellas de diferentes formas, en cualquier momento y cualquier lugar.

Menciones 2 tipos de cuentas de correo electrónico, la personal o gratuita y la institucional o empresarial, la segunda debería ser utilizada netamente para fines laborales, ya que nuestra organización ha hecho un esfuerzo muy grande

para poder prestarnos este servicio que permite estar en contacto con otras personas que tienen relación directa con la empresa.

La persona responsable de la Coordinación de Tecnologías de la Información y Comunicaciones, deberá estar en la capacidad o contar con una persona responsable de conocer y proveer de seguridades contra ataques en el correo electrónico institucional, con el fin de evitar pérdidas o desvíos de información que en muchos de los casos son de vital importancia para la empresa, ya que al estar expuestos estas informaciones permiten que cualquier persona puede apoderarse de la misma para beneficio propio o de la competencia.

Metodología:

1. Se debe adquirir un dominio organizacional, con la correspondiente dirección IP pública que permitirá proveer de este servicio a los usuarios que así lo requieran.
2. Mantener un servidor principal Exchange Server, para poder crear cuentas de correo electrónico.
3. Se debe estandarizar los nombres de las cuentas de correo, es decir al crear todos los nombres de las cuentas deberían tener una misma estructura misma que dependerá de nuestro criterio.
4. Se deben crear grupos de usuarios que determinen características para el uso del correo electrónico, es decir, quienes podrán enviar y recibir correos, quienes podrán solo recibir correo, etc.
5. Se debe crear políticas para definir el número máximo de destinatarios a los cuales enviar, el límite de almacenamiento, el

tamaño máximo de datos adjuntos para envío y recepción y el lugar de almacenamiento de los correos (servidor o cliente).

6. Establecer políticas que el uso del correo electrónico institucional es exclusivo para labores de trabajo y que cualquier otra forma de utilización tendrá consecuencias o sanciones.
7. Establecer que el uso del correo electrónico implica aspectos legales dentro de la organización y fuera de la misma.

Conclusión

El correo electrónico institucional permite a los funcionarios realizar el trabajo para el cual fueron contratados, sin importar que el usuario lo utilice en ocasiones de forma personal, pero deberíamos concientizarlo a que el uso inadecuado puede conllevar a tener problemas legales tanto dentro de la organización como fuera de la misma.

Debe explicarse que el uso del correo electrónico, implica gastos para la organización, razón por la cual el área administrativa podrá solicitar que se haga un seguimiento del correcto uso del mismo, para definir funcionarios o usuarios que lo utilicen de forma inadecuada pudiendo perjudicar de alguna forma a la institución, ya que nuestra cuenta de correo irá con el aval o nombre de dominio de la empresa a la cual pertenecemos.

Es por este motivo que debemos tener mayor cuidado con los mensajes que sean enviados desde una cuenta de correo institucional, ya que no solo se juega nuestro nombre personal sino también el de nuestra organización y

como sabemos es muy fácil detectar desde donde fue enviado un correo que puede estar inmerso en algún problema de tipo legal.

Recordemos que en nuestra legislación existe la “Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de datos”, que aplica sanciones por el mal uso de este medio de comunicación.

3.8 Uso del servicio de Internet

El uso del servicio de internet que provee la organización, está directamente ligado con los objetivos que persigue la empresa, es decir se utiliza para poder brindar el servicio que requiera el cliente externo, además está ligado con los requerimientos o necesidades del usuario para realizar su trabajo en la misma, es decir cada uno tendrá diferentes niveles de acceso al servicio de internet dependiendo de sus tareas o actividades y funciones dentro de la empresa.

Se deberá realizar una categorización por grupos para proveer de este servicio a todos quienes lo requieran y justifiquen su uso, todo esto se dará con el respectivo aval de su jefe inmediato o superior, quien confirme que su necesidad es indispensable para ejercer sus tareas o funciones inherentes a su cargo.

No olvidemos que hay que hacer consciencia a todos y cada uno de los funcionarios, que el dinero que cancela la empresa por este servicio debe plasmarse en inversión para la misma, ya que debemos mantener una imagen hacia los clientes externos y brindar el servicio que ellos solicitan de la forma más solvente.

Metodología:

1. Análisis del ancho de banda que requiere la organización para brindar el servicio a sus empleados o funcionarios.
2. Contratación del servicio de Internet.
3. Instalar con un equipo para proxy, que permita filtrar el contenido y la creación de grupos para los respectivos permisos a las páginas necesarias, dependiendo de las labores o funciones que realicen.
4. Si la organización cuenta con los fondos económicos suficientes debería adquirir un software para segmentar el ancho de banda, de esta forma estaría optimizando los recursos y dando prioridad a quienes lo necesiten y a quienes realmente lo usen.
5. Categorizar a los usuarios según sus requerimientos de internet, esto dependerá de los niveles jerárquicos dentro de la organización y los vistos buenos o aprobaciones del jefe inmediato para con el peticionario del servicio.
6. Establecer horarios de uso del servicio de internet en la organización, según las categorías o grupos que se determinen, dependiendo de la jornada normal de trabajo los días y horas definidos.

Conclusión

El uso del servicio de internet debe aportar al desarrollo de la organización de tal forma que no sea un gasto sino una inversión, para esto debemos hacer consciencia en los usuarios en que no se debe hacer un mal uso del mismo, ya

que son bienes puestos a nuestra disposición para realizar el trabajo para el cual fuimos contratados.

Sin embargo este servicio puede ser utilizado en asuntos personales, pero manteniendo un nivel aceptable de uso para esto, es decir en la mayoría del tiempo de uso del servicio debería ser para labores de trabajo.

Con el equipo proxy deberíamos estar en la capacidad de poder generar reportes de uso, cuando sea necesario y cuando lo requiera cualquier persona de la alta gerencia, por lo que deberíamos indicar a los usuarios que sus accesos están disponibles para ser auditados en el momento requerido, por lo que son ellos los únicos responsables de su uso correcto o no.

Para poder obtener este servicio la empresa debe contar con equipos para su distribución de tal forma que los gastos son altos, por este motivo deberíamos obtener el mayor provecho del mismo pero en beneficio institucional y no personal como en algunos casos.

3.9 Responsabilidad y sanciones del mal uso de sistemas y servicios informáticos

3.9.1 Delito Informático, fraude, hostigamiento, terrorismo virtual y sujetos activos y pasivos

El delito informático provoca varias operaciones ilícitas a través del internet y correo electrónico que pueden perjudicar tanto al usuario que lo realiza como a la organización a donde pertenece el mismo, es decir debemos estar consientes de que los servicios que presta la empresa donde laboramos son

exclusivamente para fines laborales e institucionales, sin embargo muchas veces hacemos un mal uso de los mismos sin medir las consecuencias que esto puedo atraer.

Hay diferentes formas de realizar daño a una empresa o persona, mediante el acceso no autorizado a su información o el daño de sus redes de computadoras, sin embargo en algunos casos estos daños son imperceptibles en un principio pero no olvidemos que tarde o temprano podemos ser descubiertos y llevados ante la ley.

Algunas formas de causar daño a la información de la organización es al ingresar datos de forma ilegal, alterar, destruir o robar los mismos, o utilizarlos de manera inadecuada o robar información clasificada, además de enviar contenidos ilegales u ofensivos, temas políticos, violencia, crimen, entre otros.

También al momento de dirigirnos a personas o grupos de personas específicamente, mediante comentarios negativos, estamos incurriendo en un delito, no olvidemos que el internet es una herramienta que entrega fácilmente todo tipo de información, buena y mala, y que permite en varios casos dependiendo de la persona que lo usa realizar ataques masivos a servidores cuando quien lo hace sabe o tiene conocimientos avanzados en informática.}

Una noticia falsa es también considerada como un delito, ya que puede alterar a la sociedad, es por este motivo que existen leyes que regulan el uso de estas herramientas como el internet y el correo electrónico.

Muchas son las formas de causar daño a la información de una organización y la información personal de los funcionarios de la misma, pero no debemos olvidar que existen métodos para identificar estas alteraciones.

No olvidemos que existen varias personas que tienen interés en realizar o cometer delitos informáticos, algunos son personas que lo hacen por el simple hecho de demostrar sus habilidades informáticas y otras lo hacen por el simple hecho de obtener beneficios personales o institucionales.

En ambos casos existen leyes que prohíben este tipo de actividades, sin embargo algunas personas lo hacen sin importar su repercusión, ya sea individual o colectivamente.

Metodología:

1. Conocer los diferentes tipos de delitos informáticos y sus consecuencias, con el fin de poder aplicar normas que regulen su buen uso dentro y fuera de la organización.
2. Interpretar la “Ley de Comercio Electrónico, Firmas Electrónicas y mensajes de datos” de la República del Ecuador en su parte concerniente a los mensajes de datos, para poder aplicar las responsabilidades y sanciones pertinentes.

Conclusión

Muchas son las formas de realizar daño a la información y a las personas que utilizan los servicios informáticos en la actualidad que posee en una organización, es decir podemos desde alterar una información hasta provocar

un caos social dependiendo mucho de la connotación de nuestra noticia o de la forma de hacer aparecer un comentario ofensivo hacia alguien o alguna empresa, es decir las formas de provocar alteraciones en los sistemas o en la información son diversas, es por este motivo que existen leyes que regulan el uso de estos servicios.

Dentro de la organización debemos desarrollar normas que se puedan aplicar en el uso de los servicios informáticos que posee la misma, como son el correo electrónico y el internet, así como la información que desprenden los sistemas que se encuentran en esta.

3.9.2 Responsabilidades y Sanciones

Dentro de la organización, todos y cada uno de los funcionarios debemos cumplir con las leyes o normas que están definidas para poder llevar a cabo nuestro trabajo con normalidad y responsabilidad, sin embargo en algunos casos no consideramos importante el cumplir y hacer cumplir estas normas, por tal motivo somos objeto de sanciones que no solo perjudican nuestra imagen sino que también al resto de personas, por la acción cometida.

Pueden ser sanciones pequeñas, como llamados de atención y otras de mayor peso como informes que manchen nuestras hojas de vida en la institución, es decir está en nuestras manos el optar por la decisión correcta a la hora de cumplir las leyes establecidas.

Metodología:

1. Administrativamente conocer sobre los recursos que provee la organización y sus procesos, de tal forma que podamos definir claramente las responsabilidades y sanciones.
2. Identificar los procesos para la elaboración de las responsabilidades y sanciones, por el mal uso de los recursos.
3. Conocer términos legales y traducir términos técnicos a lenguaje común, que pueda ser interpretado por cualquier persona.

Conclusión

La determinación de responsabilidades y sanciones en la organización, depende mucho de las personas que conformen el comité técnico para la elaboración de las políticas y procedimientos, es decir, ellos serán los encargados de aplicar las leyes que para su criterio sean las más idóneas y aplicar las sanciones correspondientes a cada caso.

Antes de establecer sanciones deberán asegurarse que éstas sean las más convenientes para los fines organizacionales, es decir no podrán ser sanciones que perjudiquen a la empresa.

Las sanciones dependerán mucho de la falta en la cual se incurra, y estarán definidas claramente y sin dar lugar a ambigüedades, ya que si no ocurre así cada persona interpretará la ley según su criterio o pensamiento y dependerá si queremos aplicar la ley a favor de unos u otros.

CAPÍTULO IV

DESARROLLO

4.1 Políticas y procedimientos de seguridad informática.

Para poner en práctica la elaboración de políticas y procedimientos de seguridad informática debemos considerar tener un documento escrito que permita ser un sustento legal para la elaboración de políticas y procedimientos de seguridad administrativa, mismo que deberá contener la autorización de la alta gerencia o administración de la organización.

El modelo para realizar la solicitud para autorizar el realizar las políticas y procedimientos informáticos en la organización, deberá estar elaborado de tal forma que involucre a la gerencia o administración de la organización el que se pueda implementar según las necesidades de la misma y deberá, estar indicado de tal forma que cuando se implemente no exista ningún impedimento que no permita su aplicación.

Las políticas y procedimientos de seguridad informática, definidas correctamente permitirán a la organización obtener los mayores beneficios de tal forma que al momento de su implementación, tanto para los usuarios que deberán aceptarlas como quienes deberán hacerlas aplicar sean de fácil entendimiento y de clara precisión.

Modelo para solicitar la autorización, a la administración de la organización para realizar las políticas y procedimientos de seguridad informáticas.

FORMATO DE LA SOLICITUD PARA AUTORIZAR EL REALIZAR LAS POLITICAS Y PROCEDIMIENTOS INFORMÁTICOS EN LA ORGANIZACIÓN

Fecha:…….

Señor

Nombre ……..

Responsable de la Coordinación de Tecnologías de la Información y Comunicaciones

Su despacho,

De mi consideración:

Por medio del presente solicito a Usted, se digne realizar el Reglamento de Políticas y Procedimientos de Seguridad Informática en la Organización, para los servidores de bases datos y servidores web así como sus respectivos respaldos, en medios físicos.

Debo indicar que cuando se realice este reglamento, el área administrativa estará comprometida para aplicarlo de la manera que sea necesaria, con el objetivo de proteger la integridad de la información y cumplir con los objetivos organizacionales.

Sin otro particular, suscribimos.

Atentamente,

…….

Responsable del Área Administrativa.

4.2 Conformación del Comité de Seguridad Informática

El Comité de Seguridad Informática, debería estar conformado por un delegado de la Coordinación de Tecnologías de la Información y Comunicaciones, un delegado o responsable del área administrativa, y un responsable del área legal, además de una persona que conozca sobre los procesos informáticos en la organización.

Se debería instalar este comité, con las personas antes mencionadas y si existe alguna otra más, depende de la visión que tenga el responsable de la Coordinación de Tecnologías de la Información y Comunicaciones.

Aquí, deberían realizar un acta en la cual firmen todos los responsables antes mencionados y que comuniquen que su conformación está dirigida a realizar el Reglamento de Políticas y Procedimientos de Seguridad Informática en la Organización, así como de hacer cumplir las medidas y aplicar las sanciones correspondientes según sea el caso.

4.3 Definición de procesos

- Proceso de Backup de Bases de Datos **PROC-BK-BD-001.**
- Proceso de Seguridad Lógica en Servidores de Bases de Datos **PROC-SEG-LOG-BD-001.**
- Proceso de Seguridad Lógica en Servidores Web **PROC-SEG-LOG-WEB-001.**
- Proceso para Administración del Correo Electrónico **PROC-EMAIL-001.**
- Proceso para el uso y contratación del servicio de internet **PROC-INTERNET-001.**

****

4.3.1 Proceso de Backup de Bases de Datos

PROC-BK-BD-001

Seguridad en el servidor de Bases de Datos

1. Defina qué base(s) de datos es(son) primordial(es) para el desarrollo normal de las actividades de su empresa u organización?

Posibles Bases de Datos existentes **Señale con "X"**

a. Base de datos del sistema contable

……

b. Base de datos de gestión documental

……

c. Base de datos de aplicaciones

……

d. Base de datos de la página web

……

2. Escoja según su criterio que tipo de respaldo de la base de datos va a realizar.

Posibles tipos de backup **Señale con "X"**

a. Completa

……

b. Diferencial

……

3. Frecuencia sugerida para realizar los respaldos de las bases de datos?
   a. Diaria-Cuatro medios (Lunes a Jueves) reutilizables.
   b. Semanal-Cuatro medios (cada viernes corresponde a semana 1 hasta semana 4) reutilizables.
   c. Mensual-Doce medios (cada cuarta semana se respalda el mes)

Día	Semana			
Lunes	X	X	X	x
Martes	X	X	X	x
Miércoles	X	X	X	x
Jueves	X	X	X	x
Viernes	Semana #1	Semana #2	Semana #3	Semana #4

Tabla # 2

4. Esquema de etiquetación o codificación de los respaldos de las bases de datos.

Codificación o etiquetación de los medios

Diaria: LUNES-MARTES-MIERCOLES-JUEVES.

Semanal: SEMANA #1- SEMANA #2- SEMANA #3- SEMANA #4.

Mensual: ENE-FEB-MAR-ABR-MAY-JUN-JUL-AGO-SEP-OCT-NOV-DIC.

5. Registro de Respaldos de las bases de datos:

REGISTRO SEMANAL Y MENSUAL DE RESPALDOS DE BASES DE DATOS				
Fecha	**Base de Datos**	**Tipo de respaldo**	**Codificación**	**Firma de Responsabilidad**
28/oct/2011	Sistema Contable	Completa	SEMANA #4	
31/oct/2011	Sistema Contable	Completa	OCT	

Tabla # 3

6. Definir en qué lugar se van a almacenar los respaldos de las bases de datos y los registros.
    a. Oficina de Tecnologías de la Información y Comunicaciones (caja fuerte)
    b. Oficina perteneciente a la organización que se encuentre en un lugar diferente a la matriz.
7. Realizar una comprobación mensual aleatoriamente de cualquier medio de respaldo, para verificar su buen estado.
8. Realizar una copia de seguridad de todo el servidor (S.O y aplicaciones) mensual y llevar un registro con los detalles de la misma.

****

4.3.2 Proceso de Seguridad Lógica en Servidores de Bases de Datos

PROC-SEG-LOG-BD-001

1. Conformar grupos de usuarios para la Base de Datos, sólo un usuario administrador que será el DBA, y el resto de usuarios se considerarán operadores.
2. Autorizar a los usuarios los permisos necesarios para acceder a la base de datos según sus requerimientos.
3. Utilizar técnicas de cifrado en la información, o al menos en las contraseñas de los usuarios.
4. Determinar una persona responsable para realizar el control de auditorías en la base de datos, esto se podría desarrollar a través del mismo SQL Server.

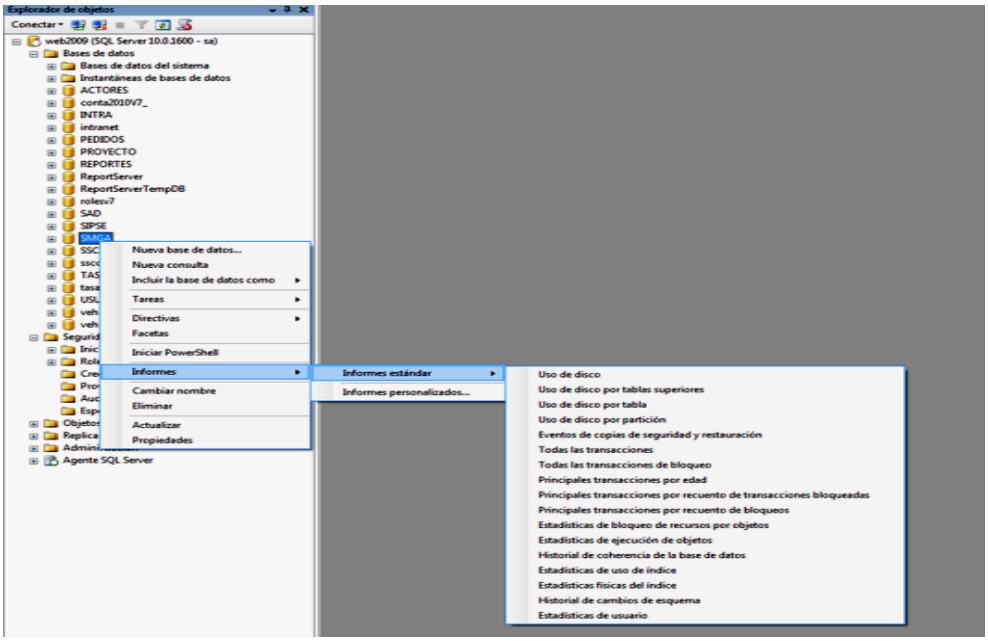

Gráfico # 3

5. Actualizar el Sistema Operativo y parches correspondientes al SQL Server, de ser necesario.
6. Definir contraseñas seguras, que debería estar compuestas por mínimo 6 caracteres alfanuméricos y con caracteres especiales.
    a. No permitir cuentas sin contraseñas
    b. No compartir las contraseñas
    c. No escribir las contraseñas en lugares de acceso público
    d. No enviar contraseñas por email
    e. Solicitar al usuario realizar cambios de contraseñas frecuentemente

****

4.3.3 Proceso de Seguridad Lógica en Servidores Web

PROC-SEG-LOG-WEB-001

1. Activar el firewall del S.O.
2. Verificar que el S.O., esté instalado correctamente, activado, que existan las cuentas de usuario del S.O que sean para necesarias y obviamente la del administrador.
3. Verificar que los puertos HTTP HyperText Transfer Protocol (Protocolo de Transferencia de HiperTexto) (www), puerto 80/TCP y el puerto HTTPS/SSL usado para la transferencia segura de páginas web, puerto 443/TCP.

   Verificar que esté levantado el IIS (Internet Information Services).

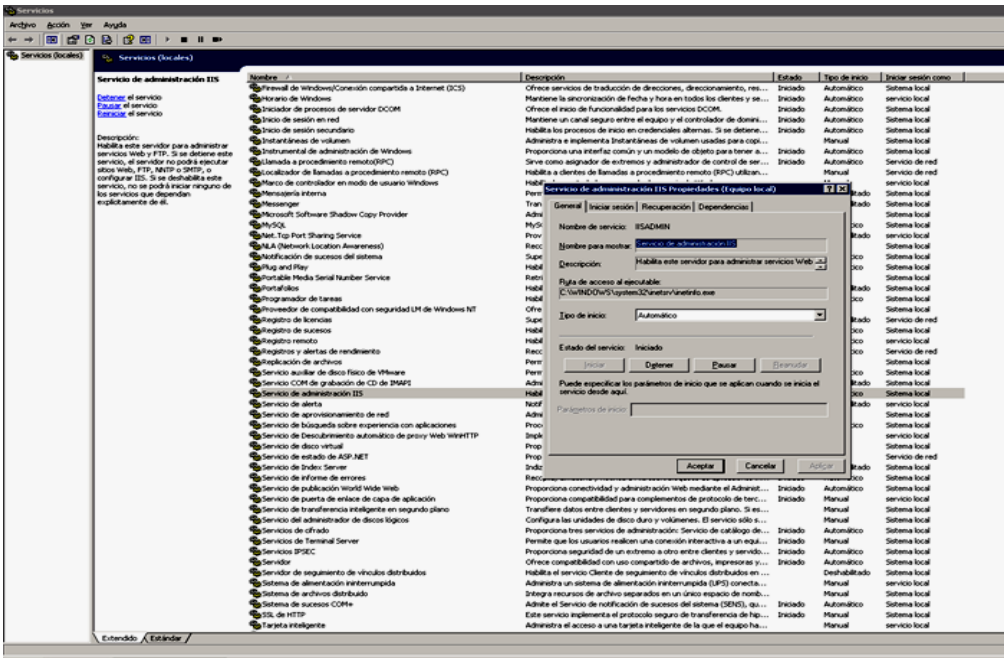

Gráfico # 4

4. Verificar que esté instalado el antivirus con la versión necesaria para servidor y que esté actualizado correctamente.

Gráfico # 5

5. Utilizar contraseñas seguras para acceder al servidor y a sus aplicaciones web.
    a. No permitir cuentas sin contraseñas
    b. No compartir las contraseñas
    c. No escribir las contraseñas en lugares de acceso público
    d. No enviar contraseñas por email
    e. Solicitar al usuario realizar cambios de contraseñas frecuentemente
6. Encriptar la información.
7. Publicar la información estrictamente necesaria.

****

4.3.4 Proceso para Administración del Correo Electrónico

PROC-EMAIL-001.

1. Adquirir un dominio para la empresa u organización, dominio "prueba.com".
2. Mantener un servidor con Exchange Server.
3. Mantener una estandarización de los nombres de las cuentas de correo electrónico.
    - Estructurar el nombre de cuenta por:
        - Inicial del primer nombre + apellido completo del usuario. (Juan Francisco Pérez Alvarez, "jperez")
        - Si ya existe una cuenta de usuario con el mismo nombre, se puede cambiar por la segunda inicial del nombre, así: (Juan Carlos Pérez Ríos, "cperez")
        - Y luego añadir el signo arroba "@" conjuntamente con el dominio de la organización, quedando así: jperez@prueba.com ó cperez@prueba.com
4. Establecer grupos para envíos de correo externo, es decir no todos los usuarios podrán realizar envíos de correo electrónico a cuentas externas.
5. Crear políticas para definir límites en las cuentas de correo.
    a. Límite máximo de envío, sugerido 5120 Kb ó 5 MB
    b. Límite máximo de recepción, 5120 Kb ó 5 MB

c. Límite de destinatarios, sin límite o máximo de destinatarios

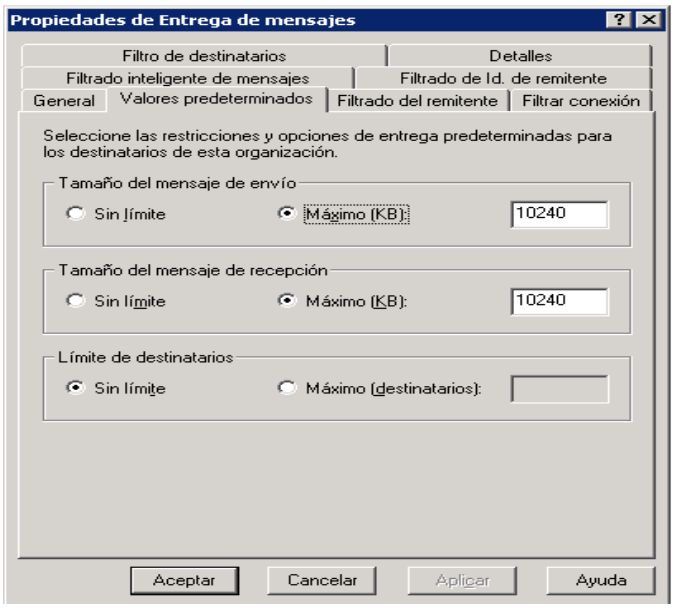

Gráfico # 6

d. Lugar de almacenamiento del archivo mdbdata, en el servidor.

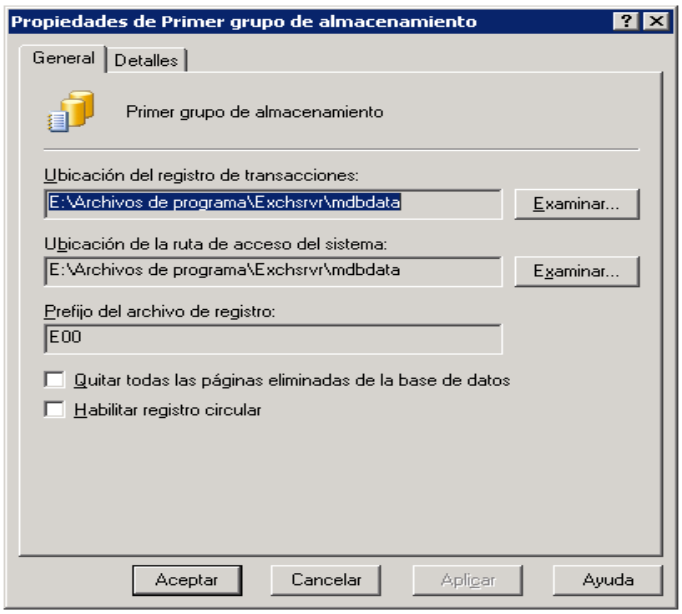

Gráfico # 7

****

4.3.5 Proceso para el uso y contratación del servicio de internet

PROC-INTERNET-001.

1. Análisis del ancho de banda necesario para cubrir los requerimientos de los funcionarios o usuarios de este servicio, con el fin de proveer el mismo con todos los beneficios necesarios para realizar las funciones que cada cargo amerite.
2. Análisis de la mejor propuesta del servicio de internet, para esto debemos solicitar a varios proveedores del servicio, las proformas que sean necesarias y realizar el estudio de cada una de ellas, con el fin de determinar la que mejor brinde los servicios requeridos y el valor a pagar sea conveniente para los intereses de la empresa, también debemos solicitar que nos entreguen información de sus clientes para poder solicitar referencias del proveedor, y poder analizar cada uno de los resultados entregados, además cuando esto se ha realizado entonces deberemos realizar la contratación del servicio, asesorándonos de la mejor forma legal para que cuando lo necesitemos podamos hacerlo sin perjudicar los intereses de la organización.
3. Debemos realizar un análisis que permita realizar la categorización de los usuarios del servicio, según sus actividades y realizar los grupos de accesos a las páginas necesarias de acuerdo a sus funciones.

4. Debemos instalar o contratar la instalación y el asesoramiento para la implementación de un equipo proxy, con el fin de conceder permisos a los usuarios del servicio según sus necesidades laborales.
5. Si existe la disponibilidad económica, deberíamos adquirir un software que permita la segmentación del ancho de banda del servicio de internet, con el fin de aprovechar de la mejor manera los recursos de la organización.
6. Establecer políticas con los horarios de uso del servicio de internet, según las categorías y grupos de páginas, que dependerán de la jornada normal de trabajo.

4.4 Análisis de la situación actual

Luego de haber realizado el levantamiento de información del análisis de la situación actual, podremos decidir cuan necesario sería para la organización poseer un reglamento de políticas y procedimientos informáticos que sirva para precautelar la información de la organización, así como los servicios informáticos que posee en beneficio de los usuarios y de sus clientes.

El análisis de la situación actual, conjuntamente con los procedimientos definidos anteriormente permitirá tener una visión más amplia de las necesidades y los recursos que posee la empresa, de esta forma al momento de conformar las políticas de seguridad será relativamente sencillo ya que vamos a tener el suficiente conocimiento como para poder interpretar cómo se van a desarrollar con respecto a las responsabilidades y sanciones.

No debemos olvidar que el desarrollo de las políticas y procedimientos de seguridad informática, deben ser realizadas de la manera más sencilla y fácil de comprensión para los usuarios de los servicios, es decir no deben contener términos técnicos y legales que sean difíciles de interpretar.

Para la realización del reglamento de políticas y procedimientos informáticos de seguridad, debería estar ya conformado el comité de seguridad por las personas designadas de las diferentes áreas, que se debieron establecer con anterioridad, sin embargo la elaboración del reglamento dependerá mucho de los alcances que se le quiera dar al mismo.

4.5 Planificación y elaboración de las políticas de seguridad informática

La planificación y elaboración de las políticas serán logradas a partir de los resultados que arrojen el análisis de la situación actual, con todos los valores a favor, en contra y con los que se desconocen que se hacen. Se debe considerar las 4 fases de desarrollo de una política, que son: Fase de Desarrollo, Fase de Implementación, Fase de Mantenimiento y Fase de Eliminación.

La elaboración de las políticas dependerá mucho de los resultados obtenidos en el *ANALISIS DE LA SITUACION ACTUAL CON RESPECTO A LA SEGURIDAD DE SERVIDORES Y POLÍTICAS INFORMÁTICAS, RESPALDOS Y SERVICIOS INFORMÁTICOS EN LA ORGANIZACIÓN,* en donde deberemos considerar los siguientes aspectos:

- Si en el resultado del análisis de la situación actual, en lo pertinente a los equipos, obtenemos las respuestas correspondientes a **"SI"** en un 75%, debemos considerar lo siguiente:

Título I

USO Y CUIDADO DE LOS EQUIPOS SERVIDORES DE LA ORGANIZACIÓN

Capítulo 1: USO Y CUIDADO DE LOS EQUIPOS SERVIDORES

Art. 1.- Normas de uso y cuidado de los equipos servidores.- Entiéndase que los equipos servidores de la organización, son de costos elevados razón por la cual deben mantenerse en buen estado técnico, para lo cual se considera:

a) Los equipos servidores serán utilizados en labores inherentes a las funciones para las cuales adquiridas.

b) Deben ser instalados programas originales con sus respectivas licencias y configurados de la forma más idónea para realizar su trabajo determinado.

c) Deben estar protegidos en un área donde se encuentre prohibido el ingreso de personas ajenas a la Coordinación de Tecnologías de la Información y Comunicaciones.

d) Debe existir el cuidado necesario de los servidores, tanto en mantenimiento preventivo y correctivo.

e) Se debe llevar un control de los mantenimientos realizados durante la vida útil de los equipos.

- Si en el resultado del análisis de la situación actual, en lo pertinente a la administración, respaldos y seguridad, obtenemos las respuestas correspondientes a **"NO"** en un 75%, debemos considerar lo siguiente:

Título II

POLÍTICAS DE SEGURIDAD PARA SERVIDORES Y PARA REALIZACIÓN DE BACKUPS

Capítulo 2: POLÍTICAS DE SEGURIDAD DE LOS SERVIDORES DE BASES DE DATOS Y SERVIDORES WEB, PARA LA INFORMACIÓN Y PARA LA REALIZACIÓN DE BACKUPS

Art. 2.- Políticas de Seguridad para la información y para los servidores de bases de datos y servidores web.- Entiéndase como políticas todas aquellas reglas o lineamientos que debemos seguir con el fin de obtener el mayor de los beneficios para la organización, es así que hay que considerar lo siguiente:

a) Toda información que se encuentre en los servidores de bases de datos y servidores web, debe poseer confidencialidad, integridad y consistencia.

b) Se deben crear perfiles de usuarios para proporcionarles sus permisos respectivos.

c) Se debe utilizar técnicas de cifrado de datos, para precautelar la información.

d) Se debe solicitar que las contraseñas sean mínimo de 6 caracteres alfanuméricos y con un carácter especial.

e) La contraseña será de uso personal y su divulgación será responsabilidad de su propietario.

f) Deberá exigirse que la contraseña del administrador se cambie frecuentemente, o al menos una vez cada trimestre.

g) Los servidores deben estar protegidos por un firewall.

Art. 3.- Políticas de respaldos de la información.

a) Respaldar las bases de datos críticas para el desarrollo normal de las actividades de la organización.

b) Realizar un esquema de etiquetación de los respaldos.

c) Registrar los respaldos de información y su forma de recuperación.

d) Guardar los respaldos de información en ubicaciones dentro y fuera de la organización.

e) Comprobar el buen estado de los medios físicos para los respaldos.

f) Verificar que los respaldos se puedan restaurar adecuadamente.

g) Realizar copias de seguridad de todo el servidor (S.O. y aplicaciones).

h) Proporcionar la infraestructura necesaria para poder realizar estos procesos en la elaboración de respaldos y copias de seguridad de los equipos servidores.

i) Designar una persona responsable para la realización de estas tareas de respaldo de bases de datos y de información.

Título III

USO CORRECTO DE LOS SERVICIOS INSTITUCIONALES, QUE PROVEE LA ORGANIZACIÓN.

Capítulo 3: CORREO ELECTRÓNICO INSTITUCIONAL

Art. 4.- Correo electrónico institucional, cuentas de usuario, contraseña y seguridad.-

a) Todos los usuarios van a poseer una cuenta de correo electrónica institucional.

b) Solo usuarios autorizados podrán utilizar la cuenta de correo electrónica para envíos externos.

c) Se estandarizará los nombres de las cuentas de correo electrónico.

d) Se definirá los límites para envío de archivos adjuntos a 5 MB, y si es necesario se habilitará mayor tamaño en los casos de ser necesarios.

e) El usuario es responsable de mantener la confidencialidad de su contraseña y será responsable de las actividades relacionadas a la misma.

Art. 5.- Uso y privacidad del correo electrónico institucional.-

a) El uso del correo electrónico institucional es de uso obligatorio, es decir se presumirá que toda información enviada por este medio es conocida.

b) La Coordinación de Tecnologías de la Información y Comunicaciones, respetará la privacidad de los usuarios, salvo que se requiera esta información para asuntos legales.

Art. 6.- Conducta de los usuarios del correo electrónico institucional

a) El uso del correo electrónico será para realizar funciones inherentes a su cargo.

b) El usuario se compromete a utilizar este medio de comunicación con fines laborales.

c) El usuario es responsable de los actos que sucedan con su cuenta de correo electrónico.

d) No se debe utilizar el correo electrónico para el envío de cadenas, concursos, cartas, ventas, etc.

Capítulo 4: SERVICIO DE INTERNET

Art. 7.- Asignación del servicio de internet.- La Coordinación de Tecnologías de la Información y Comunicaciones, proveerá a quien lo solicite previa autorización de su jefe inmediato, el servicio de internet a quienes lo necesiten para realizar tareas específicas de su cargo.

Art. 8.- Usos y contenidos.- El servicio de internet estará restringido a ciertas normas que dependerán de los permisos defina la Coordinación de Tecnologías de la Información y Comunicaciones. Considerando lo siguiente:

a) La creación de grupos de páginas web, que dependerán de las actividades que van a realizar.

b) La creación de categorías para los usuarios, dependiendo de las necesidades que requieran para realizar su trabajo.

c) Establecer horarios de uso, según las categorías antes mencionadas y dependiendo de los días de trabajo y las horas definidas.
d) Evitar el descargar archivos no autorizados y acceder a paginas no autorizadas.
e) Instalar programas no permitidos o prohibidos.

Título IV

DE LAS SANCIONES

Capítulo 5: DE LAS RESPONSABILIDADES Y SANCIONES

Art. 9.- De las responsabilidades.- Se establece que el uso del presente, está formalizado y determina que se debe cumplir con los aspectos aquí indicados, ya que estos artículos están orientados a utilizar de forma correcto los servicios informáticos y los equipos servidores de la organización, así como el realizar los respectivos backups de información.

Art. 10.- De las sanciones.- En el caso del uso incorrecto de las normas antes mencionadas o que causen algún tipo de daño a los funcionarios o atenten contra la imagen de la organización, y se consideren como faltas graves, a la persona que infrinja se le aplicará las sanciones pertinentes al reglamento interno de administración, e igualmente se aplicarán sanciones civiles y penales según sea el caso.

Título V

DE LA SOCIALIZACIÓN DE LAS PRESENTES POLÍTICAS

Capítulo 6: DE LA SOCIALIZACIÓN

Art. 11.- De la socialización.- Previo al uso de las presentes políticas, se dará a conocer a los usuarios de los equipos servidores y de los servicios informáticos que posee la organización, las instrucciones relativas al mismo, indicándoles las responsabilidades que están presentes.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Las Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos para diferentes organizaciones, permiten proteger la integridad, confidencialidad y disponibilidad de la información, los equipos servidores y las diferentes herramientas tecnológicas en virtud de que presentan las mejores prácticas administrativas para optimizar los recursos de la empresa y permiten a los usuarios concientizar sobre uso correcto de las mismas.

Los equipos y la información de la organización son activos de la misma que deben protegerse, es decir no podemos prescindir de ellos y tomarlos a la ligera, además la elaboración de políticas para resguardarlos son de gran ayuda para el normal desenvolvimiento de sus actividades normales, con el fin

de establecer responsabilidades y tomar medidas o sanciones a quienes usen de forma equivocada la información que está orientada a otros fines.

Antes de realizar políticas de seguridad informática, debemos tener la seguridad de que son necesarias, para esto se debe realizar un análisis de la situación actual en la organización y definir si realmente es necesario o no, ya que depende mucho del tamaño de la organización, en número de empleados y en relación a los equipos que poseen, además de los servicios informáticos que proveen.

No olvidemos también que al establecer políticas de seguridad informáticas, éstas deben estar directamente relacionadas con los objetivos empresariales y que deben contar con el aval de la gerencia o administración de la organización y que sin el apoyo de ésta, no se podrán implantar; es decir, partimos del apoyo tanto administrativo, técnico y legal, así como con los recursos que sean necesarios para hacerlo.

Finalmente, una vez realizadas las políticas de seguridad informáticas, éstas deben socializarse en la organización, de tal forma que se den a conocer a todos y cada uno de los usuarios de los servicios en la empresa, con el objetivo de darles a conocer cuan importantes son estas medidas para la organización, tanto grupal como personalmente, además de proporcionarles la información sobre las responsabilidades y las posibles sanciones a las cuales estarían sujetos de ser el caso cuando hayan incurrido en la contravención de alguna de estas medidas y normas.

Recomendaciones

La aplicación de Soluciones Tecnológicas en Seguridades de la Información para procesos administrativos, pueden ajustarse a las necesidades de la organización ya que define metodológicamente el procedimiento de realizar las políticas de seguridad y los procedimientos de seguridad administrativa a seguir, por lo que su aplicación depende únicamente del poder que ejerza la administración de la empresa.

Si la organización determina que es necesaria realizar la aplicación de estas políticas en la misma, se debería conformar el comité de seguridad informático, que conjuntamente con el área administrativa permitirán la aplicación de las medidas de la forma que sea mejor para la empresa.

Al establecer las políticas de seguridad informáticas, éstas deben establecerse y ponerse en práctica lo más pronto posible, con el fin de poder aprovechar los recursos y los medios que posee la organización.

No debemos olvidar que es primordial la socialización de estas medidas, y la aplicación inmediata, porque cada una de estas políticas cumplirá en algún momento sus etapas de desarrollo, con la fase de eliminación, como todo en este mundo cumplirá su ciclo de vida, además que las políticas deben de ser flexibles y permitir sus cambios acordes a las variaciones de los objetivos de la organización.

Bibliografía

- Wikipedia http://es.wikipedia.org/wiki/Pol%C3%Adtica
- Concepto de seguridad http://definicion.de/seguridad/
- Concepto de procedimiento http://definicion.de/procedimiento/
- Seguridad Informática http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- Pirámide Digital. Academia Latinoamericana de Seguridad Informática, "Política de Seguridad", Módulo #3. http://www.piramidedigital.com/Documentos/ICT/pdictseguridadinformaticapoliticas.pdf
- "Política Informática", (2004) realizada por el Comité Técnico Informático del Municipio de Guanajuato.
- Asamblea Constituyente, "Constitución Política de la República del Ecuador",(2008) http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf
- Subsecretaria de Tecnologías Informáticas - Manual de seguridad en redes "Coordinación de Emergencia en redes teleinformáticas", http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf
- "Coordinación de emergencia en redes teleinformáticas" Manual de seguridad http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf

- Actualización de Backups, Tivoli Software, http://www.redsis.com/soluciones-especializadas/automatizacion-de-backups

- Information Security and Risk Management, CISSP Security Training – Information Security and Risk Management

- Análisis de Riesgos de Seguridad de la Información, Juan Manuel Matalobos, Universidad Politécnica de Madrid.

- Manual de seguridad en Redes, Coordinación de emergencia de redes teleinformáticas de la Administración Pública Argentina.