DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR COMERCIAL

AUTORES:

María Gabriela Hernández Pinto[1], Bertha Alice Naranjo Sánchez[2].

- [1]Auditor en Control de Gestión 2006; email: marigabyher@hotmail.com.
- [2]Directora de Tesis, Ingeniera en Computación, Escuela Superior Politécnica del Litoral, 1994, Postgrado Ecuador, Escuela de Postgrado de Administración de Empresas ESPAE, 1997. Profesora de la ESPOL desde 1997, email: anaranjo2408@ubbi.com.

RESUMEN

El presente trabajo ayudará a las organizaciones comerciales a tener una concienciación permanente de mantener segura su información de amenazas que pueden causar la quiebra de una empresa, mediante el diseño de un plan estratégico de seguridad de información que contribuya a disminuir los riesgos a los que está expuesta la información.

En el primer capítulo se da a conocer la importancia, valor y vulnerabilidades de la información para formarnos un criterio del por qué es necesario mantenerla segura de todo incidente de seguridad. En el segundo capítulo se desarrollará el marco teórico del plan estratégico de seguridad de información destacando los pasos a seguir para su elaboración. En el tercer capítulo se realiza una breve descripción de las normas y estándares internacionales aplicables para el desarrollo de este tema. En el cuarto capítulo se lleva a la práctica el objetivo de este proyecto mediante una evaluación de la seguridad en una empresa comercial de nuestro medio. Finalmente en la quinta y última parte se dan a conocer las conclusiones y recomendaciones de las inseguridades encontradas durante la realización de este proyecto.

ABSTRACT

The present work will help the commercial organizations to have a permanent awareness to maintain sure its information of threats that can cause the bankruptcy of a company, by means of the design of a strategic plan of information security safe that contributes to diminish the risks to which this exposed the information.

In the first chapter is given to know the importance, value and vulnerabilities of the information to form us a criterion of why is it necessary to keep it sure of any incident of security. In the second chapter it will be developed the theoretical aspect of the plan strategic of security emphasizing the steps to follow for its elaboration. In the third chapter there is a brief description of the international norms and standards applicable for the development of this topic. In the fourth chapter is taken to the practice the objective of this project by means of an evaluation of the security in a commercial company of our means. Finally in the fifth and last chapter is given to know the conclusions and recommendations of the insecurities found during the accomplishment of this project.

INTRODUCCIÓN

Actualmente la tecnología informática es fundamental para la superación y desarrollo de un país. La información que en ella se maneja es considerada un activo cada vez más valioso, la cual puede hacer que una organización triunfe o quiebre; es por eso que debemos mantenerla segura.

La mayoría de las empresas desconocen la magnitud del problema con el que se enfrentan, considerando la seguridad informática como algo secundario y prestando poca atención a los riesgos que en la actualidad existen, como lo son: las amenazas internas, una de ellas los errores humanos y las amenazas externas dentro de las cuales podemos nombrar a los virus. Esta falta de inversión tanto en capital humano como económico muy necesario para prevenir principalmente el daño o pérdida de la información produce que la información no sea confiable ni integra y mucho menos disponible para la empresa originando así en muchos de los casos la paralización de sus actividades dejando como resultado una pérdida cuantiosa de tiempo de producción y dinero factores importantes para el desarrollo de una organización.

Para contrarrestar estos efectos de la falta de seguridad informática se presenta este trabajo que consiste en diseñar un plan estratégico de seguridad de información, que deberá seguir la organización en un corto, mediano y largo plazo.

Este plan se complementa con evaluaciones de seguridad y un pertinente análisis de riesgos que me permitió diseñar políticas de seguridad informática como un alcance concreto del plan estratégico de seguridad informática

Importancia de la Seguridad de Información

La información es la sangre de todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablamos de empresas altamente automatizadas por lo que su seguridad sigue siendo un punto pendiente y por tanto el factor más determinante por el cual fracasan.

Es muy importante ser conscientes de que por más que nuestra empresa a nuestro criterio sea la más segura, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas. Es por eso que en el ambiente competitivo de hoy, es necesario que las entidades aseguren la confidencialidad, integridad y disponibilidad de la información vital corporativa.

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

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

Por consiguiente en este nuevo entorno, es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio por una falla de seguridad, sino también que se preparen en establecer medidas que permitan reducir los problemas de seguridad que pueden surgir.

Presentación del Problema

Este trabajo busca implantar un modelo de seguridad orientado al cumplimiento de normas, procedimientos y estándares informáticos con el objetivo de crear una cultura de seguridad en la organización, mejorando las seguridades existentes requeridas para la salvaguarda de la integridad de los recursos informáticos.

CONTENIDO

Para el desarrollo de esta investigación es fundamental conocer ciertos términos que serán usados para su desarrollo.

Definiciones:

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

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.

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

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

Seguridad 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.

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.

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.

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

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

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

PASOS PARA LA ELABORACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA

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

1 Evaluación de los riesgos

Con la evaluación de los riesgos podremos identificar las causas de los riesgos potenciales a los que está expuesta la organización y cuantificarlos para que la gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos, en los diferentes puntos de análisis.

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

1. Identificar los riesgos
2. Determinación de los controles existentes
3. Análisis de los riesgos

1.1 Identificar los riesgos

En este paso se identifican los factores que introducen una amenaza para la organización. Existen muchas formas para identificar los riesgos pero para este análisis utilizaremos los cuestionarios elaborados para cada fin como son evaluar la seguridad física, lógica, redes y recursos humanos; los mismos serán respondidos por los miembros del área de sistemas y recursos humanos.

Una vez identificados los factores de riesgo, con la ayuda de los integrantes de las área antes mencionadas se procede a la ponderación de los mismos dando a cada uno de ellos su valor de importancia y determinando así los de mayor relevancia.

1.2 Determinación de los controles existentes

Después de identificar las causas de los riesgos que afectan a la organización, se determinará que riesgos el área de sistemas tiene bajo control y cuales no, para así determinar las medidas a tomar sobre estos.

1.3 Análisis de riesgos

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

1.3.1 Valoración del riesgos

Estando ya identificados los riesgos, debemos proceder a valorarlos mediante una escala como la que se presenta a continuación.

- <u>Riesgo alto</u>: Son todas las exposiciones a pérdida en las cuales la magnitud alcanza la bancarrota.
- <u>Riesgo medio</u>: Serán exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.
- <u>Riesgo bajo</u>: Exposiciones a pérdidas que no causan un gran impacto financiero.

1.3.2 Crear la matriz de riesgos

Una vez que le hemos dado un criterio de importancia a cada factor de riesgo procedemos a confrontarlos con los activos informáticos mediante la elaboración de una matriz, en la cual valoramos cada activo de acuerdo a cada factor de riesgo siguiendo la escala de riesgo Alto, Medio y Bajo; para finalizar y obtener un peso o riesgo evaluado de un recurso procedemos a realizar la siguiente operación: por cada activo realizamos una sumatoria de cada uno de los resultados obtenidos de multiplicar la valoración del activo con respecto a cada factor de riesgo por la ponderación de cada factor de riesgo. Y así determinaremos según el mayor valor cuál es el más vulnerable y a raíz de estos resultados podremos determinar que frecuencia de revisión deberá tener.

2 Políticas de seguridad

Las políticas de seguridad informática serán fijadas mediante mecanismos y procedimientos que deberá adoptar la empresa para salvaguardar sus sistemas y la información que estos contienen.

Deberán ser elaboradas a medida para así recoger las características propias de la organización.

Las políticas en su contenido incluirán:

- <u>Justificación</u>.
- <u>Generalidades</u>, dentro de este punto se incluirá: objetivo, alcance, responsabilidad, medidas a tomar en caso de incumplimiento de la política.
- <u>Estructura de la política</u>.- Seguridad física, seguridad lógica, seguridad en redes y seguridad en los recursos humanos.

Para diseñar la política nos basamos en las normas y estándares de seguridad informática como son COBIT e ISO 17799.

3 Plan de seguridad informática

Este plan será elaborado por la organización basándose en las políticas que se crearon a raíz del análisis de riesgo que han sido fundamentadas en las normas y/o estándares de seguridad ya mencionados.

Este plan debe ser realizado tomando en cuenta las actividades que podrá llevar a cabo la organización en un corto, mediano y largo plazo para concientizar a los recursos humanos e implantar medidas en cuanto a seguridad.

<u>CONCLUSIONES</u>

1. Las herramientas de tecnología son inseguras en la medida que su utilización no sea la más adecuada en la organización, convirtiéndose así en objeto de amenazas.

2. Hoy en día en toda empresa existe una necesidad más frecuente de utilizar esquemas de seguridad fuertes, que permitan una mayor confiabilidad de la información utilizada para la toma de decisiones.

3. La incomprensión de la Gerencia que conlleva a la falta de apoyo económico a la gestión de informática para implantar medidas de seguridad, provoca que la entidad tenga una mayor exposición a los riesgos.

4. La seguridad de la información es una responsabilidad compartida de todos los niveles de la organización, que requiere del apoyo de todos ellos pero debe estar dirigida por un plan y debe contar con una adecuada coordinación.

5. El avance de la tecnología y del conocimiento de los seres humanos ya sean usadas con buena o mala intención, vuelven más vulnerable a la información exponiéndola a diversas amenazas tanto internas como externas y volviéndola poco confiable.

6. Con este trabajo se desea fomentar una cultura de seguridad en todos aquellos que lo consulten y deseen ponerlo en práctica.

REFERENCIAS

1. M. Hernández, "Diseño de un plan estratégico de seguridad de información en una empresa del sector comercial" (Tesis, Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral, 2006).

2. Echenique García José Antonio, Auditoria en Informática (2da Edición, Mc. Graw Hill, 2001), pp. 194-241.

3. Laudon Kenneth C. y Laudon Jane P, Administración de los Sistemas de Información, Organización y Tecnología (3ra Edición, México, Prentice Hall Hispanoamericana S.A., 1994), pp. 702-706.

4. Lucena López Manuel José, Criptografía y Seguridad en Computadoras (2da Edición, Universidad de Jaen, 1999), pp. 30-138.

5. Norton Peter, Introducción a la Computación (1ra Edición, México, Mc Graw Hill), pp. 50-53.

6. Simson Garfinkel y Spafford Gene, Seguridad y Comercio en el Web (México, Mc. Graw Hill, 1999), pp. 8-13.

7. Simson Gar Finkel, y Spafford Gene, Seguridad Práctica en UNIX e Internet (2da Edición, Mc. Graw Hill, 1999), pp.360-366.