Seguridad y administración de riesgo en el centro de tecnologías de información

Wilberth Molina Pérez [1]

Resumen

Se presenta un marco general de lo que es la seguridad en un centro de tecnología de información (TI), a quiénes afecta la seguridad y por qué es conveniente asegurar las TI actualmente.

Se analizan los aspectos por asegurar tales como l disponibilidad, la integridad y la confidencialidad de la información. Adicionalmente, se indican los factores que se van a considerar al realizar un análisis de riesgo los cuales serían la validez de los recursos que se deben asegurar, la probabilidad de una amenaza, la sensibilidad de la información y el costo de asegurar dicha información.

Finalmente, se comenta una metodología de análisis de riesgo y la experiencia de aplicarla.

Descriptores

Seguridad de la información / riesgo / tecnologías de información

Abstract

A general mark is presented of what refers the security in the Center of Information Technology (IT) to who it affects the security and reason is convenient to assure IT at the moment.

The aspects are analyzed to assure as they are it the readiness, the integrity and the confidentiality of the information. Additionally, the factors are indicated to consider when carrying out an analysis of risk like they are the validity of the resources that you/they should make sure, the probability of a threat, the sensibility of the information and the cost of assuring this information.

Finally it is commented a methodology of analysis of risk and the experience of applying it.

[1] Licenciado en Ingeniería Informática. Decano de la Facultad de Ingeniería de ULACIT. Correo Electrónico: wmolina@ulacit.ac.cr

Key Words

Information security / risk / information technologies

I. Introducción

La seguridad en laTI está dirigida, entre otros aspectos, a evitar amenazas como: ingreso de virus, copia de archivos clasificados, copia de software, utilización de recursos no autorizados, substracción o destrucción de equipo, publicación de información clasificada, entre muchos otros.

Últimamente se han desarrollado estrategias para minimizar el problema de los "hackers", estos expertos en informática (o por lo menos que pueden utilizar programas especializados) que ejecutan actos temerarios, más que vandálicos, como pueden ser modificar la información de una página en Internet, ingresar a un centro de cómputo y modificar algunos programas del sistema, o recuperar y difundir información sobre cuentas de acceso a Internet.

Pero también existe el peligro del sujeto interno, el que normalmente no se ha analizado. Hagamos las siguientes preguntas: ¿cuántas horas laborales utilizan los empleados en sus proyectos universitarios, dentro de la empresa?, ¿cuántos discos son utilizados por los empleados en el trasiego de sus documentos personales?, ¿cuánto papel, tinta, cintasy fotocopias se utiliza en labores que no son de las empresas?, ¿cuántas reuniones de compañeros de universidad se realizan en la empresa? Amigos de los empleados pueden resultar excelentes "hackers".

En la mayoría de los casos se adopta una filosofía de sustentar la seguridad interna en el desconocimiento que tienen los empleados, lo cual evidentemente es una mala práctica, pues el daño que un usuario novato puede causar en un sistema susceptible puede ser muy grande en la mayoría de los casos, sin la intención de realizarlo.

Como se puede notar, en las anteriores líneas hay muchos elementos que revelan la importancia de asegurar los recursos tanto de externos como de internos.

II. Alcance

Actualmente, la tecnología está omnipresente en casi todas las actividades. Las computadoras son las responsables de darnos energía eléctrica, comunicación telefónica, dinero efectivo (cajeros), crédito (tarjetas), y de mantener registros médicos, legales y financieros, entre otros.

Toda persona que tiene una tarjeta de crédito o utiliza un cajero automático puede estar

segura de que en algún lugar se almacena información personal, y si se quiere privada, y que existe la amenaza de que personas sin escrúpulos utilicen "maliciosamente" esta información.

Lo anterior nos permite darnos cuenta de que, efectivamente, las personas pueden verse comprometidas si ocurriera un evento que burle la seguridad de alguna empresa.

III. ¿Por qué ahora?

Siempre se han tenido amenazas; la preocupación de hoy se da en la medida en que tenemos un sustancial aumento en las posibilidades y facilidades que tienen terceros de realizar con éxito un ataque.

Las computadoras personales anteriormente se utilizaban solo en las empresas, ahora han llegado a los hogares y son ampliamente utilizadas; desde sus casas las personas tienen acceso a los servicios de Internet como World Wide Web (WWW), correo, grupos de noticias, chat, etc.

Con la introducción del "comercio electrónico" los usuarios pueden utilizar servicios de compras en línea e inclusive realizar transacciones bancarias. Este fenómeno ha creado un incremento en la disponibilidad y cantidad de la información que se trasmite, y en las posibilidades de utilizarla en forma mal intencionada.

La tendencia del ser humano es seguir utilizando tecnología, ya que cada vez es más barata y el mundo se va automatizando con una rapidez vertiginosa, un evento que comprometa la prestación de servicios o bien la fuga de información clasificada podría redundar en un desastre con ramificaciones financieras, legales y de imagen. No obstante, si las personas se acostumbran a utilizar los servicios tecnológicos y se les eliminan, provocaría en la mayoría de los casos, una paralización casi total.

Muchos foros tratan temas de seguridad en los que se presentan casos y posibles soluciones; a estos foros ingresan todo tipo de personas, desde las que buscan información o una solución a sus problemas hasta las que utilizan la información como herramienta en sus futuros intentos de violar la seguridad de las empresas.

IV. Aspectos de aseguramiento

La seguridad de un TI debe tratarse en forma integral por medio de tres aspectos fundamentales con respecto a la información: disponibilidad, integridad y confidencialidad.

4.1 Disponibilidad

La disponibilidad se refiere a la facilidad de utilizar un recurso en el momento en que se requiere, ya sea este información o equipo; el hecho de no poder utilizar un recurso se conoce como “denegación de servicio”. No solo se da denegación de servicio al no poder acceder a cierta información; si no se puede utilizar una computadora también se tiene este efecto.

Los ataques de denegación de servicio son comunes; tratar de ingresar con la clave del gerente por más de tres intentos podría inhabilitar la cuenta del gerente, llenar de procesos innecesarios el servidor y provocar un servicio más lento, agotar la capacidad del disco del servidor, o saturar el buzón de correo, por ejemplo.

Implementar mecanismos de aseguramiento físico de la red y de la computadora son formas de cubrir la disponibilidad. Limitar el acceso físico a los equipos principales permite de alguna manera reducir el riesgo de denegación de servicio, restringir el acceso lógico es el complemento para lograr un aseguramiento más efectivo.

En lugares donde se tiene contacto con redes inseguras (como Internet) se pueden implementar un “FireWall” que asegure la confiabilidad de los accesos y por ende reduzca la amenaza de ataques. Existen muchas variantes para la creación de un “FireWall”, pero se debe indicar que este consiste en una serie de equipos, programas y reglas las que hacen el “FireWall” que conforman un ente integrado en busca de proteger la red interna del mundo exterior.

Otro mecanismo que garantiza la disponibilidad es conservar un adecuado plan de contingencia que permita de alguna manera el seguir prestando los servicios bajo situaciones adversas Mantener respaldos actualizados, redundancia de información, equipos de respaldo y centros de operación alternativos son algunas de las técnicas que se pueden implementar para estos efectos.

4.2 Integridad

La integridad se refiere al hecho de que la información no pueda ser alterada arbitrariamente, y que se guarde en estado seguro y equilibrado.

Acceder a información que ha sido modificada sin respetar la integridad, lleva a la pérdida de confianza en la empresa que la brinda y, evidentemente, en la información misma.

Existen técnicas y herramientas que facilitan el estudio y mantenimiento de la integridad; un diseño de base

de datos con reglas de integridad referencial bien definidas y procesos de chequeo en las formas y procesos en lote que validan la información son rutinas efectivas.

Finalmente, si la información que se administra es crítica, se deben instalar procedimientos que aseguren que esta no sea modificada por otros medios que los establecidos de previo. El término "encriptar" se refiere al proceso de guardar información que se considera confidencial para prevenir que otros individuos no autorizados puedan modificarla sin ser detectados.

4.3 Confidencialidad

La confidencialidad puede ser definida como el acto de mantener las cosas escondidas o en secreto, esta es una consideración necesaria para muchos tipos de datos importantes.

Existen situaciones en las que la información se torna vulnerable, por ejemplo:

- Cuando la información se almacena en una computadora.
- Cuando la información es transmitida a otra computadora por la red.
- Cuando la información se mantiene respaldada.

La confidencialidad se da cuando la información que existe puede ser vista solo por las personas que tienen los permisos correspondientes para ello.

Se deben implementar controles estrictos para asegurar este punto; los usuarios deberían ver solamente la información que les permita realizar sus labores. El término "control de acceso" es el hecho de permitir el acceso a la información o recurso solo a quienes se desea.

La práctica más común de control de acceso es la utilización de contraseñas, y la forma más común de quebrar la seguridad de un sitio es la utilización de estas contraseñas, porque los usuarios realmente no les prestan la suficiente importancia, utilizan claves fáciles, las escriben o bien simplemente las divulgan.

Los centros de TI deben enfocarse en mejorar los sistemas que permiten contraseñas y validar ciertos criterios como tamaño, combinación y no utilizar palabras comunes.

V. Métodos para minimizar el riesgo

En el proceso normal de las empresas se debe realizar una serie de acciones para

establecer y mantener los sistemas bajo control y seguros. Básicamente, esto se debe realizar en el desarrollo de los sistemas por medio del control de operaciones y seguridad, y anticipándose a los problemas. Las siguientes son algunas de las acciones que se deben ejecutar:

- Construir los sistemas correctamente en primer término.
- Entrenar a los usuarios sobre aspectos de seguridad.
- Una vez que el sistema esta en operación, mantener la seguridad física.
- Prevenir accesos no autorizados a los equipos, la red y los datos.
- Asegurarse de que las transacciones se realicen correctamente.
- Motivar la eficiencia y efectividad buscando vías de mejorarla.
- Auditar los sistemas para buscar posibles problemas.
- Continuar la vigilancia y prepararse para desastres.

VI. Factores por considerar

El nivel de seguridad o inseguridad es determinado por las políticas de la empresa y, en muchas ocasiones, estas no son claras. Por esta razón, se debe tener cuidado de evaluar y comprender la relevancia y validez de los componentes que se desean asegurar.

Definir una política de aseguramiento significa desarrollar procedimientos e implementar salvaguardas para los recursos, contra pérdidas y daños. Un método para desarrollar una política es realizar las siguientes preguntas: ¿Cuáles recursos se están tratando de proteger?, ¿de quiénes se necesita proteger los recursos?, ¿cómo deberían tratarse?, ¿qué tan importantes son los recursos?, ¿cuáles medidas se pueden implementar para protegerlos en forma rápida y efectiva?, ¿se examinan periódicamente los objetivos ante cambios en el entorno?

Una forma razonable de considerar los recursos por proteger es tener presente el valor relativo y la importancia que tienen para el buen desempeño de la empresa.

Para medir lo anterior se deben considerar los siguientes factores:

6.1 Validez

Se tiene el problema del posible sesgo que tendrán las mediciones que se realicen, pues algunas de estas son subjetivas, y desde ese momento se introduce un nivel de incertidumbre que debe ser minimizado por otros medios.

6.2 Probabilidad

En el momento de establecer las amenazas y los mecanismos que minimizan el posible impacto de estas, se debe considerar la probabilidad de que este hecho se dé, y con base en esta estimación se deberán implementar los procesos acordes a este resultado.

6.3 “Sensibilidad”

La “sensibilidad” de los datos que se desean proteger determinará el nivel de aseguramiento necesario. El archivo que mantiene información acerca de los nombres de los empleados requiere relativamente menor seguridad que el que almacena la información de los préstamos de estos.

Se debe considerar si existen sistemas de seguridad para este tipo de información; en general, no se debe permitir que los usuarios almacenen información sensible en sistemas poco seguros.

En todo caso se debe seguir la regla de oro de control: “no puede ser mayor el control que se establece a un bien, que el valor de este”.

6.4 Costo

El costo no solo se debe medir en monedas; elementos como el tiempo que se tome para normalizar un recurso luego de un ataque debe ser contemplado, al igual que el tiempo de los empleados mientras se restaura la normalidad, el compromiso con los clientes y la reputación, todos ellos permitirán establecer el costo real del no aseguramiento de un recurso.

6.5 Análisis de costo-beneficio

El análisis de costos involucra tres elementos:

A. El costo de la pérdida: calcular este costo puede ser bastante difícil, por lo visto en el punto 6.4.

B. El costo de la prevención: se debe calcular el costo de implementar todas y cada una de las posibles salvaguardas por efectuar.

C. La probabilidad de la amenaza: quizá, de todos los elementos, este es el más difícil de determinar por lo indicado en 6.1 y 6.2

En general si se cumple que $B<(A*C)$, entonces se debe instalar la salvaguarda del recurso en cuestión.

VII. Una metodología de análisis de riesgo

7.1 Identificación de la empresa

Se debe contextualizar la empresa, conociendo sus objetivos, políticas, marco del negocio y expectativas.

7.2 Conformación de equipos de trabajo

Se crea a) un comité evaluador, b) equipos de áreas especializadas (físico, lógico, telecomunicaciones) y c) un líder del proyecto.

7.3 Identificación de recursos por proteger

Con la ayuda los usuarios, los equipos (B) se dedican a buscar los recursos que se desea proteger en las diferentes áreas.

7.4 Determinación de amenazas

Para los recursos identificados, en este proceso colaboran los usuarios con los equipos.

7.5 Evaluación por comité evaluador

Una vez identificadas las amenazas, el comité evaluador las ponderará e indicará las principales amenazas por corregir.

7.6 Valoración de salvaguardas

Para cada una de las amenazas encontradas se deberán buscar las posibles medidas para eliminar o minimizar su impacto.

7.7 Implementar las salvaguardas

Luego de determinar las salvaguardas por establecer, estas se deben instalar y "monitorear", con el objetivo de conocer si efectúan la labor para la que fueron implementadas.

7.8 Valorar el riesgo residual

Una vez instaladas todas las salvaguardas convenidas, se debe valorar el riesgo que se mantiene y tomar una decisión al respecto.

El ciclo se continúa iterando, ya que las amenazas a los recursos nunca se eliminan en un 100%.

VIII. La metodología en la práctica

La metodología expuesta en el punto anterior se implementó en una empresa, con el fin de evaluarla; y seguidamente se comentan los resultados de esta aplicación:

1. La identificación de la empresa permitió conocer la misión de esta, ubicarla en

contexto y poder tomar en cuenta esta información para los alcances de las amenazas y las salvaguardas. Cabe destacar que se requirieron esfuerzos adicionales pues se debieron comprender las políticas y objetivos, lo que llevó a un análisis de la contemporaneidad de estas por parte de la administración.

2. La integración de los equipos de trabajo fue simple, en vista de que en el personal existe un ambiente de colaboración en los proyectos de investigación, debido a que en anteriores oportunidades estos se han realizado con buen suceso y han permitido crear nuevos servicios. Lo anterior no necesariamente es así en otras empresas.

3. La utilización del recurso humano de los usuarios fue efectivamente un arma de doble filo, pues por un lado para los usuarios el mundo delimitado por los procesos que ellos realizan y los recursos a los que tienen acceso son los más importantes de la empresa, y por otro, nos encontramos con una lista exhaustiva de los recursos de la empresa (importantes o no) generada al unir la información de los usuarios. Esto permitió conocer toda la gama de recursos que posee la empresa.

4. En la determinación de las amenazas, la participación de los usuarios fue relativamente pobre por no estar habituados a este tipo de labores y, en parte, al desconocimiento de lo que puede ser una amenaza.

La labor de los equipos especializados fue efectivamente amplia, y los especialistas de TI tuvieron que reforzar la labor de análisis.

5. La evaluación de las amenazas por parte del comité evaluador muestra fallas de esta metodología, pues se introducen evaluaciones subjetivas que llevan consigo un sesgo difícil de evaluar, y permiten una incertidumbre que en algunos casos podría ser perjudicial. En nuestro caso, el descartar la amenaza de robo, la facilidad de acceso físico y remoto al TI, rechazados de previo, dejan claro los efectos antes mencionados.

6. La valoración de las salvaguardas tiene la evaluación de la función discutida en el punto 6.5 que tiene elementos cualitativos, y por ello causa los mismos efectos del ítem anterior. En nuestro caso, se trató de justificar, llevando todos los elementos a valores reales, y hubo cierta satisfacción en este proceso, pero siempre quedó un sentimiento de inseguridad con respecto a si todo estará bien valorado y calculado.

7. En relación con la implementación de las salvaguardas, hubo bastante

aceptación de los usuarios, considerando que el haberles tomado en cuenta dentro de proceso fue una decisión atinada, dado que ellos se sienten parte del proceso y ven que se toman en cuenta algunos de sus aportes.

8. En nuestro caso, la valoración del riesgo residual fue la revalorización de las amenazas anteriores y las nuevas generadas por las diferentes implementaciones. Se pudo determinar que al instalar las salvaguardas, las amenazas desaparecieron o se minimizaron algunas de las que no se trataron en esta primera iteración.

IX. Conclusiones

Dado el crecimiento que tienen las empresas, la filosofía de servicio y la apertura moderna, las empresas deben asegurar los recursos, pues cada vez están más expuestas al mundo y ello provoca que traten de "atacarlas" o intenten investigar sobre estas desde la información contenida en ellas.

El control de acceso, las contraseñas, los respaldos y la redundancia son componentes candidatos a ser utilizados en las políticas de aseguramiento.

La educación tecnológica, el adiestramiento de los usuarios en temas de seguridad y la implementación de políticas de contraseñas fuertes permitirá mejorar este sistema.

Con el panorama de un mundo tecnológicamente en gran desarrollo y con las facilidades que se brindan actualmente, se puede asegurar que todos aquellos que posean una computadora o utilicen algún servicio son blancos potenciales para los ataques y, por lo tanto, se deben tomar las medidas del caso para minimizar el posible impacto.

X. Referencias bibliográficas

Hernández, R. (2003). *Administración de la Función Informática: Una Nueva Profesión*. México: Limusa.

McConnell, S. (2004). *Code Complete*. Seattle: Microsoft Press.

Sommerville, I. (2002). *Ingeniería de Software*. México: Pearson.