INGENIERÍA DE SOFTWARE AVANZADA

(SESIÓN 7)

3.2 Análisis y gestión de riesgos

3.3 Seguridad y privacidad de la información

Objetivo: Conocer las principales estrategias para brindar con seguridad, privacidad a la información.

3.2 Análisis y gestión de riesgos

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras, el cual, aunque tiene diferentes intenciones, se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco. Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso

no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

Ejemplo: Existe una Aplicación de Seguridad que se llama SEOS, para Unix, que lo que hace es auditar el nivel de Seguridad en todos los servidores, como ser: accesos a archivos, accesos a directorios, que usuario lo hizo, si tenía o no tenía permiso, si no tenía permiso porque falló, entrada de usuarios a cada uno de los servidores, fecha y hora, accesos con password equivocada, cambios de password, etc. La Aplicación lo puede graficar, tirar en números, puede hacer reportes, etc.

La seguridad informática se la puede dividir como Área General y como Área Especifica (seguridad de Explotación, seguridad de las Aplicaciones, etc.). Así, se podrán efectuar auditorías de la Seguridad Global de una Instalación Informática –Seguridad General- y auditorías de la Seguridad de un área informática determinada – Seguridad
Especifica -.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la Seguridad Informática a nivel físico. Los accesos y conexiones indebidos a través de las Redes de Comunicaciones, han acelerado el desarrollo de productos de Seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:
•□Elementos administrativos
•□Definición de una política de seguridad
•□Organización y división de responsabilidades
•□Seguridad física y contra catástrofes (incendio, terremotos, etc.)
•□Prácticas de seguridad del personal
•□Elementos técnicos y procedimientos
•□Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
•□Aplicación de los sistemas de seguridad, incluyendo datos y

archivos

- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

La decisión de abordar una Auditoría Informática de Seguridad Global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida.

Se elaboran "matrices de riesgo", en donde se consideran los factores de las "Amenazas" a las que está sometida una instalación y los "Impactos" que aquellas puedan causar cuando se presentan. Las matrices de riesgo se representan en cuadros de doble entrada <<Amenaza-Impacto>>, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz. Ejemplo:

Ejemplo:

Impacto	Amenaza				1: Improbable 2: Probable 3: Certeza -: Despreciable
	Error	Incendio	Sabotaje	……..	
Destrucción de Hardware	-	1	1		
Borrado de Información	3	1	1		

El cuadro muestra que si por error codificamos un parámetro que ordene el borrado de un fichero, éste se borrará con certeza.

Se puede definir los riesgos de auditoría como aquellos riesgos de que la información pueda tener errores materiales o que el auditor de sistemas no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera: Riesgo inherente: Cuando un error material no se puede evitar que suceda por que no

existen controles compensatorios relacionados que se puedan establecer. Riesgo de Control:

Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno. Riesgo de detección: Es el riesgo de que el auditor realice pruebas exitosas a partir de un procedimiento inadecuado.

El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad los hay. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría.

En una auditoría de sistemas de información, la definición de riesgos materiales depende del tamaño o importancia del ente auditado así como de otros factores. El auditor de sistemas debe tener una cabal comprensión de estos riesgos de auditoría al planificar.
Una auditoría tal vez no detecte cada uno de los potenciales errores en un universo. Pero, si el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados se llega a minimizar la probabilidad del riesgo de detección.

De manera similar al evaluar los controles internos, el auditor de sistemas debe percibir que en un sistema dado se puede detectar un error mínimo, pero ese error combinado con otros, puede convertiré en un error material para todo el sistema. La materialidad en la auditoría de sistemas debe ser considerada en términos del impacto potencial total para el ente en lugar de alguna medida basado en lo monetario.

Técnicas de evaluación de Riesgos.
Al determinar que áreas funcionales o temas de auditoría que deben auditarse, el auditor de sistemas puede enfrentarse ante una gran variedad de temas candidatos a la auditoría, el auditor de sistemas debe evaluar esos riesgos y determinar cuales de esas áreas de alto riesgo debe ser auditada.

Existen cuatro motivos por los que se utiliza la evaluación de riesgos, estos son: Permitir

que la gerencia asigne recursos necesarios para la auditoría. Garantizar que se ha obtenido la información pertinente de todos los niveles gerenciales, y garantiza que las actividades de la función de auditoría se dirigen correctamente a las áreas de alto riesgo y constituyen un valor agregado para la gerencia.

Constituir la base para la organización de la auditoría a fin de administrar eficazmente el departamento. Proveer un resumen que describa como el tema individual de auditoría se relaciona con la organización global de la empresa así como los planes del negocio.

3.3 Seguridad y privacidad de la información

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

El termino Seguridad de Información, Seguridad informática y garantía de la información son usados con frecuencia y aun que su significado no es el mismo, persiguen una misma finalidad al proteger la **Confidencialidad**, **Integridad** y **Disponibilidad** de la información; Sin embargo entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración.

La Seguridad de la Información se refiere a la **Confidencialidad**, **Integridad** y **Disponibilidad** de la información y datos, independientemente de la forma los datos pueden tener: electrónicos, impresos, audio u otras formas.
En este artículo representa un panorama general del concepto de la Seguridad de la Información y sus conceptos básicos.

Principios Básicos

Los Gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas acumulan una gran cantidad de información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera. La mayor parte de esta información es recolectada, tratada, almacenada y puesta a la disposición de sus usuarios, en computadoras y trasmitida a través de las redes entre los ordenadores.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.
Por lo que proteger la información confidencial es un requisito del negocio, y en muchos casos también un imperativo ético y una obligación legal.

Para el individuo común, la Seguridad de la Información tiene un efecto significativo respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, Planificación de la continuidad del negocio, Ciencia Forense Digital y Administración de Sistemas de Gestión de Seguridad por nombrar algunos.

Conceptos Importantes

Por más de veinte años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "**C**onfidentiality, **I**ntegrity, **A**vailability") son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones.

El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos.

Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La perdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se publica información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información.

Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizada para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente.

La Alta disponibilidad sistemas objetivo debe seguir estando disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y

actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque Denegación de servicio.

Vulnerabilidades

Son errores que permiten realizar desde afuera actos sin permiso del administrador del equipo, incluso se puede suplantar al usuario, actualmente, ya hay muchas amenazas que tratan de accesar remotamente a los ordenadores, ya sea para hacerlos servidores ilegales de Spam o para robar información, de los agujeros más famosos está el LSASS y el de SVSHOST, de los cuales el Sasser y Blaster se diseminaron rápidamente.

Es imposible evitar las vulnerabilidades al 100% incluso cuando tenemos operando en nuestro sistema cortafuegos, antispam, antivirus, y detectores de código maligno.

Lo que si es posible es tratar de evitarlas al máximo posible. tengamos presente que las comunicaciones en la red constan de 7 capas según el modelo OSI, y las vulnerabilidades pueden estar presentes en varias capas, o incluso dentro del núcleo de nuestro sistema operativo. No debemos imaginar que con un buen antivirus podemos estar libres de vulnerabilidades, ya que las vulnerabilidades no son solo mediante virus que estén radicando en nuestra computadora sino que también pueden llegar a ser mediante ejecución de código mientras visitemos alguna página web, o cuando el atacante tiene privilegios de acceso a nivel administrativo a nuestra computadora

Así que se debe tener presente que para evitar las vulnerabilidades no solamente basta con tener un antivirus y ejecutarlo de manera periódica

Lista de recomendaciones para tener nuestra computadora libre de virus:

--Actualice o cheque las actualizaciones cada cierto tiempo, pues eso permite casi adelantarse a cualquier peligro que se aproveche de la vulnerabilidad.

--no caer en trampas obvias como correos spam diciéndote que ganaste la lotería en un país que ni siquiera conoces

--si vas a descargar música, libros, programas ejecutables, etc. procura hacerlo solo de fuentes confiables

para la mayoría de los usuarios de internet estas simples recomendaciones serán

suficientes y útiles

Aunque no siempre hay una regla general para explotar vulnerabilidades de los sistemas podemos describir a grandes rasgos una serie de pasos para llegar a tal cometido:
paso 1 conocer la existencia de la vulnerabilidad
paso 2 documentarse sobre las características de la vulnerabilidad paso 3 conocer las características del sistema que se va a explotar paso 4 conseguir acceso a ese sistema con los privilegios suficientes

Una ves conseguido el acceso al sistema en cuestión, se es libre de hacer lo que se quiera hacer, es como estar operando frente al computador victima esto, simplifica un ataque, permitiendo a los crackers obtener más permisos en el equipo víctima y poder usarlo al libre albedrío, o el sistema puede ejecutar automáticamente códigos maliciosos, abrir puertos, o en algunos casos es el almacenamiento incorrecto de datos privados, como contraseñas. Un ejemplo es el Remote File Inclusión.

Otros Conceptos
Otros conceptos relacionados son:
•□**Auditabilidad:** Permitir la reconstrucción, revisión y análisis de la secuencia de eventos
•□**Identificación:** verificación de una persona o cosa; reconocimiento.
•□**Autenticación:** Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.
•□**Autorización:** Lo que se permite cuando se ha otorgado acceso
•□**No repudio:** no se puede negar un evento o una transacción.
•□**Seguridad en capas:** La defensa a profundidad que contenga la inestabilidad
•□**Control de Acceso:** limitar el acceso autorizado solo a entidades autenticadas
•□**Métricas de Seguridad, Monitoreo:** Medición de actividades de seguridad
•□**Gobierno:** proporcionar control y dirección a las actividades
•□**Estrategia:** los pasos que se requieren para alcanzar un objetivo
•□**Arquitectura:** el diseño de la estructura y las relaciones de sus elementos

- **Gerencia:** Vigilar las actividades para garantizar que se alcancen los objetivos
- **Riesgo:** la explotación de una vulnerabilidad por parte de una amenaza
- **Exposiciones:** Áreas que son vulnerables a un impacto por parte de una amenaza
- **Vulnerabilidades:** deficiencias que pueden ser explotadas por amenazas
- **Amenazas:** Cualquier acción o evento que puede ocasionar consecuencias adversas
- **Riesgo residual:** El riesgo que permanece después de que se han implementado contra medidas y controles
- **Impacto:** los resultados y consecuencias de que se materialice un riesgo
- **Criticidad:** La importancia que tiene un recurso para el negocio
- **Sensibilidad:** el nivel de impacto que tendría una divulgación no autorizada
- **Análisis de impacto al negocio:** evaluar los resultados y las consecuencias de la inestabilidad
- **Controles:** Cualquier acción o proceso que se utiliza para mitigar el riesgo
- **Contra medidas:** Cualquier acción o proceso que reduce la vulnerabilidad
- **Políticas:** declaración de alto nivel sobre la intención y la dirección de la gerencia
- **Normas:** Establecer los limites permisibles de acciones y procesos para cumplir con las políticas.

Ataques: tipos y naturaleza de inestabilidad en la seguridad

Clasificación de datos: El proceso de determinar la sensibilidad y Criticidad de la información