Unidad I

Fundamentos de la Seguridad Informática

Introducción

Muchas empresas son amenazadas constantemente en sus activos lo que pudiera representar miles o millones de dólares en pérdidas. Las vulnerabilidades en nuestros sistemas de información pueden representar problemas graves, por ello es muy importante comprender los conceptos necesarios para combatirlos y defendernos de posibles ataques a nuestra información.

Objetivos

- Con la finalidad de proteger todos los activos vitales para la empresa.
- Conocer las diferentes categorías existentes de los activos de una empresa.
- Comprender el concepto de puntos débiles para identificar las posibles vulnerabilidades y amenazas existentes en los activos.
- Interpretar la clasificación propuesta de las posibles amenazas encontradas en los diferentes procesos de la empresa.
- Revisar los conceptos de integridad, confidencialidad y disponibilidad de la información.
- Conocer el concepto de riesgo y su implicación en el ciclo de seguridad de la informática de la empresa.
- Distinguir la diferencia entre aplicar o no medidas de seguridad en los diferentes aspectos de la empresa.

- Comprender los conceptos básicos de análisis de riesgo y política de seguridad los puntos muy importantes para definir las acciones en materia de seguridad que se aplican en las empresas.

En la actualidad la información es el objeto de mayor valor para las empresas. El progreso de la informática y de las redes de comunicación nos presenta un nuevo escenario, donde los objetos del mundo real están representados por bits y bytes, que ocupan lugar en otra dimensión y poseen formas diferentes de las originales, no dejando de tener el mismo valor que sus objetos reales, y, en muchos casos, llegando a tener un valor superior.
Por esto y otros motivos, la seguridad informática es un asunto tan importante, pues afecta directamente a los negocios de una empresa o de un individuo .

Así, para empezar, es necesario identificar los elementos que laseguridad de la información busca proteger:

- La información
- Los equipos que la soportan
- Las personas que la utilizan

Es importante, además, que todos los empleados de la compañía tomen conciencia sobre el manejo de la información de forma segura, ya que de nada sirve cualquier sistema de seguridad por complejo y completo que este sea, si los empleados, por ejemplo, facilitan su usuario y contraseña a personas ajenas a la empresa y con esto dejar abierta la puerta a posibles ataques o filtraciones de información crítica al exterior de la compañía.

Un Activo:

Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, su emisor, el medio por el cual se transmite, hasta

su receptor. Los activos son elementos que la seguridad de la información busca proteger. Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados.

Son tres elementos que conforman lo que denominamos activos: la información, los Equipos que la soportan y, las personas que los utilizan.

1. La Información:

En este grupo están los elementos que contienen información registrada, en medio electrónico o físico, dentro de los más importantes tenemos:

Cualquier tipo de información, sin importar en qué tipo de medio se tenga almacenada, que sea de importancia para la empresa y sus negocios.

Ejemplos de este tipo de activos: documentos, informes, libros, anuales, correspondencias, patentes, información de mercado, código de programación, líneas de comando, archivos de configuración, planillas de sueldos de empleados, plan de negocios de una empresa, etc.

Posibles vulnerabilidades Robo de documentos, pérdida de archivos de configuración, entre otros.

2. Los Equipos Que La Soportan

El Software:

Este grupo de activos contiene todos los programas de computadora que se utilizan para la automatización de procesos, es decir, acceso, lectura, tránsito y almacenamiento de la información. Entre ellos citamos: las aplicaciones comerciales, programas institucionales, sistemas operativos, otros.

La seguridad informática busca evaluar la forma en que se crean las aplicaciones, cómo están colocadas a disposición y la forma como son utilizadas por los usuarios y por otros sistemas, para detectar y corregir problemas existentes en la comunicación entre ellos.

Las aplicaciones deberán estar seguras para que la comunicación entre las bases de datos, otras aplicaciones y los usuarios se realice de forma segura, atendiendo a los principios básicos de la seguridad de la información. Los Sistemas operativos (Unix, Windows, Linux, sistemas informatizados, aplicaciones específicas etc.), programas de correo electrónico, sistemas de respaldo entre otros.

Posibles vulnerabilidades Fallas publicadas no reparadas que puedan representar accesos indebidos a los equipos. Pérdida de los sistemas de respaldo.

El Hardware:

Estos activos representan toda la infraestructura tecnológica que brinda soporte a la información durante su uso, tránsito y almacenamiento.

Los activos que pertenecen a este grupo son: Cualquier equipo en el cual se almacene, procese o transmita la información de la empresa. Ejemplos de este tipo de activos: las computadoras, los servidores, los equipos portátiles, los *mainframes* los medios de almacenamiento los equipos de conectividad, enrutadores, *switchs* y cualquier otro elemento de una red de computadoras por donde transita la información.

Posibles vulnerabilidades Fallas eléctricas que dañen los equipos, inundaciones en centros de cómputo, robo de equipos portátiles.

La Organización:

En este grupo se incluyen los aspectos que componen la estructura física y organizativa de las empresas Se refiere a la organización lógica y física que tiene el personal dentro de la empresa en cuestión. Ejemplos de este tipo de activos.

Como ejemplos de estructura organizativa, tenemos entre otros:

- la estructura departamental y funcional
- el cuadro de asignación de funcionarios
- la distribución de funciones y los flujos de información de la empresa

En lo que se refiere al ambiente físico, se consideran entre otros: salas y armarios donde están localizados los documentos, fototeca, sala de servidores de archivos.

Posibles vulnerabilidades Ubicación insegura de documentos, equipos o personas. Estructura organizacional que no permita los cambios en materia de seguridad.

3. Las Personas Que La Utilizan

Usuarios:

El grupo usuarios se refiere a los individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información.

El enfoque de la seguridad en los usuarios, está orientado hacia la toma de conciencia de formación del hábito de la seguridad para la toma de decisiones y acción por parte de todos los empleados de una empresa, desde su alta dirección hasta los usuarios finales de la información, incluyendo los grupos que mantienen en funcionamiento la estructura tecnológica, como los técnicos, operadores y administradores de ambientes tecnológicos. Ejemplos de este tipo: Empleados del área de contabilidad. Directivos de la empresa.

Posibles vulnerabilidades Olvido de contraseñas. Falta de cooperación por parte de los usuarios en materia de seguridad. Descuido de parte de los usuarios en el manejo de la información.

Protección de Los Activos

Una vez que conocemos los diferentes tipos de activos que podemos encontrar en las empresas, ahora profundizaremos en los principios básicos que nos ayudarán a proteger el activo de más valor en los negocios modernos: la información.

Principios Básicos de la Seguridad Informática

Proteger los activos significa mantenerlos seguros contra amenazas que puedan afectar su funcionalidad: Corrompiéndola, accediéndola indebidamente, o incluso eliminándola o hurtándola.

Por lo tanto, entendemos que la seguridad informática tiene en vista proteger a estos activos de una empresa o individuo, con base en la preservación de tres principios básicos:

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

Enseguida encontrará información más detallada de cada uno de estos principios:

Principio de la Integridad de la Información

El primero de los tres principios de la seguridad de la información que aplicamos es la integridad, la cual nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra.

Una información íntegra es una información que no ha sido alterada de forma indebida o no autorizada. Para que la información se pueda utilizar, deberá estar íntegra. Cuando ocurre una alteración no autorizada de la información en un documento, quiere decir que el documento ha perdido su integridad.

La integridad de la información es fundamental para el éxito de la comunicación. El receptor deberá tener la seguridad de que la información obtenida, leída u oída es

exactamente la misma que fue colocada a su disposición para una debida finalidad. Estar íntegra quiere decir estar en su estado original, sin haber sido alterada por quien no tenga autorización para ello. Si una información sufre alteraciones en su versión original, entonces la misma pierde su integridad, ocasionando errores y fraudes y perjudicando la comunicación y la toma de decisiones.

La quiebra de integridad ocurre cuando la información se corrompe, falsifica o burla.

Una información se podrá alterar de varias formas, tanto su contenido como el ambiente que la soporta. Por lo tanto, la quiebra de la integridad de una información se podrá considerar bajo dos aspectos:

1**. Alteraciones del contenido de los documentos** – donde se realizan inserciones, sustituciones o remociones de partes de su contenido;

2. Alteraciones en los elementos que soportan la información – donde se realizan alteraciones en la estructura física y lógica donde una información está almacenada.

Buscar la integridad es asegurarnos que sólo las personas autorizadas puedan hacer alteraciones en la forma y contenido de una información, así como en el ambiente en el cual la misma es almacenada y por el cual transita, es decir, en todos los activos. Por lo tanto, para garantizar la integridad, es necesario que todos los elementos que componen la base de gestión de la información se mantengan en sus condiciones originales definidas por sus responsables y propietarios.

En resumen: garantizar la integridad es uno de los principales objetivos para la seguridad de las informaciones de un individuo o empresa.

Principio de la Confidencialidad de la Información

El principio de la confidencialidad de la información tiene como propósito el asegurar que sólo la persona correcta acceda a la información que queremos

distribuir. La información que se intercambian entre individuos y empresas no siempre deberá ser conocida por todo el mundo. Mucha de la información generada por las personas se destina a un grupo específico de individuos, y muchas veces a una única persona. Eso significa que estos datos deberán ser conocidos sólo por un grupo controlado de personas, definido por el responsable de la información.

Por ese motivo, se dice que la información posee un grado de confidencialidad que se deberá preservar para que personas sin autorización no la conozcan.

Tener confidencialidad en la comunicación, es la seguridad de que lo que se dijo a alguien o escribió en algún lugar será escuchado o leído sólo por quien tenga ese derecho.

Pérdida de confidencialidad significa pérdida de secreto. Si una información es confidencial, es secreta, se deberá guardar con seguridad y no ser divulgada para personas no autorizadas.

El acceso debe ser considerado con base en el grado de sigilo de las informaciones, pues no todas las informaciones sensibles de la empresa son confidenciales. Pero para garantizar lo anterior, sólo la confidencialidad de las

Informaciones no es suficiente, es importante que además de ser confidenciales, las informaciones también deben estar íntegras. Por lo tanto, se debe mantener la integridad de una información, según el principio básico de la seguridad de la información.

Como se acaba de mencionar, la forma de instrumentar la confidencialidad de la información es a través del establecimiento del grado de sigilo.

Grado de sigilo:

L a información generada por las personas tiene un fin específico y se destina a un individuo o grupo. Por lo tanto, la información necesita una clasificación en lo

que se refiere a su confidencialidad. Es lo que denominamos grado de sigilo, que es una graduación atribuida a cada tipo de información, con base en el grupo de usuarios que poseen permisos de acceso.

Dependiendo del tipo de información y del público para el cual se desea colocar a disposición los grados de sigilo podrán ser: Confidencial, Restricto, Sigiloso, Público

Principio de Disponibilidad de la Información:

Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad.

Para que una información se pueda utilizar, deberá estar disponible. La disponibilidad es el tercer principio básico de la seguridad informática.

Se refiera a la disponibilidad de la información y de toda la estructura física y Tecnológica que permite el acceso, tránsito y almacenamiento. La disponibilidad de la información permite que:

- Se utilice cuando sea necesario
- Que esté al alcance de sus usuarios y destinatarios
- Se pueda accederla en el momento en que necesitan utilizarla.

Este principio está asociado a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de los negocios de la empresa o de las personas, sin impactos negativos para la utilización de las informaciones. No basta estar disponible: la información deberá estar accesibles en forma segura para que se pueda usar en el momento en que se solicita y que se garantice su integridad y confidencialidad. Así, el ambiente tecnológico y los soportes de la información deberán estar funcionando correctamente y en forma segura para que

la información almacenada en los mismos y que transita por ellos pueda ser utilizada por sus usuarios.

Referencias Bibliográficas

Academia Latinoamericana de Seguridad Informática. Unidad I. *Introducción a la Seguridad Informática*. Curso En línea página principal se encuentra en: http://www.microsoft.com/latam/technet/video/alsi.aspx