UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

Plan estratégico informático para la empresa "American Deportes"

ESTUDIANTE

Romel Patricio Cobos León.

Tutor

Ing. Diego Fajardo

Cuenca – Ecuador

Diciembre 2011

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Diego Fajardo certifico que el señor Romel Patricio Cobos León con C.C. No. 010229238-0 realizó la presente tesis con título "**Plan estratégico informático para la empresa "American Deportes**"", y que es autor intelectual del mismo, que original auténtico y personal.

_____

Ing. Diego Fajardo

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

ACTA DE CESIÓN DSE DERECHOS

Yo, **Romel Patricio Cobos León**, estudiante de **Sistemas Informáticos** declaro conocer y aceptar las disposiciones del Programa de Estudios de Ingeniería Informática, que en lo pertinente dice: “Es patrimonio de la Universidad Israel, todos los resultados provenientes de investigaciones, de trabajos artísticos o de creación artística o científicos o técnicos o tecnológicos, y de tesis o trabajos de grado que se realicen a través o con el apoyo de cualquier tipo de la Universidad Tecnológica Israel. Esto significa la cesión de los derechos de propiedad intelectual a la Universidad Tecnológica Israel”.

_____

Romel Patricio Cobos León

UNIVERSIDAD TECNOLÓGICA ISRAEL

FACULTAD DE SISTEMAS INFORMATICOS

CERTIFICADO DE AUTORÍA

El documento de tesis con título "**Plan estratégico informático para la empresa "American Deportes**"" ha sido desarrollado por Romel Patricio Cobos León con C.C. No. 010229238-0 persona que posee los derechos de autoría, responsabilidad, restringiéndose la copia o utilización de cada uno de los productos de ésta tesis sin previa autorización.

_____

Romel Cobos León

DEDICATORIA

A Clary y Amelia, por ser la fuerza que me impulsa.

AGRADECIMIENTO

A mis padres, por la espera.

A mi director de tesis por la paciencia y el apoyo.

A la Universidad Israel por la oportunidad y facilidades brindadas.

RESUMEN

El incontenible avance del internet a todos los niveles y rincones del planeta, adicionado al gran crecimiento en la oferta de servicios que ésta presenta a permitido que muchas empresas a nivel global dependan y necesiten estar siempre en contacto con sus clientes, proveedores, bancos, empresas públicas a través de mensajeros, redes sociales y correos electrónicos.

Por otro lado también ha existido un crecimiento de los delitos informáticos en sus diferentes niveles cada día aumenta en relación al desarrollo tecnológico.

Por ello es preciso desarrollar un plan estratégico informático, que involucre además una serie de instrucciones para conseguir iniciativas para la empresa “American Deportes” que permitan evitar el decaimiento de su capacidad de procesamiento de información.

Este proyecto, pretende presentar un manual de procedimientos mínimos que se deben tomar en cuenta a la hora de tratar con la información generada en “American Deportes” en lo relacionado con la seguridad.

SUMMARY

The unstoppable advance of the internet to all levels and corners of the globe, added to the great growth in the supply of services which it presents to allowed many companies at the global level dependent and need to be always in contact with customers, suppliers, banks, public enterprises through messengers, social networks and emails.

On the other hand also there has been a growth of computer-related crime in its different levels every day increases in relation to technological development.

It is therefore necessary to develop a manual of procedures for computer security, involving a number of instructions to get initiatives for the company "American Deportes" to avoid externally as internal attacks on its information processing ability.

This project aims to provide a Handbook of minimum procedures to be taken into account when dealing with the information generated in "American Deportes".

INDICE

CAPITULO 1

INTRODUCCIÓN

La información que empresas e individuos poseen son uno de los activos con más valor, debido a que representan en muchos casos grandes oportunidades de negocio, información de seguridad, información sobre cuentas bancarias, o simplemente informaciones que deben permanecer disponibles, accesibles y seguras sólo para las personas autorizadas para este propósito.

En la actualidad, con el creciente acceso a internet por parte de empresas e individuos y con las facilidades de acceso a estos recursos y el aumento en el caso del uso de las redes sociales, esa información corre grandes riesgos de ser observada y modificada por personas no autorizadas para tal cometido.

Por otro lado, la seguridad de la información no solo se ve expuesta por factores ligados al exterior de la organización sino también al interior, debido en parte a las facilidades de extracción, compresión y transporte de información en grandes volúmenes en dispositivos realmente pequeños y por lo tanto difíciles de detectar.

Además el último aspecto que afecta la seguridad de la información, está relacionado con los medios físicos o hardware que se usan para contenerla y sobre todo la calidad de los respaldos que se tenga de ella.

En consideración a lo anterior, es necesario diseñar planes de seguridad sustentados por manuales para este efecto, en donde se determine de forma clara, el cómo, el quién y cuándo se deben ejecutar las tareas dedicadas a este propósito. Asegurando de este modo que con la aplicación de éstos procedimientos se minimizará el riesgo de pérdida o fuga de información.

Además de permitir al máximo posible la disponibilidad, integridad y confidencialidad de la información. (ISO/IEC 13335-1:2004).

Finalmente se puede decir que la elaboración de un plan estratégico integral empresarial, sería de mucha utilidad como un factor de apoyo al crecimiento de la empresa.

1.2.- Planteamiento del problema

1.2.1.- Antecedentes:

American Deportes es una empresa dedicada a la elaboración de uniformes deportivos, establecida en Cuenca desde el año 1984 y desde entonces hasta el año 2009, sus procesos de producción y contabilidad eran llevados de forma manual en su totalidad; a partir de esa fecha se implementó un sistema de control de la producción a partir de órdenes de trabajo.

El primer inconveniente se presenta en el manejo correcto de los equipos de cómputo.

Sin embargo de lo anterior expuesto, durante este tiempo se han venido produciendo ciertos problemas con los clientes, relacionados con los tiempos de entrega de la produccción, por razones generadas en la vulnerabilidad de la red en general.

Se producen retrazos en la entrega de producto terminado con alguna frecuencia durante los ultimos tres años en un promedio de cinco por año; relacionada directamente con el mantenimiento adecuado del hardware involucrado en la producción de bordadosy patrnaje; generándose de este modo un sentimiento de desconfianza por parte de los clientes.

Existen además tiempos de para en las jornadas de trabajo de los empleados del área de producción debido a multiples problemas que tiene relacion con entes internos y externos por maleware que afectan el desempeño del software de los equipos dedicados tanto al area de producción como de los del área administrativa. Ocasionando de esta forma tiempos osciosos y por lo tanto pérdidas economicas derivadas de esto.

Además algunos empleados pierden valioso tiempo para la empresa en redes sociales y en navegación en internet, poniendo en riesgo los datos de la empresa.

Esto fue determinado mediante un seguimiento realizado por el departamento de gestión de talento humano de la empresa.

1.3. Sistematización

1.3.1.- Diagnóstico:

¿Podrán disminuir los tiempos de para de la producción de la empresa una serie de políticas de seguridad planteadas para tal efecto?

1.3.1.1.- Causa - Efectos

Al no existir políticas de mantenimiento, se presentan fallas en los equipos de cómputo en todas las áreas.

Los antivirus instalados son ilegales y están desactualizados, por lo tanto no sirven de protección.

No disponen de ningún tipo de actualización del software, lo que deja huecos de seguridad en cada equipo y por lo tanto en la red empresarial.

Tampoco existe un plan de contingencia ante fallos, es decir nadie sabe que hacer en caso de una falla en los equipos informáticos.

El mecanismo de respaldos es inexistente, lo que ocasiona un alto riesgo de perder información vital para la empresa.

Todo lo anterior se refleja en el grafico 1.

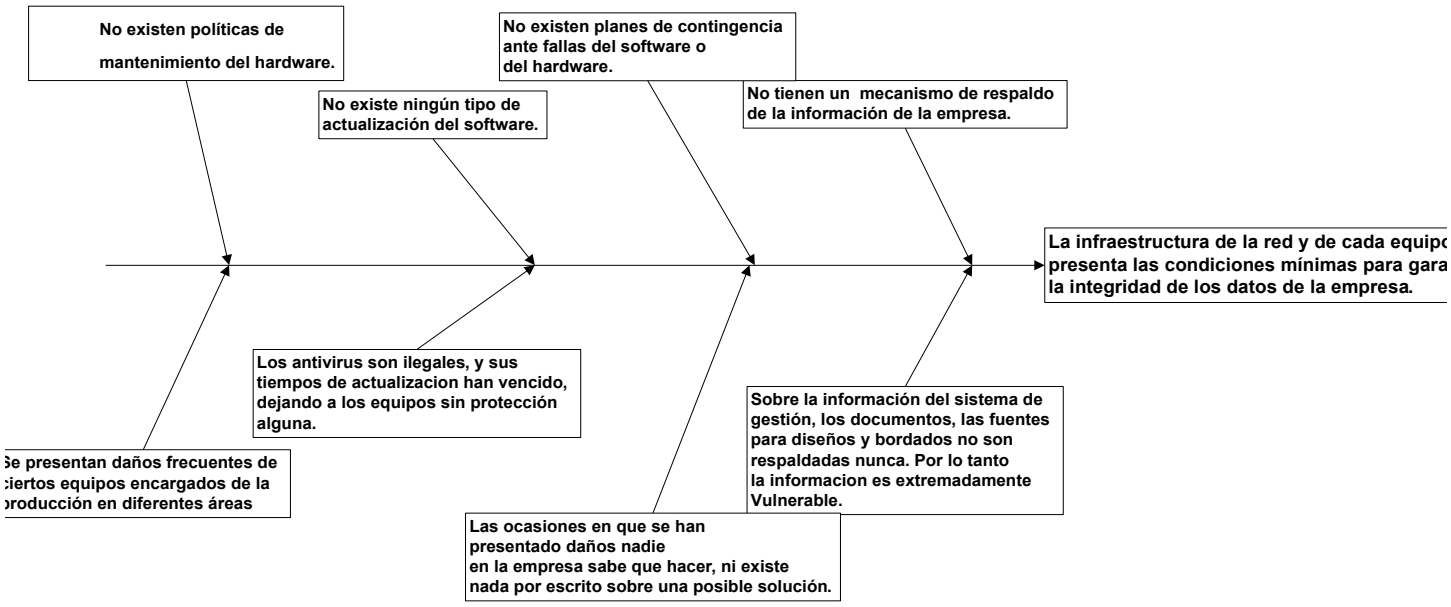

Gráfico 1.- Espina de pescado, diagrama de causa y efecto.

1.3.2.- Pronóstico:

Si se mantiene la tendencia actual de mantenimiento, es posible llegar a perder la confianza de los clientes mayoristas por tiempos de entrega muy extensos en razón de que al no existir mantenimiento preventivo adecuado y oportuno de los equipos, éstos fallan impidiendo la continuidad de los procesos productivos.

Al no tener un plan estratégico de TI anti maleware la empresa paga a sus empleados por tiempos nó productivos, es decir los equipos suelen contaminarse con frecuencia dejando a los empleados sin poder realizar las tareas que la empresa requiere durante el tiempo que se toma para la desinfección de los equipos.

La inconciencia con respecto a la seguridad por parte de todos los empleados y la inexistencia de apropiados controles puede en algún momento poner en riesgo la integridad de los datos y otro tipo de información estratégica de la empresa.

1.3.3.- Control del Pronóstico:

Con este proyecto, se espera que las políticas planteadas contribuyan a mejorar el desempeño de los equipos dedicados a la producción a través de la elaboración de un cronograma de mantenimiento preventivo, permitan mejorar los tiempos de entrega de producto terminado a sus clientes, proporcionando así la confianza necesaria que este negocio requiere de sus clientes.

Si se llegan a implementar el plan estratégico de seguridad propuesto en este proyecto en lo relacionado con el control de amenazas a la empresa, se proveerá a los empleados de un ambiente detrabajo adecuado para el desempeño de sus tareas.

Con las políticas relacionadas con el control de de acceso a sitios de internet se espera mejorar la seguridad de la red de la empresa frente a las amenazas de un servicio de internet indiscriminado además de descongestionar el tráfico para las tareas propias del giro del negocio.

1.3.3.1.- Formulación de la Problemática Específica

1.3.3.1.1. - Problema principal:

La infraestructura de la red y de cada equipo no presenta las condiciones mínimas para garantizar la integridad de los datos de la empresa.

1.3.3.1.2.- Problemas secundarios

a) No existen políticas de mantenimiento del hardware.

b) No existe ningún tipo de actualización del software.

c) No existen planes de contingencia ante fallas del software o del hardware.

d) No tienen un mecanismo de respaldo de la información de la empresa.

1.4.- Objetivos

1.4.1.- Objetivo General:

Elaborar un plan estratégico informático para mejorar la gestión de seguridad de la empresa American Deportes como factor de apoyo para elevar su productividad.

1.4.2.- Objetivos Específicos:

- Elaborar un manual de procedimientos que permita garantizar la seguridad informática en la empresa American Deportes.

- Evaluar el estado actual de la empresa agrupando los problemas de seguridad informática que se detecten.

- Crear un método para evaluar los mejores caminos para determinar las opciones tanto técnicas como económicas para la empresa, acorde con su capacidad. Con respecto a mantenimiento, seguridad, actualización, uso, capacitación de software y de hardware.

- Desarrollar una metodología para el mantenimiento preventivo y daños de equipos informáticos ante amenazas internas y externas.

1.5.- Justificación.

1.5.1.- Teórica:

La seguridad no sólo involucra el software y el hardware sino también otros aspectos como la forma en la que los usuarios de la red se comportan con relación a los datos, para lo que se requiere generar responsabilidad.

Además se debe tomar en cuenta un artículo que publica la BBC de Londres relacionada al tema “Más de 70 organizaciones en todo el mundo, entre ellas Naciones Unidas y el Comité Olímpico Internacional, han sido blanco de ciberataques, señaló la empresa McAfee.

Los ataques han continuado por años y, según McAfee, 49 de las 72 organizaciones afectadas están situadas en Estados Unidos.

La compañía indicó que los intrusos estaban buscando información delicada en sistemas militares y comunicaciones satelitales.

"Estamos enfrentando una transferencia masiva de riqueza en la forma de propiedad intelectual que no tiene precedente en la historia", señaló Dmitri Alperovitch, directivo de McAfee.

Según expertos citados por el diario *The Washington Post* los ataques parecen tener origen en China, aunque esto no ha sido confirmado por McAfee.". Alperovitch, D. (2011, 3 de Agosto). Revelan ciberataques a más de 70 organizaciones en todo el mundo. *BBC de Londres en español*. Recuperado de : http://www.bbc.co.uk/mundo/ultimas_noticias/2011/08/110803_ultnot_ciberataques_mcafee_sao.shtml

1.5.2.- Práctica:

Se debe en principio establecer un cambio radical a la forma de tratar a los equipos de red y de su interconexión.

El presente proyecto consiste en elaborar una política lo más completa posible para el mantenimiento de los equipos dedicados a la producción que son apoyados por el departamento de TI, en la empresa American Deportes, de forma que los clientes confíen que sus productos terminados sean entregados a tiempo.

También se pretende elaborar un plan que permita disminuir al mínimo posible los tiempos de para de las jornadas laborales ocasionadas por amenazas externas o internas y de éste modo se ahorre dinero.

Además se debe establecer una serie de reglas para permitir o negar ciertos aspectos relacionados con el acceso a los servicios de internet.

Para conseguir todo lo anterior se aplicarán todas las estrategias que estén disponibles y que sean accesibles tanto técnicamente como económicamente para la empresa de elaboración de prendas de vestir de modo que tienda a conseguir confidencialidad, integridad y disponibilidad de la información.

1.6. Alcance y Limitaciones.

1.6.1. Alcance

El Plan estratégico Informático tendrá cuatro partes principales:

- Evaluación e la situación actual
- Método de Evaluación Técnica y económica
- Manual de Procediminetos de Seguridada Informática
- Metodología para mantenimineto preventivo.

1.6.2. Limitaciones

No se hará la implementación por razones por razones de tiempo y económicas.

1.7. Estudios de Factibilidad

1.7.1. Factibilidad Técnica

En éste aspecto se debe tener en cuenta que la empresa no dispone de un material como el que se propone en el presente proyecto denominado Plan Estratégico Informático para la empresa “American Deportes”, de modo que será una contribución de carácter novedoso para todo el personal y directivos de dicha empresa. Además se espera que con este proyecto se motive a los directivos a la conclusión del Plan Estratégico Empresarial.

1.7.2. Factibilidad Económica

En este punto se debe aclarar que los costos de elaboración del presente Plan Estratégico Informático serán asumidos por la Empresa “American Deportes”, por lo que no es un problema su construcción.

CAPITULO 2.

MARCO DE REFERENCIA

2.1.- Marco Teórico

Se planteará inicialmente una fase de observación, donde se hará una visita a las instalaciones de la empresa de elaboración de prendas de vestir en todos sus departamentos, secciones y bodegas de almacenamiento, tanto de producto terminado, mercadería y materia prima, con el objetivo de tener una visión clara de cuáles son los departamentos con mayores conflictos de seguridad, y cuales son

más críticos para el giro del negocio, además de las áreas previamente revisadas por los directivos de la empresa.

En el presente trabajo de elaboración del plan estratégico informático tratará específicamente de implementar al máximo posible las normas de seguridad establecidas en el CISSP “Certified Information Systems Security Profesional”, acreditada bajo los estándares *ISO/IEC 17024; todo esto únicamente delimitado por la capacidad económica de la empresa American Deportes al momento de su aplicación.

En adición a esto se pretende que las seguridades físicas y el ambiente de trabajo del servidor sean lo más adecuados posible.

También se prevé que cada computador de la red tenga las instalaciones tanto eléctricas como de red mejoradas sustancialmente, es decir que su ambiente sea el apropiado.

Se debe evaluar las ventajas y prestaciones de algunos software de seguridad anti software malicioso para cada computador de la red con mecanismos de actualización centralizada para no usar el ancho de banda todo el tiempo.

También se realizará una mejora en la calidad de las conexiones de red has conseguir al menos una red de categoría 5.

Por último se debe establecer un plan de protección a datos a base de respaldos oportunos y bien implementados.

Todo esto enmarcado en la Seguridad Física del Entorno.

2.2.1. Conceptos Básicos

Antes de empezar con la elaboración del manual de procedimientos de seguridad, se debe conocer ciertas definiciones para poder entender el desarrollo del presente proyecto.

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

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

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

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

2.2.1.5. Seguridad física.- Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a

los recursos e información confidencial que puedan interrumpir procesamiento de información.

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

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

2.2.1.8. Seguridad en los recursos humanos.- Consiste en los controles que se deben tener con respecto a la selección, contratación, capacitación y despido del empleado.

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

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

2.2.1.11. Qué es un Plan Estratégico Informático?

"Un Plan Estratégico de Informático es un conjunto de definiciones tecnológicas e iniciativas de TI que deben soportar la visión, misión y estrategias que el negocio tiene para un horizonte de tiempo definido."

Recuperado de:

http://www.deloitte.com/view/es_PE/pe/servicios/consultoria/tecnologia-de-la-informacion/planeamiento-estrategico-de-tecnologias-de-informacion/index.htm

2.2.1.12. Qué es manual de procedimientos informático de seguridades?

"Un manual de la procedimientos de seguridad informática 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".

Recuperado de:

Adolfo Araujo J. *Ingeniero* de la Universidad Tecnológica de El Salvador y *Máster en Ingeniería Web* de la Universidad Carlos Tercero de Madrid. Obtenido el: 27/10/2011. Recuperado de: http://inf-tek.blogia.com/2009/060207-8.5-manual-de-politicas-de-seguridad-informatica.php

2.2.- Marco Espacial

La investigación se hará para American Deportes que es una empresa dedicada a la elaboración de uniformes deportivos, establecida en Cuenca.

2.3 Marco Temporal:

El presente trabajo se realizará en el transcurso de dos meses.

CAPITULO 3.

METODOLOGÍA

3.1. Metodología de Investigación.

3.1.1. Tipo de Investigación

Se aplicará el tipo de Investigación de Campo.

3.1.2. Métodos

Para la elaboración general de este proyecto será usado el método propositivo, en razón de que al final se propondrá una solución tentativa a la problemática planteada.

3.1.3 Técnica de Investigación

Para el levantamiento de la información me basaré en el método de investigación científico de observación "Prof. María Soledad Fabbri, Argentina., *Las técnicas de investigación: la observación.* Obtenido el: 02/09/2011.

Recuperado de: http://www.fhumyar.unr.edu.ar/escuelas/3/materiales%20de%20catedras/trabajo%20de%20campo/solefabri1.htm".

En cambio para la parte de análisis de los datos recopilados se utilizara el método deductivo, "Roberto Gómez López, Universidad de Málaga, España., *Evolución Científica y Metodológica de la Economía.* Obtenido el: 02/09/2011.

Recuperado de: http://www.eumed.net/cursecon/libreria/rgl-evol/2.4.2.htm".

Para la elaboración del plan estratégico informático se usarán las técnicas descritas en el CISSP “Certified Information Systems Security Profesional”, Acreditada bajo los estándares * ISO/IEC 17024 "General Requirements for Bodies Operating Certification of Persons“ (Normativa Internacional para Organizaciones y Entidades en busca de Reconocimiento Internacional en Materia de Certificación de Individuos); que son una serie de técnicas y recomendaciones de cómo se debe llevar de una manera estándar que permite asegurar confidencialidad, integridad y disponibilidad de la información.

3.1.4. Instrumentos

En un inicio se aplicará una entrevista con el gerente general para determinar las secciones de la empresa con problemas.

Se aplicará el método de observación con el objetivo de precisar los equipos con problemas de seguridad físicos.

También se procederá a tomar nota de los tiempos históricos de para de los equipos informáticos dedicados a la producción.

Por último se pondrá énfasis en los tiempos perdidos en los departamentos administrativos por contaminación con algún tipo de maleware, recabando información del departamento de personal que durante el año 2010 y lo que va del 2011 ha realizado el seguimiento.

Todo será colocado en una matriz, para ser presentado y evaluado.

3.1.4.1. Método de evaluación técnico en mantenimiento.

1. Sabe si disponen de un antivirus los equipos de computación de la empresa que usted dirige?

2. Sabe si sus equipos de computación disponen de seguridades ante amenazas provenientes del exterior tal como internet?

3. Sus antivirus poseen licencias actualizadas?

4. Existe algún tipo de restricción en el uso de memorias flash para los usuarios de la red de datos de su empresa?

5. Por qué su servidor de archivos y base de datos no tiene un lugar acondicionado adecuadamente para su ubicación?

3.1.4.2. Método de evaluación técnica en actualización.

1. Sabe que existen mecanismos de actualización de software ?

2. Sabe que beneficios puede obtener su empresa mediante las actualizaciones de software?

3.1.4.3. Método de evaluación técnica en capacitación de uso.

1. Sus empleados saben qué información es de exclusiva propiedad de la empresa?

2. Sus empleados están entrenados para tomar las mediadas adecuadas a la hora de usar memorias flash?

3. Sus empleados y usted saben cuál es la forma de mantener sus equipos informáticos en buen estado físico?

4. Cuantas veces durante el año 2010 se ha quedado sin trabajar sus equipos de computo por daños causados de forma involuntaria de parte de sus empleados, y cuantos en los seis primeros meses de este año?

3.1.4.4. Método de evaluación técnica en respaldo de información.

1. Se hacen respaldos de la información de la empresa con alguna frecuencia?

2. Los respaldos de la información contemplan las bases de datos del sistema de gestión de la producción y los documentos o solamente uno de ellos?

3. Cuantas veces durante el año 2010 ha perdido algún tipo de información de sus equipos de computo por falta de respaldo de información, y cuantos en los seis primeros meses de este año?

CAPÍTULO IV

DESARROLLO

4.1. Plan estratégico Informático.-

Al presentar el plan estratégico informático para la empresa “American Deportes” se trata de asignar un cierto grado de organización al área de TI con respecto a la situación actual, sin embargo se debe tener en cuenta que la empresa carece de un plan estratégico empresarial lo que únicamente permite establecer que el plan de TI se centra en la tarea de mantenerla funcionando.

El objetivo de este plan es proporcionar un punto de partida de carácter urgente a la situación en la que se encuentra en la actualidad, enfocando la atención en cuatro ejes fundamentales:

a) Evaluar el estado actual de la empresa agrupando los problemas de seguridad informática que se detecten.
b) Utilizar un método para evaluar los mejores caminos para determinar las opciones tanto técnicas como económicas para la empresa, acorde con su capacidad. Con respecto a mantenimiento, seguridad, actualización, uso, capacitación de software y de hardware.
c) Elaborar un manual de procedimientos que permita garantizar la seguridad informática en la empresa American Deportes.

d) Desarrollar una metodología para el mantenimiento preventivo y daños de equipos informáticos ante amenazas internas y externas.

Se debe tener presente que el plan informático aquí propuesto debe ser revisado, mejorado y actualizado en el corto plazo, es decir dentro del año siguiente luego de su aplicación inicial.

4.2. Fase de Análisis

4.2.1. Análisis de la situación actual.

A través de una entrevista con la Gerente General de la empresa American Deportes, al iniciar la relación de trabajo, se pudo notar cierto descontento relacionado con la disponibilidad de los equipos de la empresa, se mencionó que a veces la computadora encargada de llevar a cabo el bordado de prendas no funciona, y que deben llamar a una persona que luego de algunos días llega a la empresa, hace algo en ese computador y funciona nuevamente bien durante unos días, pero que luego vuelve a presentar algún tipo de fallas, debiendo tener presente que durante el tiempo que demora en llegar a la empresa la persona encargada, los bordados deben ser enviados a maquilar en otra empresa, lo que les ocasiona un incremento en los costos de producción.

Para poder determinar las falencias en los diferentes aspectos de la seguridad informática se plantearon las siguientes entrevistas al Gerente de la Empresa clasificadas como sigue:

4.2.1.1. Método de evaluación técnico en mantenimiento.

En este caso es el gerente general el que responde el cuestionario:

1. No sabe cada cuanto tiempo se hace mantenimiento preventivo a nivel físico de los equipos de computación.

2. El último mantenimiento preventivo a nivel físico de los equipos de computación se hizo aproximadamente hace un año y medio.

3. Había un responsable que bajo demanda hacia el mantenimiento preventivo, pero desde hace un año y seis meses que le llamamos, pero él no viene, dice que está muy ocupado en otra cosa.

4. El gerente sí está de acuerdo en crear un plan de mantenimiento preventivo a nivel físico de los equipos de computación.

5. Tres veces, lo que significa que tuvimos que mandar a producir en otro lado unos bordados para los bomberos, perdimos 0.25 por gorra, y eran 5000 gorras.

4.2.1.2. Método de evaluación técnica en seguridad.

En vista de que no existe un técnico responsable de la red de datos y de los equipos de cómputo se continúa el cuestionario con el gerente general.

1. No sabe si disponen de un antivirus los equipos de computación de la empresa, aunque dice “que parece que todas tienen, pero así mismo en

cada computadora sale que el antivirus no se puede conectar con algo, la verdad no entiendo nada de eso".

2. No sabe si los equipos de computación disponen de seguridades ante amenazas provenientes del exterior tal como internet.

3. Nunca ha comprado licencias de antivirus.

4. No existe ningún tipo de restricción en el uso de memorias flash para los usuarios de la red de datos de su empresa.

5. El lugar donde se encuentra el servidor de archivos y base de datos actualmente estaba vacío y era solo para ese equipo de computación, pero luego nos hizo falta un lugar para cortar tela y aprovechamos el espacio de ese cuarto.

4.2.1.3. Método de evaluación técnica en actualización.

1. No sabe que existen mecanismos de actualización de software.

2. No sabe qué beneficios puede obtener su empresa mediante las actualizaciones de software.

4.2.1.4. Método de evaluación técnica en capacitación de uso.

1. Los empleados no tienen idea alguna que la información es de exclusiva propiedad de la empresa.

2. Los empleados no están entrenados para tomar las mediadas adecuadas a la hora de usar memorias flash.

“La verdad no tengo esa información, pero el jefe de producción ha dicho un par de veces que la computadora de bordados se ha infectado por causa de un virus de una memoria flash, pero como él es ingeniero agrónomo no sé si creerle”.

3. Ni el gerente ni ninguno de los empleados saben cuál es la forma de mantener sus equipos informáticos en buen estado físico.

4. Dos veces durante el año 2010 se han quedado sin trabajar los equipos de cómputo por daños causados de forma involuntaria de parte de sus empleados.

4.2.1.5. Método de evaluación técnica en respaldo de información.

1. No se hacen respaldos de la información de la empresa, porque el único que sabía hacer eso era el anterior encargado que ya no viene.

2. No existen respaldos de bases de datos del sistema de gestión de la producción y los documentos.

3. Existen datos importantes perdidos durante el 2010, a continuación las respuestas del gerente:

Se perdieron unos datos de configuración del plotter de patronaje y nos quedamos dos semanas sin poder trabajar.

También se perdió los datos de marcado de asistencia del personal de todo un mes, en junio del 2010, dijeron los señores del reloj que había sido por

un virus que llego al computador de la contadora que es la que recibe los datos de ese reloj.

4.2.2. Método de Recopilación de Información a través de la Observación de Campo

Para esto se realizó una sesión fotográfica y captura de pantallas en las instalaciones de la empresa con el fin de documentar gráficamente los datos encontrados durante la investigación.

4.2.2.1. Observación del mantenimiento:

Por las imágenes captadas se puede observar que no se ha realizado durante algún tiempo, lo que ha permitido la peligrosa acumulación de polvo y pelusas dentro de los equipos, lo que hace evidente la necesidad de un plan para este propósito, además de los equipos de red como se ve a continuación:

Ilustración 1 Aspecto de un concentrador de la red LAN

Ilustración 2 Otro aspecto del mismo concentrador de la red LAN

4.2.2.2. Observación de la Seguridad:

Por los datos que se pueden ver a continuación se puede tener una idea de lo que ocurre en la empresa, en lo relacionado con los antivirus, y los accesos a internet en computadores claves para el giro del negocio, además se pudo apreciar que todas los computadores tienen acceso ilimitado a internet, no existe un firewall para el tráfico red, solo a nivel de PC, el que viene con Windows XP, y en la mayoría de los casos está inactivo. Además debo presentar a continuación el estado del cableado de red que en algunos casos no es categoría 5.

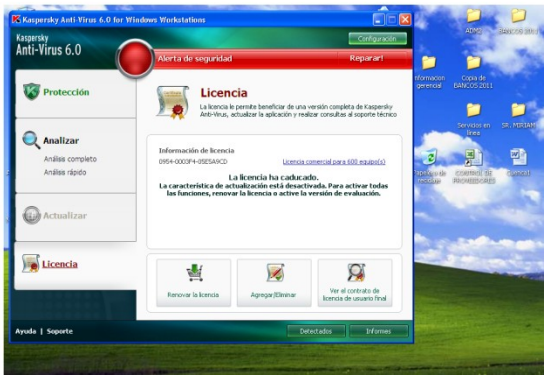

Ilustración 3 Antivirus Vencido.

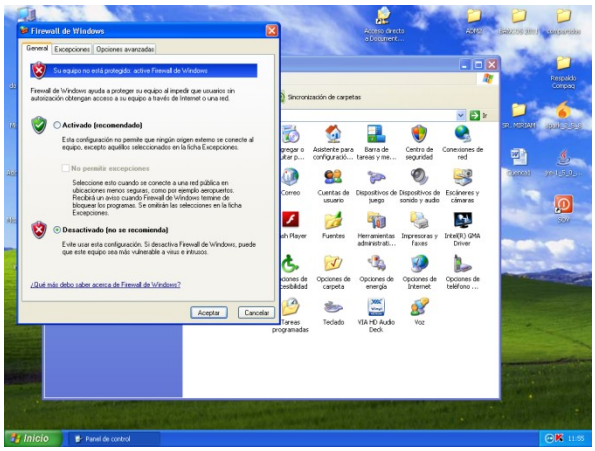

Ilustración 4 Muro de fuego sin usarse

4.2.2.3. Observación de la Actualización:

A través de la observación se determinó que la empresa no tiene sus software tanto de sistemas operativos como de utilitarios de oficina las actualizaciones de seguridad necesarias, tampoco en los navegadores de internet.

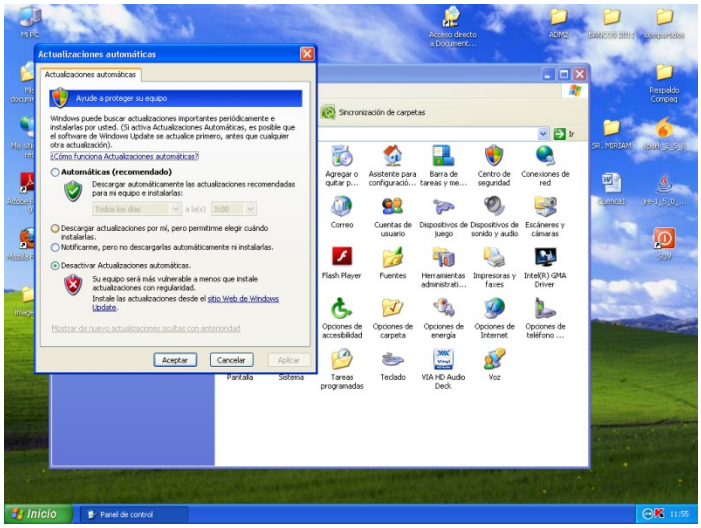

Ilustración 5 Motor de actualizaciones automáticas desactivado

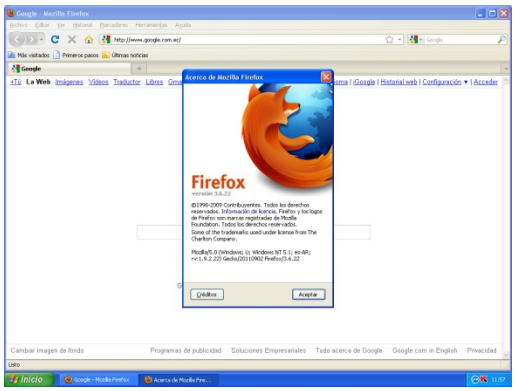

Ilustración 6 FireFox de Mozilla sin actualizar

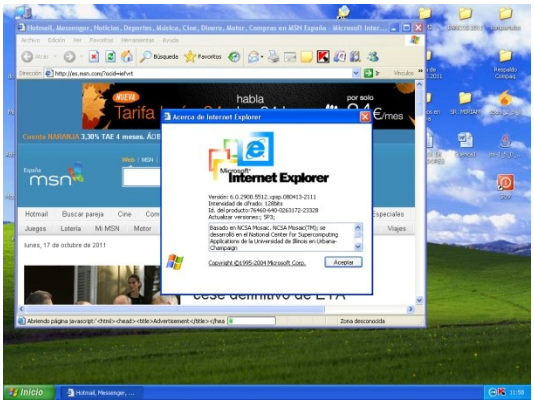

Ilustración 7 Internet Explorer de Microsoft sin actualizarse

4.2.2.4. Observación de la Capacitación de uso:

Se observa falta de conocimientos por parte del personal para el manejo apropiado de los equipos cómputo a ellos entregados por la empresa, como se puede ver a continuación en el computador destinado a la recepción de contratos y el computador de caja:

Ilustración 8 Computador del área de atención al público para contratos de producción.

Ilustración 9 Computador de Caja en el Almacén Matriz

Otro factor sobre el cual se puede presentar un par de fotos es el estado actual; del servidor de la base de datos de la empresa, a continuación:

Ilustración 10 Servidor de bases de datos.

Ilustración 11 Servidor de bases de datos otro ángulo.

4.2.2.5. Observación del Respaldo de información:

No se pudo realizar, porque no existe.

A continuación Tabla1 resume la situación actual de la empresa American Deportes:

	Estado Actual	Descripcion Problemática	Soluciones	Resultado Esperado
Mantenimiento	No se hace mantenimiento preventivo	Actualmente no existe un responsible del mantenimiento preventivo, la ultima vez que es tuvo hizo un mantenimiento hace mas de un año. Cuando hay fallas llaman a un señor de cybercafe	Mantenimineto integral urgente	Disminución de los tiempos de para de los equipos de cómputo
	Ultimo mantenimietno realizado hace 1 año			
	No existe un responsible		Plan cuatrimestral de mantenimiento	
	Numero de veces de interrupcion 3			
	Timepo de para promedio, entre dos y tres dias			
Seguridad	Nunca se han comprado licencias de antivirus	Riesgo legal sobre el uso de software pirata.	Tratar de usar software libre o adquisición de licenias	Mejoramiento en general del estado en el que se encuentra la seguridad en American Deportes de modo que se pueda disminuir las vulnerabilidades
	Uso indiscriminadodel acceso a internet al no disponer de un muro corta fuegos	Todos los equipos tiene acceso total a internet	Determinar que usuarios tienen acceso a internet y a que sitios	
			Usar un software de muro de fuego de preferencia gratuito	
	Cualquier persona tiene acceso al servidor	Todas las personas que transitan en la empresa tiene acceso fisico a las instalaciones donde se encuentra el servidor	Restringir el acceso a las instalaciones del servidor solo a personal de TI o autorizados expresamente para esto.	
	Ubicacion no adecuada del servidor de DB	Incidencia directa de la luz solar, ademas del polvo y pelusas	Ubicar el servidor en un lugar bien veitilado y libre de polvo y pelusas	
Actualización	Antivirus con bases de datos sin actualizar	Nadie sabe sobre los beneficios de tener software legal y actualizado	Tratar de usar software libre o adquisición de licencias	Eliminar si es posible a corto plazo el uso de software sin licencias
	Instalaciones de SO sin actualizar		Tratar de usar software libre o adquisición de licenias y activar las actualizaciones automáticas	Tratar de llegar a usar software libre en todas las áreas de la empresa.
Capacitacion de Uso	Escasa capacitación sobre la forma de manipular los computadores	Los computadores son usados como escritorios auxiliares	Definir a todo el personal sobre la disposición de los equipos de cómputo	Mejorar la calidad del factor humado en lo relacionado con la seguridad de la información empresarial
	Los emplados no son concientes de que la informacion es propiedad exclusiva de la Empresa	Nadie nunca ha hablado de confidencialidad en la empresa	Definir a todo el personal que la información es confidencial y de propiedad de American Deportes	
	Uso despreocupado de todo tipo de memorias flash	Nadie sabe vacunar las memorias	Enseñar a todos los usuario de la red el uso de software antivirus	
Respaldo de Información	No existe ningun tipo de respaldo de información	Lo único que tiene cd s de respaldo son los instaladores de software de gestión y de uno que otro sistema operativo	Establecer un mecanismo de respaldos integral de la informacion de la empresa, para estar preparados ante cualquier concreción de amenazas	Mantener segura toda la información.
				Definir los pasos para la recuperacion de los respaldos en caso de incidentes

Tabla 1.- Descripción de la situación actual con las soluciones propuestas y el resultado esperado.

4.3. Métodos de Evaluación Económica

En esta parte se van a establecer las ponderaciones de los costos que la concreción de una amenaza causaría en la empresa, estos datos se tomarán de la entrevista obtenida del gerente de American Deportes.

Para esto se deben seguir los siguientes pasos, que se detallan en el Análisis Cuantitativo de Riesgos presentado en CISSP Security Training – Information Security and Risk Management

1.- Asignar valores a los activos.

2.- Estimar la pérdida potencial por cada amenaza

3.- Analizar las Amenazas.

4.- Estimar la pérdida anual.

Antes de realizar el análisis cuantitativo de riesgo se debe establecer los siguientes conceptos:

Activo.- Cualquier cosa dentro de una organización que tenga un valor, ya sea de tipo tangible (datos, software, computadoras, documentos, libros, etc.) o intangible (privacidad, seguridad, etc.).

Factor de Exposición (EF).- Porcentaje de pérdida sobre un activo generado por la concreción de una amenaza.

Expectativa de Pérdida Individual (SLE).- Valor monetario asociado a un evento determinado. Representa la pérdida producida por una amenaza determinada en forma individual.

Tasa de Ocurrencia Anual (ARO).- Representa la frecuencia estimada de ocurrencia de un evento (amenaza), dentro del período de un año.

Expectativa de Pérdida Anualizada (ALE).- Representa la pérdida anual producida por una amenaza determinada individual.

Todos estos conceptos tomados de CISSP “Certified Information Systems Security Profesional”. También se debe revisar la Tasa de Ocurrencia Anual (ARO) en el Anexo 3.

4.3.1. Mantenimiento.

ACTIVO :	EQUIPOS DE COMPUTO	EF :	50%
VALOR :	$ 9,100.00	ARO:	3
AMENAZA :	POLVO Y PELUSAS		
SLE :	**Valor x EF**	**$ 4,550.00**	
ALE :	**SLE x ARO**	**$ 13,650.00**	

4.3.2. Seguridad.

ACTIVO :	PROGRAMAS DE SOFTWARE DE GESTION DE CONTROL DE PRODUCCION Y CONTABILIDAD.		EF : 25%
VALOR :	$ 3,500.00		ARO: 2
AMENAZA :	VIRUS		
SLE :	**Valor x EF**	**$ 875.00**	
ALE :	**SLE x ARO**	**$ 1,750.00**	

ACTIVO :	PROGRAMAS DE SOFTWARE REINSTALACION: S.O. Y APLICACIONES		EF : 25%
VALOR :	$ 560.00		ARO : 2
AMENAZA :	VIRUS		
SLE :	**Valor x EF**	**$ 140.00**	
ALE :	**SLE x ARO**	**$ 280.00**	

4.3.3. Actualización.

ACTIVO :	DOCUMENTOS CONTRATOS Y COTIZACIONES.		EF : 75%
VALOR :	$ 10,000.00		ARO: 4
AMENAZA :	INTRUSIONES		
SLE :	Valor x EF	$ 7,500.00	
ALE :	SLE x ARO	$ 30,000.00	

4.3.4. Capacitación de uso.

ACTIVO :	TODA LA INFORMACION EMPRESARIAL	EF :	25%
VALOR :	$ 277,712.10	ARO:	0.50
AMENAZA :	FALTA DE CAPACITACION DE USO		

SLE :	Valor x EF	$	69,428.03
ALE :	SLE x ARO	$	34,714.01

4.3.5. Respaldo de información.

ACTIVO :	SOFTWARE DEL SISTEMA DE GESTION Y SUS BASES DE DATOS	EF :	25%
VALOR :	$ 267,712.10	ARO:	0.50
AMENAZA :	NO RESPALDO DE INFORMACION		

SLE :	Valor x EF	$	66,928.03
ALE :	SLE x ARO	$	33,464.01

El valor es tomado del reporte de ventas correspondiente al año 2010 ver Anexo 2.

Por todos los resultados obtenidos se puede deducir que la empresa tiene un altísimo riesgo de perder mucho dinero debido a la falta de seguridad informática en todas las áreas.

4.4. Elaboración del Manual de Procedimientos de Seguridad Informática

A continuación se detallan los pasos que deben darse para al seguimiento de la implantación de la seguridad en la empresa “American Deportes” de acuerdo al siguiente esquema:

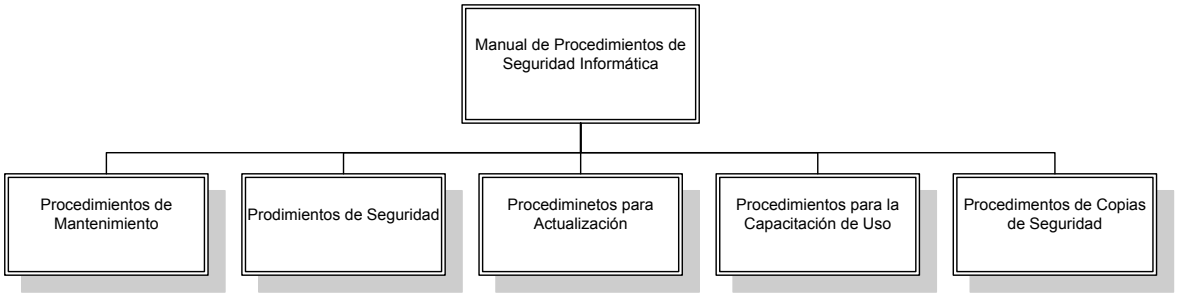

Gráfico 1.- Estructura del manual de procedimientos de seguridad

4.4.1 Procedimientos para el mantenimiento:

Este procedimiento debe ser ejecutado al menos tres veces por año, además debe ser coordinado con los jefes de los diferentes departamentos para que no entorpezca las actividades diarias de cada empleado; y debería comprender todos los componentes físicos electrónicos y mecánicos de los equipos de cómputo de la siguiente manera:

1.- En los CPU se debe ejecutar limpieza de los ventiladores de forma que queden en óptimas condiciones de funcionamiento y todos los demás componentes queden libres de polvo y pelusas.

2.- En las pantallas de debe ejecutar limpieza usando los productos adecuados para éste propósito en relación al tipo de las mismas.

3.- Los teclados deben ser limpiados de forma completa, extrayendo todos los objetos que con el uso se acumulan entre y debajo de las teclas.

4.- Los ratones deben ser limpiados en su interior y exterior de forma y con los productos adecuados en concordancia con el tipo de dispositivo de bola o de luz.

5.- En las impresoras se debe ejecutar un proceso de limpieza completa tanto interna como externa, además de aplicar lubricación especial para este propósito en todas las partes móviles de ser necesario para cada uno de los aparatos de éste tipo que la empresa posea.

6.- Los reguladores de voltaje se deben limpiar de forma profunda y se deben verificar de voltajes de salida con la ayuda de voltímetro y el amperímetro.

7.- Sobre los UPS se debe ejecutar limpieza profunda y verificación de funcionamiento con la ayuda del voltímetro y el amperímetro.

8.- En las Conexiones de la red eléctrica deben ser verificar de voltajes de salida con la ayuda de voltímetro de la siguiente manera:

a) Entre la fase y el neutro se debe medir 110 – 120 voltios de corriente alterna.

9.- La conexión a tierra del edificio debe dar los de voltajes de salida con la ayuda de voltímetro que a continuación se detalla:

a) Entre la fase y la conexión a tierra se debe medir 110 – 120 voltios de corriente alterna.

b) Entre neutro y la conexión a tierra se debe medir menos de un voltio de corriente alterna.

En el aspecto del software se deben ejecutar las siguientes tareas:

1.- Ejecutar el software antivirus sobre cada equipo y sobre todas las memorias flash que se utilicen en la empresa.

2.- Ejecutar programas en busca de software malicioso para su eliminación.

3.- Ejecutar programas de escaneo de errores en el disco duro.

4.- Ejecutar programas de desfragmentación de discos duros.

Este procedimiento debe ser realizado por personal capacitado para el efecto ya sea perteneciente a la empresa o por alguna empresa contratada para éste propósito.

4.4.2 Procedimientos para la Seguridad

1.- Se debe hacer un análisis de programas necesarios por usuario de computador, de modo de poder identificar los que no deben estar en los computadores de los usuarios, puesto que éstos podrían ocasionar problemas de seguridad o de licencias. Este procedimiento debería

comprender la búsqueda de programas instalados a través del panel de control y su posterior desinstalación.

2.- Implementar y verificar el funcionamiento de un software de políticas de filtrado en el perímetro externo conocido también como muro de fuego o firewall; tratando en lo posible el uso de software libre.

3.-En relación a los programas antivirus

a) Se debe instalar el software antivirus en todas las estaciones de trabajo y el servidor de bases de datos.

b) Verificar que las bases de datos de los antivirus se encuentren actualizadas a la fecha de la comprobación.

c) El software antivirus deberá estar certificado por la ICSA (International Computer Security Association).

d) Se debe evaluar la factibilidad de instalar antivirus con capacidades de inteligencia colectiva.

El valor de 5 licencias de Kaspersky Internet Security tiene un valor en el mercado de $ 128.00 dólares de los Estados Unidos de Norteamérica.

Estas tareas se deben realizar con la periodicidad que el factor económico de la empresa lo permita y por personal capacitado para el

efecto ya sea perteneciente a la empresa o por alguna empresa contratada para éste propósito.

4.- El servidor de bases de datos debería ser reubicado con suma urgencia a un lugar que presente mejores condiciones de funcionamiento para evitar daños y exposición innecesaria a peligros de pérdidas de información o de disponibilidad de la siguiente forma:

a) El servidor debe estar alejado del polvo.

b) El equipo servidor debe estar alejado de el exceso de temperatura por la incidencia de los rayos del sol sobre el equipo.

c) El servidor deberá ser ubicado en un lugar con buena ventilación.

d) El área donde se instale el servidor debe tener acceso restringido, de forma que solo pueda acceder a él personal autorizado o de TI exclusivamente.

El valor de la licencia de Win2008 server 32 bits es de $ 790.00 dólares de los Estados Unidos de Norteamérica.

Todo éste procedimiento debe estar acorde con la disponibilidad de económica de American Deportes.

5.-Sobre el uso y cambio de contraseñas

a) Se debe instruir a los usuarios de la red y de los diferentes servicios de internet sobre el uso de palabras que solo ellos recuerden.

b) Que las contraseñas tengan una longitud lo mayor posible de recordar.

c) Que sean cambiadas cada tres meses al menos.

4.4.3. Procedimientos para la Actualización.

En este caso se deben tener presentes muchos factores, sobre todo por la seguridad de los sistemas operativos, por lo tanto:

a) Verificar la instalación de actualizaciones de seguridad liberadas para sistemas operativos.
b) También se debe realizar una verificación del software de aplicaciones instalado en cada computador para determinar su compatibilidad con nuevas versiones disponibles en el mercado.
c) Y si fuere necesario la inmediata instalación de los paquetes de actualización liberados para éstos propósitos.

El precio de la licencia de Win7 32 bits es de $ 162.00 dólares de los Estados Unidos de Norteamérica.

El precio de la licencia de Microsoft Office 2010 es de $ 219.00 dólares de los Estados Unidos de Norteamérica.

4.4.4. Capacitación de Uso:

El proceso de capacitación hacia los empleados debe contar con el apoyo de los diferentes jefes departamentales, de modo que sea programado en horas que afecten menos al normal desempeño de sus tareas cotidianas, debe ser ejecutado lo antes posible y su duración debe estar en un periodo de 10 horas; sin embargo se recomienda que dicho periodo de capacitación transcurra en horas fuera del horario de trabajo y sol a los empleados que tengan relación con algún equipo de cómputo. El contenido del programa de capacitación debe tratar sobre las siguientes áreas:

a) Definir claramente el trato y uso que se debe dar a los equipos entregados para realizar las actividades relacionadas con el giro del negocio. Esta actividad debe ejecutarse de manera inmediata, y posterior a esto, se la debe efectuar para cada empleado nuevo que ingrese a la empresa; además como manera de actualización, debe hacer una vez por año con los empleados que en ese momento presten sus servicios en la empresa American Deportes.

b) Se debe definir a los empleados que la informacion es confidencial y propiedad de la empresa “American Deportes”, bajo la pena de sanciones económicas o la remocion del cargo, dependiendo de la gravedad de la falta.

c) Se debe enseñar el uso del software antivirus para desinfectar tanto el computador como las memorias flash.

d) Fomentar el buen trato a los equipos, haciendo énfasis en que se tratan de herramientas que les facilitan el trabajo día a día.

e) También se debe dar a conocer el presente manual en sus partes pertinentes a cada empleado.

Este proceso debe ser aprobado por la gerencia general, además se debe tomar en consideración que se realizará en horas fuera del horario normal de trabajo, por lo que debe contar con un presupuesto:

CAPACITACION A EMPLEADOS QUE USAN EQUIPOS DE COMPUTO				
SALARIO MINIMO	SUALDO DIARIO	Valor x hora suplementaria	10 horas de capacitacion	Por 10 empleados
$ 270.00	$ 1.13	$ 1.69	33.75	$ 337.50

Tabla 2 .- Costo de la capacitación de uso a empleados

4.4.5 Capacitación de Copias Seguridad

Se debe fijar la frecuencia de la ejecución de los respaldos de información tanto de bases de datos como de otros documentos de la empresa en cd's o dvd's o cintas de respaldo y en el internet de la siguiente forma:

a) Se deben ejecutar a diario, rotando cada nueva semana.
b) Uno semanal.
c) Uno mensual y

d) Uno más al año

Sobre su almacenamiento:

a) Cada dispositivo de respaldo debe estar identificado con la fecha y qué tipo de respaldo y que información contiene.
b) Cada semana debe se entregado para su custodia a la persona responsable de la caja fuerte de la empresa.
c) El respaldo correspondiente a cada mes y a cada año debe ser almacenado en un lugar geográficamente distinto de la ubicación de la empresa.
d) En el caso de los respaldos que también se pueden subir al internet, éstos deben ser almacenados en cuentas diferentes (espacio gratis si fuere posible), es decir una cuenta para los dias, otra para las semanas, otra para los meses y otra para los años; las contraseñas las deben saber al menos dos personas más aparte del encargado de hacer las copias de seguridad por escrito y con las actualizaciones cuando éstas deban ser cambiadas.
e) Se debe dar a conocer cual es el método de recuperación de la informacion almacenada en los respaldos de seguridad en caso de algun tipo de inconveniente con los datos a todo el personal de TI que pudiera estar al momento en la empresa a través de un manual detallado para tal propósito.

4.5. Procedimientos para el mantenimiento preventivo:

Este procedimiento debe ser ejecutado mensualmente, en cada uno de los equipos pertenecientes a la red de computadores además debe ser coordinado con los jefes de los diferentes departamentos para que no entorpezca las actividades diarias de cada empleado; y debería comprender todos los componentes físicos electrónicos y mecánicos de los equipos de cómputo de la siguiente manera:

1.- Verificación del funcionamiento de los ventiladores de forma que estén en buenas condiciones de funcionamiento.

2.- Instruir a los empleados en la limpieza de cada una de las pantallas con el uso de los productos adecuados para éste propósito en relación al tipo de las mismas.

3.- Los usuarios de cada computador deben ser instruidos en cómo mantener sus teclados y ratones limpios.

4.- La verificación del funcionamiento de las impresoras debe abarcar tanto la acumulación de polvo y la acumulación de restos de papel y su limpieza.

5.- Para los reguladores de voltaje y los UPS se debe ejecutar limpieza profunda y verificación de funcionamiento con la ayuda del voltímetro y el amperímetro.

6.- En las Conexiones de la red eléctrica deben ser verificar de voltajes de salida con la ayuda de voltímetro de la siguiente manera:

a) Entre la fase y el neutro se debe medir 110 – 120 voltios de corriente alterna.

b) Entre la fase y la conexión a tierra se debe medir 110 – 120 voltios de corriente alterna.

c) Entre neutro y la conexión a tierra se debe medir menos de un voltio de corriente alterna.

En el aspecto del software se deben ejecutar las siguientes tareas:

1.- Ejecutar el software antivirus sobre cada equipo y sobre todas las memorias flash que se utilicen en la empresa.

2.- Ejecutar programas en busca de software malicioso para su eliminación.

3.- Ejecutar programas de escaneo de errores en el disco duro.

4.- Ejecutar programas de desfragmentación de discos duros.

Este procedimiento debe ser realizado por personal capacitado para el efecto ya sea perteneciente a la empresa o por alguna empresa contratada para éste propósito.

4.6. Presupuesto.- El presupuesto que necesario al no requerir la reposición de equipos de cómputo se fundamentará en la conveniencia de contratar personal para laborara en la empresa como encargado de TI o a su vez el contrato de mantenimiento anual con alguna empresa dedicada a esta tarea, cabe aclarar que este tipo de empresas trabajan bajo demanda y su valor mensual es de una salario mínimo es decir un valor anual de $ 3240.00 dólares de los Estados Unidos de Norteamérica, esto más los valores expuestos en cada sección nos dejaría el presupuesto general anual como sigue:

AREA	VALOR UNITARIO	CANTIDAD	UNIDADES	VALOR
CAPACITACIÓN	$ 33.75	10	EMPLEADOS	$ 337.50
ANTIVIRUS 5 LICENCIAS	$ 128.00	2	5 LICENCIAS	$ 256.00
PERSONAL CAPACITADO	$ 270.00	12	CONTRATADO	$ 3,240.00
WIN2008 SER.	$ 790.00	1	LICENCIA	$ 790.00
WIN 7 32 BITS	$ 162.00	7	LICENCIAS	$ 1,134.00
MICROSOFT OFFICE2010	$ 219.00	3	LICENCIAS	$ 657.00
	TOTAL :			$ 6,414.50

Tabla 3.- Tabla de presupuestos.

Si analizamos solo la eventualidad de la concreción de una sola amenaza de las amenazas analizadas como por ejemplo la pérdida anual por la concreción de una amenaza de originada en mantenimiento quedaría completamente cubierta.

CAPUTULO 5.

CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones

a) Al no tener una política de mantenimiento de los equipos de cómputo, la empresa “American Deportes” pone en riesgo su capacidad de procesamiento de información, ocasionando pérdidas económicas.

b) Por no tener ningún tipo de planificación en lo relacionado con la seguridad, se pone en riesgo la información estratégica de la empresa.

c) Al no tener ningún plan de capacitación de uso de equipos de computación no tienen la menor idea de cómo se los debe tratar y mantener para evitar daños.

d) Tampoco tienen ningún tipo de capacitación sobre el software relacionado con el giro del negocio, los empleados de la empresa no tienen claro, lo que se debe hacer y lo que no con los equipos en lo relacionado con su indiscriminado acceso a internet y del correo electrónico.

e) Los trabajadores y empleados de la Empresa “American deportes” no tienen ningún tipo conocimiento relacionado con las reglas de confidencialidad de la información.

f) Los jefes departamentales no están consientes de que sus actividades afectan directa o indirectamente a la seguridad e la información al permitir

que los empleados a su cargo tengan libre acceso a correos electrónicos personales y a las redes sociales.

5.2. Recomendaciones

a) La empresa “American Deportes” debería incluir en su presupuesto anual un rubro dedicado a la contratación de una persona o una empresa especializada en mantenimiento de equipos de cómputo y de la seguridad de la información, para que sea el ente encargado del área de TI.

b) Los equipos deben estar alejados de maquinarias y en ambientes libres de pelusas y polvo que sin embargo en este caso son propios del negocio.

c) Los usuarios de la empresa deben ser capacitados constantemente sobre el uso de los recursos que la empresa “American Deportes” pone en sus manos en lo relacionado con el uso apropiado y la confidencialidad de los datos.

d) A mediano plazo se debe establecer un plan dedicado a implementar las normas ISO/IEC 27001 para la seguridad y mantenimiento tanto de los equipos de cómputo como de la red y la información.

e) Se debe realizar evaluaciones y mejoras permanentes en todo el proceso de seguridad de la información, de modo que a largo plazo se trate de asegurar lo más que se pueda el trabajo sin interrupciones generadas en el área de TI en la empresa “American Deportes”.

f) Además la empresa debe asegurarse que el personal más importante, como son los jefes departamentales estén consientes de que sus actividades tienen que contribuir a la seguridad de la información.

g) La elaboración de un plan estratégico empresarial integral lo más pronto posible sería de mucha utilidad como un factor de apoyo al crecimiento de la empresa.

h) Se debe recomendar a la empresa el uso masivo de software libre, lo que permitiría bajar los costos de las licencias de software en una buena medida.

Bibliografía:

- http://www.gms.com.ec/web2_/index.php?option=com_content&view=article&id=84:gms-y-kaspersky-lab-presentaron-el-estudio-delitos-ciberneticos-en-el-ecuador-en-la-puce
- Norma ISO/IEC 13335-1:2004.
- CISSP “Certified Information Systems Security Profesional”.
- *“Las técnicas de investigación: la observación”.* Prof. María Soledad Fabbri ,Argentina.
- *“Evolución Científica y Metodológica de la Economía.”* Roberto Gómez López, Universidad de Málaga, España.
- http://inf-tek.blogia.com/2009/060207-8.5-manual-de-politicas-de-seguridad-informatica.php.
- Norma ISO/IEC 27001:2005 (E).

Anexos:

Anexo 1.- Cuadro de resumen de Ventas del año 2011 con corte al 30/09/2011

26.10.11 AMERICAN DEPORTES COMERCIALIZACION Pag: 1

Resumen de Ventas por Fecha

Desde : 1.01.2011 Hasta : 30.09.2011

		Total Factura	Total Abono
Mes : 1	de 2011	14,368.92	2,062.10
Mes : 2	de 2011	17,413.61	2,582.00
Mes : 3	de 2011	17,292.83	1,583.00
Mes : 4	de 2011	15,870.89	2,125.10
Mes : 5	de 2011	14,876.76	1,352.60
Mes : 6	de 2011	13,424.34	825.00
Mes : 7	de 2011	11,839.26	320.00
Mes : 8	de 2011	88,308.15	264.01
Mes : 9	de 2011	64,814.35	.00
Total		258,209.10	11,113.82

Anexo 2.- Cuadro de resumen de Ventas del año 2010 con corte al 31/12/2010.

26.10.11 AMERICAN DEPORTES COMERCIALIZACION Pag.: 1

Resumen de Ventas por Fecha

Desde : 1.01.2010 Hasta : 31.12.2010

	Total Factura	Total Abono
Mes : 1 de 2010	12,480.35	0.00
Mes : 2 de 2010	16,965.70	0.00
Mes : 3 de 2010	11,257.95	0.00
Mes : 4 de 2010	15,430.51	0.00
Mes : 5 de 2010	15,399.00	0.00
Mes : 6 de 2010	6,072.78	9.00
Mes : 7 de 2010	15,094.94	55.00
Mes : 8 de 2010	63,802.00	60.00
Mes : 9 de 2010	53,476.34	0.00
Mes : 10 de 2010	13,398.82	0.00
Mes : 11 de 2010	13,379.39	0.00
Mes : 12 de 2010	31,488.31	410.00
Total	268,246.10	534.00

Anexo 3.- Tasa de Ocurrencia Anual (ARO) según CISSP Security Training – Information Security and Risk Management.

Valores ARO	Frecuencia de Ocurrencia
0.01	Una vez cada 100 años (1/100)
0.02	Una vez cada 50 años (1/50)
0.2	Una vez cada 5 años (1/5)
0.5	Una vez cada 2 años (1/2)
1	Una vez al año
10	10 veces al año
20	20 veces al año