Final Seguridad Informática

Introducción

Antecedentes

La seguridad informática garantiza la continuidad operativa de la organización, minimiza el daño a la misma y maximiza el retorno sobre las inversiones y las oportunidades.

La alta dirección de cualquier empresa tiene la responsabilidad de atender y facilitar lo necesario para llevar a cabo un análisis de la seguridad informática. El mismo debe abarcar no sólo las áreas de sistema sino también las áreas de negocio o funcionales.

El profesional de seguridad en IT necesita asegurar que el proceso de análisis y evaluación apoye los objetivos del negocio o la misión de la organización. El éxito del mismo depende de su aceptación por parte de todo el personal de la organización.

Características

La mayoría de los enfoques del proceso de análisis de riesgos se basan en los siguientes cuatro principios:

- **Integridad:** Se requiere que la información no sea modificada inapropiadamente.
- **Confidencialidad:** La información debe ser accedida por usuarios autorizados.
- **Disponibilidad:** Que la información esté disponible en el momento necesario.
- **Confiabilidad/Trazabilidad:** Saber de dónde viene la información y quién la utiliza.

El objetivo de un programa de seguridad de IT en una empresa es disminuir el impacto de la materialización de las amenazas en toda esta infraestructura.

Elementos a proteger

Cada organización debe establecer su propio conjunto de requisitos para la protección de sus activos de información. Algunos activos a proteger son: Datos, Hardware, Software, Redes, Sistemas Operativos, BD, Aplicaciones, Instalaciones, Personal, Dinero, Procesos de Negocio, etc.

Esto es documentado a través de una política de clasificación de la información. Se necesita implementar una metodología para ayudar a los usuarios a determinar el nivel de clasificación como parte del proceso de análisis y evaluación de riesgos.

Será necesario hacer que los usuarios visualicen todos los elementos que dan valor al activo, como pueden ser:

- Costo de producir información.
- Valor de información en el mercado.

- Costo de reproducir la información en caso de que fuese destruida.
- Beneficio de la información para cumplir objetivos de negocio.
- Repercusiones si la información no está disponible.
- Ventaja que le daría a la competencia el uso de la información propia.
- El costo para la empresa si la información fuese divulgada.
- La pérdida de confianza del cliente si la información no está asegurada.
- La pérdida de imagen por no tener información segura.

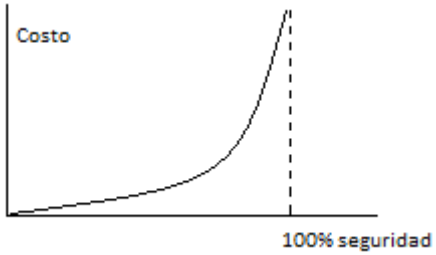
La información y la necesidad de ser protegida

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

La seguridad de la información se refiere a la confidencialidad, integridad y disponibilidad de la información y los datos, independientemente de la forma en la que estén almacenados.

Alcance y costo de la seguridad informática

El alcance determinará qué sectores se verán involucrados en el proceso de seguridad de la información, mientras que el costo determinará el esfuerzo necesario para la implantación del mismo.



Es importante mencionar que la seguridad nunca llega a un 100 % de eficiencia, y el costo tiende a infinito a medida que se intenta llegar a este valor. Por lo tanto es importante determinar correctamente el alcance de la seguridad.

Relación entre operatividad y seguridad

Hay que tener en cuenta que si aumenta la seguridad de un sistema informático, naturalmente la operatividad disminuirá. Esto es debido a que el personal se ve sometido a estrictas normas de seguridad, las cuales pueden complicar la producción. Por ejemplo, en el ámbito de software, un antivirus utiliza recursos de una PC, y por ende, la misma tiene menos operatividad.

$$Operatividad = \frac{1}{seguridad^k}$$

Siendo k un factor que depende de parámetros específicos del sistema en cuestión.

Requerimientos de seguridad

El primer paso para la seguridad informática es identificar los requerimientos de seguridad, existen tres recursos principales para lograrlo:

- Evaluar los riesgos que enfrenta la organización. Identificar las amenazas, evaluar las vulnerabilidades, probabilidades de ocurrencia y estimar el impacto.
- Requisitos legales, tales como normas y reglamentos que debe cumplir la organización.
- Qué principios se utilizan para el procesamiento de la información dentro de la organización.

Riesgos

Definición

Es aquella eventualidad que imposibilita el cumplimiento de un objetivo. Conlleva a dos tipos de consecuencias: ganancias o pérdidas. Aunque en lo relacionado a la seguridad informática, un riesgo siempre es planteado como una amenaza, en donde sólo puede conllevar a una pérdida.

- **Probabilidad:** Probabilidad de ocurrencia del riesgo o amenaza.
- **Amenaza:** Fallas, ingresos no autorizados, virus, desastres ambientales.
- **Vulnerabilidades:** Condiciones de los activos (Falta de conocimiento del usuario, antivirus no actualizado, etc.)
- **Activos:** Los afectados por las amenazas.
- **Impactos:** Pérdida directa de dinero, pérdida de confianza, pérdida de oportunidades de negocios.

Administración y análisis de riesgos

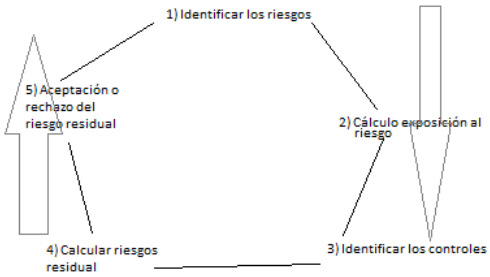
El riesgo total se refiere al riesgo que presenta una determinada amenaza. Este se calcula con el valor del impacto promedio de la misma multiplicada por la probabilidad de ocurrencia.

$$RT = probabilidad\ x\ impacto\ promedio$$

A esto se le debe agregar el riesgo residual. Este es el riesgo que sigue existiendo una vez que se haya implementado una normativa de seguridad. Por ejemplo, un seguro en caso de un incendio que no cubra el 100 % de los activos, tendrá un riesgo residual).

El ciclo de administración del riesgo se cierra una vez que se decide qué acción tomar con los riesgos residuales identificados. Las acciones a tomar son las siguientes:

- Controlar el riesgo.
- Eliminar el riesgo.
- Compartir el riesgo.
- Aceptar el riesgo.



Identificar activos

Debemos identificar todos los recursos cuya integridad pueda ser amenazada de cualquier forma, algunos ejemplos son los siguientes:

- Hardware: Procesadores, tarjetas, impresoras, servidores, etc.
- Software: Sistemas operativos, programas, código fuente, etc.
- Información: Bases de datos, documentos, etc.
- Personas: Clientes, operadores.
- Accesorios: Papel, cintas, tóners, etc.

Con los recursos correctamente identificados, se generará una lista final, que incluirá todo lo que necesitamos proteger en nuestra organización.

Identificar amenazas

Una vez conocidos los recursos que debemos proteger, debemos identificar vulnerabilidades y amenazas que atentan contra ellos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que se aprovecha de una vulnerabilidad para crear un problema de seguridad. Entre ambos conceptos existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Las amenazas se clasifican en 3 grupos:

- **Desastres de entorno:** Desastres naturales, desastres producidos por elementos cercanos (cortes eléctricos), y peligros relacionados con operadores, programadores o usuarios del sistema.
- **Amenazas en el sistema:** Vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, fallos en los programas, etc.
- **Amenazas en la red:** Vulnerabilidades asociadas a la comunicación de un ordenador en una red, como alteración de la información que viaja en la red (Pérdida de integridad).

Algo importante a la hora de analizar las amenazas a las que se enfrentan nuestros sistemas es analizar los potenciales tipos de atacantes que pueden violar nuestra seguridad. En realidad, la

inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema. Muchos de los problemas pueden ser ocasionados por accidentes, desde un operador que vuelca una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica.

Medidas de protección

Tras identificar todos los recursos que queremos proteger, así como las posibles vulnerabilidades y amenazas a la que nos exponemos, y los potenciales atacantes que pueden intentar violar nuestra seguridad, estudiaremos cómo proteger nuestros sistemas, sin ofrecer aún implementaciones concretas para protegerlos. Esto implica en primer lugar cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede realizarse partiendo de hechos sucedidos con anterioridad en la organización, en caso que se los hubiese registrado. En caso que no estén registrados, existen diversas aproximaciones como el método “Delphi”, que consiste en preguntar a una serie de especialistas sobre el daño y las pérdidas que cierto problema puede causar; no obstante, la experiencia del administrador de seguridad suele tener la última palabra a la hora de evaluar los impactos de cada amenaza.

La clasificación de riesgos de cara a estudiar medidas de protección suele realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad. Se trata principalmente de no gastar más dinero en una implementación para proteger un recurso de lo que vale el mismo o de lo que nos costaría recuperarnos de un daño en él o de su pérdida total.

Una vez que conocemos el riesgo evaluado de cada recurso, es necesario efectuar lo que se llama el “análisis de costes y beneficios”. Consiste en comparar el coste asociado a cada problema con el coste de prevenir dicho problema. Por ejemplo, para consultar el coste de prevenir un incendio, basta con saber el precio de los sistemas de extinción de fuego, o para saber lo que nos cuesta proteger una red, deberemos averiguar el precio de routers que bloqueen paquetes o posean un firewall statefull. No sólo tendremos en cuesta el costo de los materiales, sino también su implementación y mantenimiento.

Cuando ya hemos realizado este análisis, no tendremos más que presentar nuestras cuentas a los responsables de la organización, siempre teniendo en cuenta que el gasto de proteger un recurso ante una amenaza ha de ser inferior al gasto que se produciría si la amenaza se convirtiera en realidad. Hay que tener en cuenta que los riesgos se pueden minimizar, pero nunca eliminar por completo, por lo que será recomendable planificar no sólo la prevención de un problema sino también la recuperación si el mismo se produce. Se suele hablar de medidas proactivas (prevención de un problema) y medidas reactivas (posterior al daño).

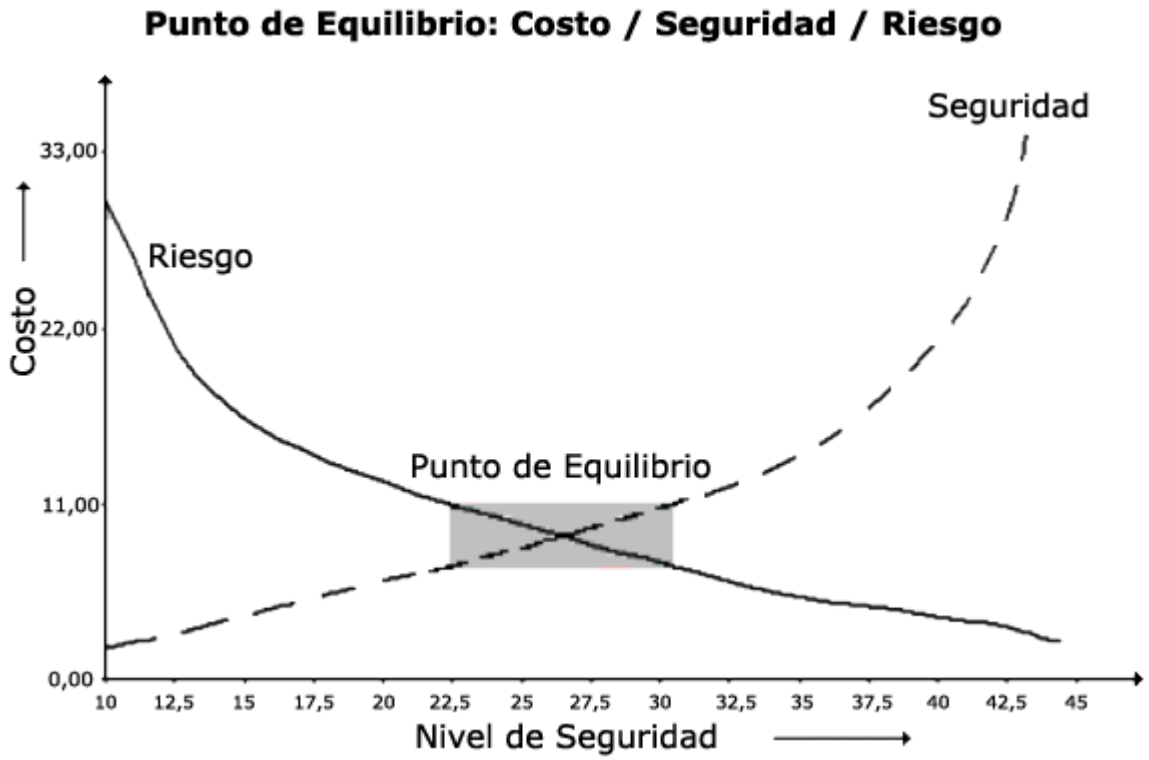
Matriz de riesgo

El proceso de análisis de riesgo genera habitualmente un documento al cual se le conoce como "matriz de riesgo". En este documento se muestran los elementos de riesgo identificados, la manera en que se relacionan y los cálculos realizados. Este análisis de riesgo es indispensable para lograr una correcta administración de riesgo.

La matriz es un simple mecanismo para incrementar la visibilidad de riesgos y poder tomar decisiones correctas en caso que sea necesario.

Punto de equilibrio

Una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir y decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio entre estas magnitudes.



Como puede apreciarse, los riesgos disminuyen al aumentar la seguridad (y los costos) pero como ya se sabe, los costos tenderán al infinito sin lograr el 100 % de seguridad, y por supuesto nunca se logrará cubrir todos los riesgos. Lo importante es lograr conocer cuán seguro se estará conociendo los costos y los riesgos que se corren (punto de equilibrio).

Seguridad Física

Perímetro de Seguridad

El perímetro físico es una delimitación de acceso a una determinada área. El área delimitada está claramente definida y tiene que poseer algún método de identificación o control de acceso. El grado de seguridad de este control depende del tipo de información que se maneja dentro del perímetro. El área estará delimitada por una barrera, como por ejemplo una pared, puerta de acceso, etc.

Deben existir controles sobre entrada y salida del personal, las oficinas de trabajo solo deben ser accesibles por el personal de trabajo y no al personal exterior sin una debida autorización. El área de entrega y carga debe ser aislada de forma segura de las demás instalaciones.

Controles de Acceso

El control de acceso no solo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una organización.

Algunos tipos de controles de acceso son los siguientes:

- Utilización de guardias
- Utilización de detectores de metales
- Utilización de sistemas biométricos (Huellas digitales, Verificación de voz, etc.)
- Verificación automática de firmas (Se considera lo que el usuario es capaz de hacer)
- Seguridad con animales
- Protección electrónica (Circuitos de TV, Detector ultrasónico, etc.)

Copias de seguridad

Una copia de seguridad sirve para restaurar datos en caso de una eventual pérdida de los mismos. Los medios donde residen estas copias tendrán que estar protegidos físicamente.

Lo primero que debemos pensar es dónde se almacenan los dispositivos donde se realizan las copias. Es recomendable guardar las copias en una zona alejada de la sala de operaciones; lo que se suele recomendar es disponer de varios niveles de copia, una que almacena en una caja de seguridad en un lugar alejado y que se renueva con una periodicidad alta, y otras de uso frecuente en lugares más próximos.

Para proteger más aun la información copiada se pueden emplear mecanismo de cifrado, de modo que la copia que guardamos no sirva de nada si no disponemos de la clave para recuperar los datos almacenados.

Suministro de energía

Es muy habitual tener que implementar esta clase de servicio si se quiere que algún dispositivo trabaje ininterrumpidamente. Esto puede realizarse con UPS o generadores. Y para evitar un único punto de fallo de energía eléctrica se pueden usar múltiples bocas de suministro.

Además hay que tener en cuenta que al tener un generador, éste debe estar aislado apropiadamente y debe poseer algún tipo de desconexión manual de fácil acceso en caso de alguna amenaza natural.

Cableados

El cableado de energía eléctrico y de comunicaciones debe ser apropiadamente protegido, ya sea por eventuales errores humanos (desconexión) o por intereses malignos.

Algunas características que deben cumplir son:

- Subterráneas siempre que sea posible.
- Separación entre cables de energía y de comunicación.
- Cableado apropiadamente ordenado, con canaletas y demás.

Mantenimiento de equipos

El mantenimiento predictivo trata de percibir una posible falla de un equipo que pueda ocurrir en un futuro, de manera que se tomen acciones posteriormente. Un ejemplo puede ser el caso de un ventilador en un servidor que está haciendo más ruido de lo normal.

El mantenimiento preventivo es una actividad programada de inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, análisis, limpieza, etc. que deben llevarse a cabo en forma periódica en base a un plan establecido. El propósito es prever desperfectos en su estado inicial y corregirlos para una operación optima.

El mantenimiento correctivo se da una vez que se ha producido el fallo del equipo que prohíbe la utilización completa o parcial del mismo.

Disposición, Refrigeración y Mantenimiento del equipamiento

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

Protecciones contra incendios

Existen diversos mecanismos de protección contra incendios. Mencionaremos los más comunes.

El **FM 200 es un agente extintor**, se trata de un gas incoloro, no conductor de la electricidad y casi inodoro. Es muy eficiente para la **extinción de incendios de tipo A, B y C**. Este gas se aplica donde antiguamente se usaba el halón 1301. Pero la gran ventaja del FM 200 sobre el halón es que no atenta contra el medio ambiente ni supone ningún riesgo sobre las personas. Es por tanto un agente extintor limpio. Es capaz de extinguir el fuego en menos de 10 segundos.

Ver http://www.youtube.com/watch?v=KjJhSRn3vQ0

Existen alternativas más baratas al FM-200 pero que en muchos casos, no pueden ser aplicados en ambientes donde hay personas.

Seguridad Lógica

Seguridad en capas

Combina diferentes componentes de seguridad: Antivirus, firewall, tablas de ruteo, etc. Aumenta el costo pero dificulta la penetración de intrusos desde el exterior.

Componentes de seguridad

Un firewall es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Un antivirus es un programa cuyo objetivo es detectar y/o eliminar virus informáticos.

Un Gateway antivirus constituye la primera barrera o barrera perimetral de protección frente a virus para una red empresarial. Se instala en gateways y suele proteger los datos provenientes de protocolos estándares (Http, Smtp, etc.)

Detección de intrusos

Existe un programa llamado IDS (Intrusion detection system) que permite detectar el acceso no autorizado a un host o una red. Funcionan analizando paquetes, puertos, qué tipo de tráfico hay en la red, su contenido y su comportamiento. Difiere de un firewall, ya que el primero analiza mientras que el otro deniega o permite el acceso. Existen dos tipos:

- Host IDS: Se basa sobre un equipo afectado, protege un solo host.
- Network IDS: Analiza toda la red buscando patrones.

También se pueden clasificar por el tipo de respuesta que dan:

- Pasivos: Notifican al administrador de la red sobre un intruso.
- Activos: Generan una respuesta sobre el sistema atacante como cerrarle la conexión.

Un ejemplo de sistema IDS es Snort. http://www.snort.org/

Detección de vulnerabilidades

Existen herramientas que permiten realizar pruebas o tests de ataque para determinar si una red o equipo tiene fallos de seguridad.

Ejemplos de herramientas de detección de vulnerabilidad son Nessus, Metasploit, Nmap, etc.

Subdivisión de redes

Un método para controlar la seguridad de redes extensas, es dividirlas en dominios lógicos separados, por ejemplos dominios de red internos y externos de una organización, cada uno protegido por un perímetro de seguridad definido. Dicho perímetro puede ser implementado mediante la instalación de un Gateway seguro entre las dos redes, que han de ser interconectadas, para controlar el acceso y flujo de información entre los dos dominios.

Control de acceso

Es un concepto general de cómo se determina el acceso a recursos, incluye controles sobre los recursos accedidos y sobre los orígenes de esos accesos, los horarios de los accesos, la forma en que se acceden a esos recursos (ej.: vía módem o vía LAN). Los criterios de denegación o permiso de acceso pueden ser tan variados y/o complicados como las políticas corporativas lo necesiten.

Existen diversos modos de autenticación:

- Password
- Tokens
- Sistemas biométricos
- Ubicación geográfica
- Certificados digitales
- Protocolos PAP, CHAP, RADIUS

Lo importante es seleccionar los métodos de autenticación en base a la criticidad del recurso a proteger.

Políticas de password

Las políticas de passwords son un aspecto muy importante en la seguridad informática. La existencia de passwords débiles puede resultar en riesgos importantes para la organización (ante ataques por fuerza bruta).

Las políticas de password más importantes son:

- Expiración por fecha
- Expiración por tiempo
- Expiración por reintentos fallidos
- Reuso
- Consistencia

Camino forzado

Puede resultar necesario controlar el camino desde la terminal de usuario hasta el servicio informático. Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad de ruteo. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de negocios, o para el uso no autorizado deservicios de información. Estos riesgos pueden reducirse mediante la incorporación de controles, que limiten la ruta entre una terminal de usuario y los servicios del computador, a los cuales sus usuarios están autorizados a acceder, por ejemplo creando un camino forzado.

El objetivo de un camino forzado es evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo está autorizado a acceder.

Firewall de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. Un cortafuego de aplicación puede filtrar protocolos de capas superiores tales como FTP, TELNET, DNS, DHCP, HTTP, TCP, UDP y TFTP (GSS).

VPN

Una VPN es básicamente una red privada que utiliza una red pública para conectar sitios remotos o usuarios dentro de una misma red.

En vez de usar líneas dedicadas, se utilizan conexiones “virtuales” ruteadas a través de Internet hacia las redes privadas de la compañía.

A esa red privada, es necesario adicionarle ciertos mecanismos que aseguren la integridad y confidencialidad de la información que circula por la VPN.

Una VPN se logra mediante el “tunneling”. Esto significa conectar dos puntos finales de VPN como si pertenecieran a la misma red o en el mismo edificio

Control de contenidos

Existe en la actualidad una extensa gama de herramientas de control y monitorización, capaces bloquear el acceso a contenidos no apropiado para menores. Tales herramientas pueden variar mucho cuanto a los métodos de control empleados y la facilidad de configuración por parte de los usuarios.

Tales herramientas realizan el control de acceso a contenidos no deseados de distintas maneras: bloqueando direcciones, controlando horas de acceso, impidiendo que páginas con determinados contenidos puedan ser consultadas, utilizando listas de acceso o no acceso (listas positivas y negativas), aceptando listas de direcciones predeterminadas o estableciendo una lista propia de direcciones aceptadas o negadas, asignando diferentes perfiles en diferentes días y horas (trabajo, tiempo libre, etc.), regular qué servicios se pueden utilizar en cada momento y por cada usuario (correo, chat, etc.), etc.

Seguridad administrativa y legal

Política de personal

Se deben llevar a cabo controles de verificación del personal permanente en el momento en que se solicita el puesto. Éstos deben incluir los siguientes:

- Disponibilidad de certificados de buena conducta satisfactorios (laboral y personal)
- Comprobación de integridad y veracidad del CV del aspirante
- Constatación de las aptitudes académicas y profesionales alegadas
- Verificación de la identidad (pasaporte o similar)

Política de seguridad de la empresa

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

Ley de habeas datas

Habeas data es el derecho, en ejercicio de una acción constitucional o legal, que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

Firma digital

Una firma digital es un esquema matemático que sirve para demostrar la autenticidad de un mensaje digital, que puede ser por ejemplo un documento electrónico. Una firma digital da al destinatario seguridad de que el mensaje fue creado por el remitente (autenticidad de origen), y que no fue alterado durante la transmisión (integridad). Las firmas digitales se utilizan comúnmente para la distribución de software, transacciones financieras y en otras áreas donde es importante detectar la falsificación y la manipulación.

La firma digital consiste en un método criptográfico que asocia la identidad de una persona o de un equipo informático, al mensaje o documento. En función del tipo de firma, puede además asegurar la integridad del documento o mensaje.

Propiedad intelectual

La propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación. El mismo tiene el derecho exclusivo a la explotación de la obra. La ley protege las creaciones originales expresadas en cualquier medio, incluidos programas de ordenador o bases de datos.

Confidencialidad

La confidencialidad también se refiere a un principio ético asociado con varias profesiones (por ejemplo, medicina, derecho, religión, psicología profesional, y el periodismo); en este caso, se habla de secreto profesional. En ética, y (en algunos lugares) en Derecho, concretamente en juicios y otras formas de resolución de conflictos legales, tales como la mediación, algunos tipos de comunicación entre una persona y uno de estos profesionales son "privilegiados" y no pueden ser discutidos o divulgados a terceros. En las jurisdicciones en que la ley prevé la confidencialidad, por lo general hay sanciones por su violación.

Contratos informáticos

En sentido amplio u objetivo, abarca todos aquellos convenios cuyo objeto sea un bien o servicio informático, independientemente de la vía por la que se celebren. El objeto del contrato, por tanto, sería la prestación de un servicio informático.

Los contratos informáticos pueden referirse tanto a bienes (hardware o software) como a servicios informáticos (tales como mantenimiento preventivo, correctivo o evolutivo; desarrollo y hospedaje de sitios web, prestación de servicios de certificación digital, etc.).

Metodología MAGERIT

Introducción

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

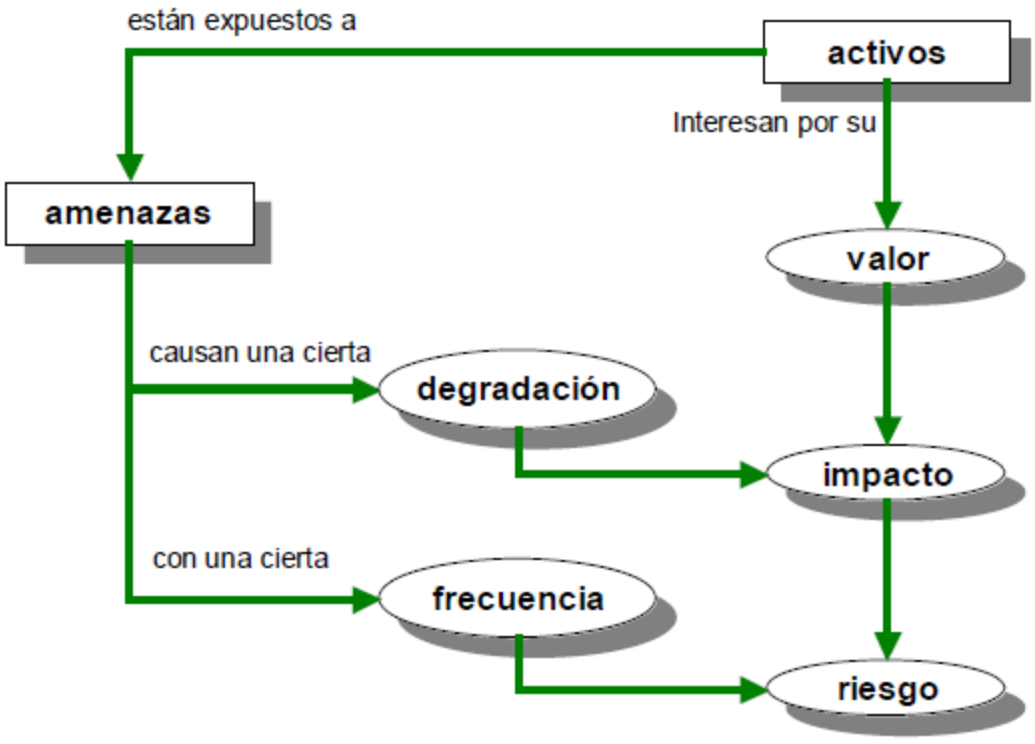
La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

Evaluación y gestión de riesgos

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

El análisis de riesgos es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.

La gestión de riesgos es la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.



El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

Matriz de riesgo

Una matriz de riesgo (o mapa de riesgo) nos informa de amenazas posibles, caracterizadas por su frecuencia de ocurrencia y la degradación que causarían en los activos.

		dimensiones de seguridad						
activo / amenaza	frecuencia	D	I	C	A_S	A_D	T_S	T_D
[D_exp] Expedientes en curso		50%	50%	100%	100%	100%	100%	100%
[E.1] Errores de los usuarios	10	10%	10%					
[E.2] Errores del administrador	1	20%	20%	10%	10%	10%	20%	20%
[E.3] Errores de monitorización (log)	1						50%	50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%	50%	50%
[E.14] Escapes de información	1			1%				
[E.15] Alteración de la información	10		1%					
[E.16] Introducción de falsa información	100		1%					
[E.17] Degradación de la información	10		1%					
[E.18] Destrucción de la información	10	1%						
[E.19] Divulgación de información	1			10%				
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%	100%	100%
[A.11] Acceso no autorizado	100		10%	50%	50%			
[A.14] Intercepción de información (escucha)	10			50%				
[A.15] Modificación de información	10		50%					
[A.16] Introducción de falsa información	20		50%					
[A.17] Corrupción de la información	10		50%					
[A.18] Destrucción de la información	10	50%						
[A.19] Divulgación de información	10			100%				

La primera columna muestra las amenazas típicas sobre el activo. La segunda columna recoge la frecuencia de ocurrencia expresada como tasa anual (incidencias por año). Las demás columnas recogen la degradación del activo expresada como porcentaje de su valor.

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A_S] autenticidad de los usuarios del servicio
- [A_D] autenticidad de quien accede a los datos
- [T_S] trazabilidad del servicio
- [T_D] trazabilidad de los datos

Tipos de activos

Se denominan activos los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan
- para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Dimensiones de valoración

¿Por qué interesa un activo? Por lo que vale. No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; eso es lo que hay que averiguar pues eso es lo que hay que proteger.

De un activo puede interesar calibrar diferentes dimensiones:

- Su autenticidad: ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- Su confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
- Su integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?
- Su disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Hay accidentes naturales (terremotos, inundaciones, etc.) y desastres industriales (contaminación, fallos eléctricos, etc.) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- Degradación: cuán perjudicado resultaría el activo
- Frecuencia: cada cuánto se materializa la amenaza

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos:

100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

Salvaguardas

Hasta ahora no se han tomado en consideración las salvaguardas desplegadas. Se miden, por tanto, impactos y riesgos a que estarían expuestos los activos si no se protegieran en absoluto. En la práctica no es frecuente encontrar sistemas desprotegidos: las medidas citadas indican lo que ocurriría si se retiraran las salvaguardas presentes.

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Gestión de la continuidad del negocio

Continuidad del negocio y el análisis del impacto

Un plan de continuidad del negocio es la respuesta prevista por la empresa ante situaciones de riesgo que le pueden afectar de forma crítica. No importa el tamaño de la empresa o el coste de las medidas de seguridad implantadas, toda organización necesita un plan de continuidad en el negocio, ya que tarde o temprano se encontrará con una incidencia de seguridad.

En líneas generales, podemos decir que estos planes tienen como objetivo impedir que la actividad de la empresa se interrumpa, y si no puede evitarse, que el tiempo de inactividad sea el mínimo posible.

Además, se debe intentar lo siguiente:

- Mantener el nivel de servicio en los límites definidos por la compañía y que han sido asumidos por la misma.
- Establecer un período de recuperación mínimo para garantizar la continuidad del negocio.

- Recuperar la situación inicial de los servicios y procesos. Puede que existan procesos más críticos que necesiten recuperarse antes.
- Analizar el resultado de la aplicación del plan y los motivos de fallo para optimizar las acciones a futuro. Es decir, aprender de las incidencias para mejorar en la respuesta.

Cuando desarrollamos nuestro plan de continuidad del negocio tenemos que tener en cuenta que debe contener los siguientes apartados:

- Establecimiento y definición de las situaciones críticas: Se han de identificar, entre los riesgos analizados, aquellos que no podrán ser evitados a través de las diversas medidas implantadas.
- Establecimiento de un comité de emergencia: Será encargado de gestionar la situación de crisis ante una incidencia.
- Definición de situaciones posibles: Elaborar procedimientos para cada una de las incidencias que se podrían dar en la organización.
    - Situación que provoca una incidencia.
    - Acciones y secuencias a llevar a cabo.
    - Registros durante la incidencia para su análisis y mejora.

El plan debe ser conocido por todo el personal involucrado directa o indirectamente.

Plan de contingencias

Un Plan de contingencias es un instrumento de gestión que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. Un plan de contingencias es un caso particular de plan de continuidad del negocio aplicado al departamento de informática o tecnologías. Otros departamentos pueden tener planes de continuidad que persiguen el mismo objetivo desde otro punto de vista.

El plan de contingencias sigue el conocido ciclo de vida iterativo PDCA (plan-do-check-act, es decir, planificar-hacer-comprobar-actuar). Nace de un análisis de riesgo donde, entre otras amenazas, se identifican aquellas que afectan a la continuidad del negocio.

Sobre dicha base se seleccionan las contramedidas más adecuadas entre diferentes alternativas, siendo plasmadas en el plan de contingencias junto con los recursos necesarios para ponerlo en marcha.

El plan debe ser revisado periódicamente. Generalmente, la revisión será consecuencia de un nuevo análisis de riesgo. En cualquier caso, el plan de contingencias siempre es cuestionado cuando se materializa una amenaza, actuando de la siguiente manera:

- Si la amenaza estaba prevista y las contramedidas fueron eficaces: se corrigen solamente aspectos menores del plan para mejorar la eficiencia.

- Si la amenaza estaba prevista pero las contramedidas fueron ineficaces: debe analizarse la causa del fallo y proponer nuevas contramedidas.
- Si la amenaza no estaba prevista: debe promoverse un nuevo análisis de riesgos. Es posible que las contramedidas adoptadas fueran eficaces para una amenaza no prevista. No obstante, esto no es excusa para evitar el análisis de lo ocurrido.

El plan de contingencias comprende tres subplanes. Cada plan determina las contramedidas necesarias en cada momento del tiempo respecto a la materialización de cualquier amenaza:

- El plan de respaldo. Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.
- El plan de emergencia. Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.
- El plan de recuperación. Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

Por otra parte, el plan de contingencias no debe limitarse a estas medidas organizativas. También debe expresar claramente:

- Qué recursos materiales son necesarios.
- Qué personas están implicadas en el cumplimiento del plan.
- Cuáles son las responsabilidades concretas de esas personas y su rol dentro del plan.
- Qué protocolos de actuación deben seguir y cómo son.

Ejemplo

Supongamos una pequeña compañía que se dedica a la producción de prendas textiles. Un análisis de riesgos identificaría (entre otras cosas) lo siguiente:

Activos e interdependencias: Oficinas centrales → Centro de proceso de datos → Computadoras y almacenamiento → Información de pedidos y facturación → Proceso de negocio de ventas → Imagen corporativa

Este análisis demuestra que una amenaza materializada en las oficinas centrales podría llegar a afectar al proceso de negocio dedicado a la venta. Aunque esto no impida a la compañía seguir comercializando productos, supondría una interrupción temporal de las ventas. Además afectaría negativamente a la imagen corporativa provocando la pérdida de clientes. Así, se evaluaría la siguiente amenaza y su impacto:

- Amenaza: Incendio. (los activos afectados son los anteriores).
- Impacto: (es un ejemplo ficticio)

    - Perdida de un 10% de clientes.
    - Imposibilidad de facturar durante un mes.
    - Imposibilidad de admitir pedidos durante un mes.
    - Reconstrucción manual de pedidos y facturas a partir de otras fuentes.
    - Sanciones por accidente laboral.
    - Inversiones en equipamiento y mobiliario.
    - Rehabilitación del local.

Todas estas consecuencias pueden valorarse en términos monetarios, que junto a la probabilidad de materialización ofrecen una estimación del riesgo.

El plan de contingencias contendría someramente las siguientes contramedidas:

- Medidas técnicas:
    - Extintores contra incendios.
    - Detectores de humo.
    - Salidas de emergencia.
    - Equipos informáticos de respaldo.
- Medidas organizativas:
    - Seguro de incendios.
    - Precontrato de alquiler de equipos informáticos y ubicación alternativa.
    - Procedimiento de copia de respaldo.
    - Procedimiento de actuación en caso de incendio.
    - Contratación de un servicio de auditoría de riesgos laborales.
- Medidas humanas:
    - Formación para actuar en caso de incendio.
    - Designación de un responsable de sala.
    - Asignación de roles y responsabilidades para la copia de respaldo.

Los subplanes contendrían las siguientes previsiones:

- Plan de respaldo:
    - Revisión de extintores.
    - Simulacros de incendio.
    - Realización de copias de respaldo.
    - Custodia de las copias de respaldo (por ejemplo, en la caja fuerte de un banco).
    - Revisión de las copias de respaldo.
- Plan de emergencia:
    - Activación del precontrato de alquiler de equipos informáticos.
    - Restauración de las copias de respaldo.
    - Reanudación de la actividad.
- Plan de recuperación:
    - Evaluación de daños.

- Traslado de datos desde la ubicación de emergencia a la habitual.
- Reanudación de la actividad.
- Desactivación del precontrato de alquiler.
- Reclamaciones a la compañía de seguros.