La seguridad en sistemas de red. Servicios de seguridad.

TEMA 63

INFORMATICA

Sistemas y Aplicaciones Informáticas (SAI)

OPOSICIONES 2023

ABACUSNT

Tema de muestra. Esta Página está en blanco a propósito.

Tema de muestra. Esta Página está en blanco a propósito.

- **No repudio:** En origen y/o destino, de forma que se garantice la emisión y/o recepción de la misma.
- **Trazabilidad:** Debe ser posible tener un registro de lo que ocurre con dicha información desde que es creada hasta cualquier momento en el tiempo con fines de **análisis forense**.

2.1. Políticas de seguridad.

Dos principios fundamentales de la seguridad informática son:

- **No existen sistemas completamente seguros.** Por tanto, el objetivo es conseguir un sistema suficientemente seguro teniendo en cuenta las necesidades específicas de cada caso.
- **La seguridad es un proceso continuo** que requiere **participación universal**.

Estos dos principios implican que **no existe la seguridad absoluta,** por lo que el objetivo debe ser garantizar una seguridad adecuada, haciendo un adecuado **análisis del riesgo** y buscando un compromiso **entre el coste de las medidas de seguridad y los beneficios derivados de aumentar la seguridad del sistema**.

2.2. Análisis de riesgos.

El proceso de gestión de Riesgos consiste en el tratamiento y análisis de los riesgos que pueden afectar a una organización.

La inversión en análisis y gestión de Riesgos de la información trata de prevenir los fallos y estar preparados por si estos ocurren.

Podemos entender el análisis de riesgos como un estudio con el fin de identificar los activos críticos de los sistemas de información que dan soporte a los procesos de negocio de nuestra organización y las **amenazas que puede comprometer su disponibilidad, integridad o confidencialidad.**

El análisis de riesgos pretende calcular el riesgo al que está sometida la organización mediante un procedimiento **metódico** que nos dé una **estimación cuantitativa del riesgo.**

Un buen sistema es aquel que, en caso de tener un incidente informático, **lo tiene bajo control**, es decir, sabía que podía ocurrir, sabe lo que puede provocar y sabe arreglar el problema.

Por tanto, debemos tener en cuenta los siguientes tres elementos:

- **Activos**: los activos son elementos de la empresa que deben protegerse.
- **Amenazas**: son las situaciones de las cuales deben protegerse los activos.

- **Vulnerabilidades:** son los aspectos que facilitan la materialización de las amenazas

El riesgo consiste en la relación de estos tres elementos. Combinándolos entre sí se obtienen los diferentes tipos de riesgos a los que se haya expuesta una organización.

Este proceso de **securización** en el que deben participar **todos los empleados** de la empresa requiere de un análisis previo en el que se **estimen las amenazas y vulnerabilidades** existentes, **la posibilidad de que ocurran**, y el **coste en los activos** de las mismas de hacerse realidad, estimando cuantitativamente estos factores y obteniendo **un valor numérico** que nos indique el riesgo real de que una situación de riesgo comprometa seriamente la seguridad de la red y a qué coste.

Con el **tratamiento de los riesgos** se pretende **diseñar un plan de seguridad** que permita a la dirección tener la confianza necesaria para comenzar o continuar con la actividad en caso de fallo.

3. Control de acceso y gestión de credenciales.

3.1. Autenticación. Tipos y sistemas de autenticación.

Vista la importancia de la autenticación, a continuación, se exponen las técnicas y tecnologías para implantar la identificación y autenticación de usuarios.

3.1.1. Identificador y contraseña

La autenticación por medio de contraseñas es relativamente sencilla: el usuario A envía su identificador IDA y acto seguido su contraseña PA. La implementación del protocolo de identificación puede precisar que ambas informaciones se manden en un mismo mensaje, o bien que primero se pida el nombre de usuario y después la contraseña.

Esta contraseña es usada por el servicio para validar la identidad del usuario. Si A es el único conocedor de PA , es altamente probable que el usuario sea realmente A.

Para verificar que la contraseña PA es correcta, primero se encripta con algún sistema de cifrado generando CA y después se compara con la almacenada en el servidor: En la base de datos del servidor **nunca se almacena la clave plana del usuario**, sino cifrada, para evitar cualquier que un robo de información comprometa a los usuarios. Por tanto, se recupera la clave cifrada del servidor CS y si coincide con CA, se puede garantizar la identidad del usuario y por tanto se realiza la autenticación del mismo.

El **sistema de PIN** funciona exactamente igual, pero utilizando usa secuencia de un mínimo de 4 dígitos numéricos como contraseña.

3.1.2. OTP (One-Time Password)

En este caso, el usuario posee un “calculador” específico que va a permitirle proporcionar una contraseña válida durante un período limitado.

Para poder utilizar su calculador, debe entrar previamente una contraseña. El calculador le proporciona entonces a cambio otra contraseña de un solo uso que el usuario va, a su vez, a proporcionar al módulo de autenticación.

El módulo de autenticación dialoga a continuación con el servidor OTP para asegurarse de la validez de la información proporcionada y para aceptar o no la conexión.

3.1.3. Certificados electrónicos

Los sistemas de clave pública representan otra forma de autenticación ante un servicio. La firma electrónica o los certificados electrónicos son dos de las utilidades que sirven a modo de autenticación de identidad. Estos sistemas utilizan **dos claves, una pública y otra privada**, para poder generar un potente sistema de autenticación usando la criptografía como base del mismo. Los sistemas de clave pública se tratarán en el próximo tema.

3.1.4. Dispositivos de usuario

En algunos servicios que funcionan sobre Internet ya es habitual que la autenticación de la identidad sea a través de un certificado de cliente, en lugar de una infraestructura de clave pública como en los certificados digitales.

En general, para usar este sistema de autenticación, se acabará usando una clave privada que estará albergada en un dispositivo o en el propio sistema. Esta clave secreta debe estar protegida (cifrada), y sólo se debe poder usar tras introducir una **contraseña o PIN**. A veces, la propia contraseña introducida por el usuario se usará como clave para descifrar la clave secreta y poder usarla.

Cuando la clave privada se almacena en un dispositivo extraíble, tal como un USB o una tarjeta inteligente, reciben el nombre de tokens de seguridad, aunque realmente el token es un código que se almacena en su interior.

El dispositivo “token” a su vez, puede ser un dispositivo USB, Bluetooth, una etiqueta RFID, una tarjeta inteligente (tarjeta bancaria con chip, etc), una tarjeta SIM (Subscriber Identity Module) telefónica o un DNIe (DNI electrónico).

3.1.5. Biometría

La biometría vendría a significar algo así como "medir" los rasgos "biológicos" de un individuo.

Esta tecnología hace años que aparece como habitual sistema de autenticación en la literatura y películas de fantasía y ciencia ficción. De todos modos, el análisis del iris, la forma de la mano, incluso la manera de andar, etc. ya juegan un papel importante en sistemas de control de acceso reales.

Tema de muestra. Esta Página está en blanco a propósito.

2 **cifrado de datos por sustitución**. Sustituye cada carácter del texto con un carácter diferente de acuerdo con un algoritmo determinado.

Ambos tipos pueden ser combinados para formar cifrados más complejos.

3.3.2. Criptografía moderna.

Con el algoritmo de Diff y Hellman de clave asimétrica y la aparición de los ordenadores, la criptografía toma un enfoque completamente distinto. Actualmente se utilizan dos tipos de algoritmos de cifrado en las comunicaciones:

Cifrado con clave simétrica o privada. Se usa una única clave para cifrar y descifrar la información, que debe ser conocida únicamente por el emisor y el receptor. Plantea el problema del envío de la clave al receptor de manera segura. Por ejemplo, DES.

Cifrado con clave asimétrica o pública. Se usa una clave secreta para cifrar y otra pública para descifrar la información, o viceversa. No es necesario enviar ningún tipo de clave al receptor. Son algoritmos mucho más lentos que los de clave privada. Por ejemplo, RSA.

3.4. Integridad. Funciones HASH

Se denominan funciones resumen o HASH a aquellos procedimientos que, dado un mensaje de tamaño cualquiera, **producen una salida de tamaño fijo**. Las aplicaciones más extendidas de las funciones HASH son el control de **integridad de documentos** y la creación de firmas digitales.

Las funciones HASH se implementan normalmente mediante los algoritmos de cifrado MD5 o SHA.

La función HASH sobre un documento concreto genera una huella digital del mismo, única para cada documento. Una alteración en el documento original provocaría que la función HASH generase una huella completamente distinta.

Las huellas digitales mediante funciones HASH **son una garantía de que el documento no ha sido alterado**.

3.5. Aceptación/no repudio. Certificados y Firma electrónica.

La firma electrónica es un conjunto de datos electrónicos que acompañan o que **están asociados** a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca
- Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

El proceso básico que se sigue para la firma electrónica es el siguiente:

1. El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
2. La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
3. La aplicación utiliza la clave privada para codificar el resumen.
4. La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante.

4. Seguridad física (Técnicas y sistemas de protección)

4.1. Protección de los equipos y las instalaciones.

4.1.1. Protección ante agentes ambientales.

Electricidad estática. Para evitar descargas electroestáticas no deseadas, todos los puntos de suministro de corriente eléctrica deben tener toma de tierra.

Temperaturas extremas. Los equipos informáticos son sensibles al calor excesivo, por lo cual deben estar dotados de disipadores para los microprocesadores y ventiladores para la caja.

Agua. Los equipos deben estar lejos de cualquier lugar que pueda tener una fuga de agua.

Polvo y suciedad. El lugar en el que están situados los equipos debe estar limpio y ordenado.

4.1.2. Precauciones eléctricas y físicas

Allí donde exista una ruta de comunicaciones bajo control completo de los usuarios, puede ser posible tender cables a través de conductos de metal apantallados de forma que no puedan ser abiertos por intrusos sin que eso sea detectado,

Las emisiones electromagnéticas comprometedoras procedentes del equipo pueden reducirse adoptando las siguientes precauciones:

a) Situar el equipo dentro de un recinto apantallado con conexiones a tierra que actúen como una caja de Faraday, impidiendo el paso por ella de radiación electromagnética.

b) Seleccionar equipamiento que haya sido diseñado para cumplir los requisitos de seguridad necesarios o que tenga un buen apantallamiento y filtrado interno para evitar la radiación electromagnética.

c) Instalar filtros de paso bajo efectivos en los cables principales y en los cables de señalización eléctrica conectados al equipo.

d) Instalar los equipos en un área que no tenga cables, tuberías conductoras o teléfonos que puedan conducir las señales comprometedoras fuera del área de seguridad.

e) Utilizar para los equipos una conexión a tierra de baja impedancia.

La presencia de escuchas en los cables eléctricos se puede detectar mediante una inspección visual regular del camino completo de señal. Las escuchas que consumen potencia o las de baja impedancia se pueden detectar utilizando un voltímetro electrónico para comprobar la línea a intervalos regulares. **Las escuchas de alta impedancia son casi indetectables**, pero, en algunas circunstancias, los puentes de capacitancia equilibrada han demostrado que son capaces de detectar su presencia. Las escuchas por acoplamiento inductivo no son detectables eléctricamente. Las escuchas en cables de fibra óptica se pueden detectar mediante refractómetros en el dominio del tiempo o medidores de nivel de señal en el receptor.

4.1.3. Sistemas de alimentación ininterrumpida (UPS).

Un SAI es un sistema redundante de suministro eléctrico. Cuando hay un corte en el suministro eléctrico, el SAI proporcionará dicha electricidad. No obstante, existen una serie de SAI de uso más profesional que lo que hacen es suministrar la corriente a los equipos dando una señal perfecta sin importar si hay algún problema en el suministro eléctrico.

Los SAI tienen **rectificadores y reguladores** de la tensión para que el equipo no sufra las consecuencias de bajadas y subidas de tensión de la red eléctrica.

En empresas con servidores, la instalación de un SAI es prácticamente obligatoria, puesto que el perjuicio que pueden sufrir frente a un corte de electricidad sería funesto. Los cortes de tensión en una empresa que maneje un volumen alto de información pueden ocasionar pérdidas de información, pérdidas monetarias y fallos en el servicio ofrecido.

Aunque no es común instalar un SAI en un equipo doméstico, en ocasiones, si existen muchos tallos de la señal eléctrica, sería altamente recomendable.

Un SAI soluciona los defectos de la señal eléctrica posibles. La diferencia entre un SAI de ámbito empresarial frente a uno doméstico son la capacidad, la fiabilidad, los defectos de señal que cubre, el tiempo de conmutación etc.

En la gama baja de SAI están los **interactivos y los standby,** frente a la gama alta como son los **online**. Por ejemplo, los SAI online de **conversión Delta** son un tipo de SAI del alto rendimiento y estabilidad.

Tema de muestra. Esta Página está en blanco a propósito.

Independientemente del nivel RAID empleado, la capacidad del conjunto RAID es función del número de discos y del tamaño del disco más pequeño.

Se describen a continuación los niveles RAID más empleados en la práctica:

RAID 0 (**striping** sin tolerancia a fallos). No almacena información redundante y tiene un rendimiento muy elevado. Requiere al menos dos discos para su implementación. Tiene una fiabilidad muy baja, ya que si se estropea un disco se pierden todos los datos del conjunto.

RAID 1 (**mirroring**). Es muy fácil de implementar, proporciona una gran fiabilidad y la reconstrucción del disco averiado es rápida y sencilla. La velocidad de lectura puede llegar a ser el doble que con un disco. Requiere al menos dos discos para su implementación.

RAID 5 (**striping con paridad distribuida**). Almacena información redundante (paridad). Requiere al menos **tres discos** para su implementación. Cuando se estropea un disco la reconstrucción del mismo es costosa en tiempo y requiere de todos los discos del sistema.

RAID 10 (**mirroring de conjuntos RAID 0**). Es una combinación de los niveles 0 y 1. El rendimiento y la tolerancia a fallos son muy buenos, a expensas de un coste elevado, pues la sobrecarga es del 100 %. Para su implementación son necesarios al menos **4 discos**.

4.2.1. Almacenamiento en red

En entornos profesionales, los sistemas de almacenamiento externo compartidos en red son muy utilizados, es por lo que le hemos dedicado este apartado del tema. Los tipos que podemos encontrar son:

- **NAS** (Network Attached Storage): Tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un equipo (servidor) con otros (clientes), a través de una red, haciendo uso de un sistema operativo optimizado.
- **SAN** (Storage Area Network): Infraestructura telemática que suministra una conexión física y una capa de gestión, mediante la que se organiza las conexiones, y los elementos de almacenamiento. Obtiene un mejor rendimiento que el modelo NAS.

5. Gestión de redes seguras

La gestión interna de la red, pasa por dos puntos diferentes; por un lado, la securización de dispositivos y sistemas de la red (servidores y clientes) y la seguridad de la red en sí.

En este tema no se tratará la securización de dispositivos y sistemas por estar enfocado a servicios, por lo que se **tratarán técnicas de securización** de la red en sí.

Tema de muestra. Esta Página está en blanco a propósito.

Una red privada virtual (VPN) extiende una red privada a través de una red pública mediante un proceso de encapsulamiento o **tunelización** y permite a los usuarios enviar y recibir datos a través de redes públicas o compartidas como si sus dispositivos informáticos estuvieran conectados directamente a la red privada.

De esta forma la red privada virtual proporciona acceso a recursos que son inaccesibles en la red pública y, por lo general, se usa para trabajadores remotos.

El cifrado es común, aunque no es una parte inherente de una conexión VPN.

Una VPN se crea estableciendo una **conexión punto a punto virtual mediante el uso de circuitos dedicados o con protocolos de tunelización** sobre redes existentes.

Una VPN disponible desde la Internet pública puede proporcionar algunos de los beneficios de una red de área amplia (WAN). Desde la perspectiva del usuario, se puede acceder de forma remota a los recursos disponibles dentro de la red privada.

6. Seguridad perimetral.

6.1. Cortafuegos

En informática, **un firewall o cortafuegos** es un sistema de seguridad de red que supervisa y controla el tráfico de red entrante y saliente en función de reglas de seguridad predeterminadas. Un firewall generalmente establece una barrera entre una red confiable y una red que no es confiable, como Internet, permitiendo o denegando conexiones mediante las reglas preestablecidas por el sistema y por el administrador.

6.2. Proxy

Un servidor proxy es una interfaz de comunicación software, que se hace cargo de las peticiones y las transmite en calidad de representante a un ordenador de destino, **anonimizando la conexión**.

El servidor configurado como proxy se presenta, en este caso, como la única posibilidad de conexión con la red pública.

6.3. Proxy Inverso

Mientras que un proxy protege los dispositivos cliente en una red de las peticiones que ellos realizan contra Internet, un proxy inverso, por el contrario, trabaja de modo que **los proteja en sentido opuesto:** Uno o varios servidores web activan un servidor proxy de tales características como componente de seguridad adicional para que pueda hacerse cargo de las **solicitudes procedentes de Internet** y las transmita a un servidor en concreto, de varios que pueda tener la empresa en su zona desmilitarizada (DMZ).

Una combinación así hace posible controlar el tráfico de datos entrante, poner a disposición varios servidores bajo la misma URL, **distribuir solicitudes** de manera simultánea por diferentes servidores

Tema de muestra. Esta Página está en blanco a propósito.

Simplicidad

Hay dos razones por las que la simplicidad es una estrategia de seguridad: la primera es que, haciendo las cosas simples, se comprenden más fácilmente y la segunda es que cuanto más complejo sea algo, más cosas puede ocultar.

Defensa por capas

Los riesgos potenciales de Internet se producen en varios niveles, por lo que **una única línea de defensa no es suficiente**. En lugar de reforzar la defensa en un único punto, la estrategia de defensa por capas aplica varias líneas de defensa consecutivas y distribuidas físicamente.

8. Conclusión.

Proteger las comunicaciones es de gran importancia para preservar la integridad de la información de cualquier ordenador aislado o en red.

Los servicios de seguridad y **bastionado de redes**, son cada vez más necesarios y más demandados a nivel personal y empresarial, por lo que su conocimiento en profundidad se hace imprescindible para el alumnado en diversas asignaturas y módulos relacionados con la gestión y uso de redes informáticas.

Un conjunto de **buenas prácticas de seguridad**, así como el uso de **distintas estrategias**, minimizarán el riesgo de sufrir daños por robo de datos o modificación de los mismos sin autorización.

8.1. Relación con el Currículo

Este tema es aplicado en el aula en los módulos profesionales siguientes, con las atribuciones docentes indicadas (PES/SAI):

- FP Básica
  - TPB en Informática de Oficina
    - (PES/SAI) IMRTD Instalación y mantenimiento de redes para transmisión de datos
  - TPB en informática y Comunicaciones
    - (PES/SAI) IMRTD Instalación y mantenimiento de redes para transmisión de datos
- GRADO MEDIO
  - Técnico en Sistemas Microinformáticos y Redes
    - (PES/SAI) SOR - Sistemas operativos en red
    - (PES) REDL - Redes locales
- GRADO SUPERIOR
  - TS en Administración de Sistemas en Red
    - (PES) PAR - Planificación y administración de redes
    - (PES) SRI - Servicios de red e Internet

- CURSOS DE ESPECIALIZACIÓN
  - CE Ciberseguridad TIC
    - (PES/SAI) Bastionado de Redes y Sistemas

9. Bibliografía

- Alberto León-García, Indra Widjaja; "**Redes de Comunicación**". Primera edición. 2001. Ed. Me Graw Hill
- William Stallings.; "**Comunicaciones y Redes de Computadores**". sexta edición. Ed. Prentice-Hall. 2000.
- Andrew S. Tanenbaum; " **Redes de computadores**". Ed. Prentice-Hall. 2003.
- Kurose, James; Ross, Heith; **"Redes de computadoras: un enfoque descendente"** Ed. Pearson 2017
- Carlos Álvarez y Pablo González: "**Hardening de servidores GNU / Linux**" Ed. 0xW0RD 2021