SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.8.1. Capítulo 8
Parte 2 de 2

Robustecimiento de sistemas

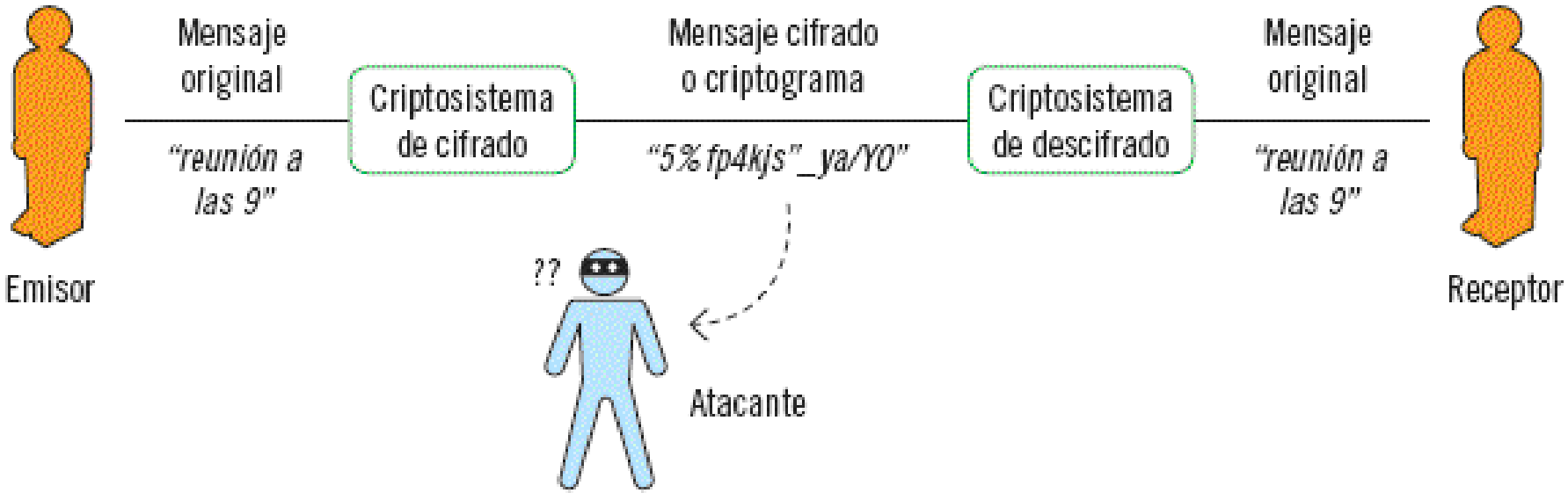
JOSÉ PABLO HERNÁNDEZ

5. CONFIGURACIÓN DE LOS SISTEMAS DE INFORMACIÓN

Muchos de los servicios más habituales que se prestan a través de internet no son seguros, en tanto en cuanto la información que se envía no viaja cifrada.

Para mejorar la seguridad en el aspecto de la confidencialidad de los servicios prestados sobre internet (que es una red pública no fiable), se recurre al empleo de mecanismos que cifren la información intercambiada, de manera que, si un atacante obtuviera acceso al tráfico, tendría que descifrar la información para acceder a ella.

Protección de la información mediante su cifrado y su descifrado, usando un criptosistema



5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

La **criptografía** es la ciencia que estudia cómo proporcionar comunicaciones seguras a través de canales inseguros.

Para que el intercambio de un texto entre dos personas sea seguro, el texto se cifra, de manera que el texto obtenido o **criptograma** resulte ilegible para quien no sepa realizar el proceso inverso: el de descifrarlo para recuperar el texto original.

El proceso completo de cifrado y descifrado se realiza mediante un **criptosistema**, que define los **algoritmos** (o procedimientos) y las **claves** (o parámetros del algoritmo) necesarios para transformar una información en otra.

Hay que mantener secreto el algoritmo o procedimiento, y/o sus claves.

5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

La **criptografía** es la ciencia que estudia cómo proporcionar comunicaciones seguras a través de canales inseguros.

Para que el intercambio de un texto entre dos personas sea seguro, el texto se cifra, de manera que el texto obtenido o **criptograma** resulte ilegible para quien no sepa realizar el proceso inverso: el de descifrarlo para recuperar el texto original.

El proceso completo de cifrado y descifrado se realiza mediante un **criptosistema**, que define los **algoritmos** (o procedimientos) y las **claves** (o parámetros del algoritmo) necesarios para transformar una información en otra.

Hay que mantener secreto el algoritmo o procedimiento, y/o sus claves.

Los criptosistemas se dividen en dos tipos, según la naturaleza de sus claves o parámetros:

- Criptosistemas de clave simétrica o de clave secreta
- Criptosistemas de clave asimétrica o de clave pública.

5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

Criptosistemas de clave simétrica o de clave secreta

Son aquellos en los que la clave que se emplea para cifrar y descifrar la información es la misma, es decir, emplean una clave que de antemano es conocida por el emisor y el receptor del mensaje (de ahí el nombre de simétrico). Por lo tanto, la clave debe permanecer secreta, porque de conocerse se puede descifrar la información.

Estos sistemas son sencillos, y por lo tanto se usan frecuentemente, sin embargo, no se emplean habitualmente en procesos de autenticación, porque requieren que emisor y receptor se intercambien la clave secreta por una vía segura (de la que precisamente no disponen si solo tienen acceso a internet).

5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

Criptosistemas de clave asimétrica o de clave pública

Son aquellos en los que se emplea una clave que conoce todo el mundo (por lo tanto es pública), que pertenece al receptor del mensaje; de manera que todos los emisores que quieran enviarle un mensaje al receptor emplean esa clave para cifrar la información.

Para descifrar la información, el receptor dispone de una segunda clave que solo él conoce (por lo tanto esa es privada), de manera que solo él puede descifrar la información. Si un atacante captura un mensaje cifrado que se ha enviado a un receptor, no podrá descifrarlo, porque carece de la clave secreta para ello, que solo conoce el receptor lícito del mensaje.

5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

Firma electrónica: Se trata del "conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medios de identificación del firmante", según la Ley 59/2003. Este es por tanto un concepto jurídico y un método de identificación, equivalente o análogo a la firma manuscrita.

Firma digital: Es el conjunto de caracteres que se añaden al final de un documento o cuerpo de un mensaje para informar, dar fe o mostrar validez y seguridad.

Identifica a la persona emisora de dicho mensaje

Certificar la veracidad de que el documento no se ha modificado con respeto al original.

No se puede negar haberlo firmado, puesto que esta firma implica la existencia de un certificado oficial emitido por un organismo o institución que valida la firma y la identidad de la persona que la realiza.

La firma digital se basa en los sistemas de **criptografía de clave pública** (PKI – Public Key Infrastructure) que satisface los requerimientos de definición de firma electrónica avanzada.

5.1. CRIPTOSISTEMAS DE CLAVE SECRETA Y CRIPTOSISTEMAS DE CLAVE PÚBLICA

Certificado electrónico o digital: Este documento o fichero informático es el que una persona física o jurídica utiliza para identificarse en la red, autenticada por un tercero o autoridad certificador y la aplicación automática de un algoritmo matemático que asocia la identidad al mensaje o documento. El ejemplo más popular es el **DNI electrónico**.

Firma digitalizada: A pesar de que muchas personas la confunden con la firma digital, no tiene nada que ver. Este término alude a la simple representación gráfica de la firma manuscrita obtenida a través de un escáner, que puede ser insertada en cualquier documento

5.2. PROTOCOLOS SEGUROS

El empleo de criptosistemas otorga seguridad a las comunicaciones y servicios, en mayor o menor medida, según la complejidad de las medidas técnicas aplicadas:

- Cifrado simétrico o asimétrico.
- Firmas electrónicas.
- Certificados digitales.

Los diferentes protocolos de los servicios de internet hacen uso de estas técnicas, de manera que se obtienen sus variantes seguras.

Para servicios específicos, debe investigarse siempre qué soluciones existen disponibles, y en la medida de lo posible, elegir siempre servicios protegidos mediante cifrado; preferiblemente asimétrico, y con empleo de certificados digitales

5.2. PROTOCOLOS SEGUROS

HTTPS en lugar de HTTP

HTTPS (Hypertext Transfer Protocol Secure) es el resultado de añadir al protocolo HTTP estándar para navegación web las prestaciones de cifrado SSL (Secure Socket Layer), y de su sucesor TLS (Transport Layer Security), que son protocolos de la capa de transporte.

Esta combinación permite asegurar que el servicio lo ofrece un servidor web auténtico (no un impostor) y que las comunicaciones con este servidor están protegidas.

Se emplea un mecanismo de cifrado asimétrico, con una clave pública y una clave privada.

El servidor HTTPS debe tener un certificado digital X.509, firmado por una autoridad de certificación, de forma que el navegador web del cliente que se conecta lo acepte para emplearlo.

A partir de esta clave pública, y de otra información que aporta el cliente, se genera en ambos extremos una clave privada, que es la que se emplea para el cifrado simétrico de las comunicaciones.

5.2. PROTOCOLOS SEGUROS

ESMTP en lugar de SMTP

Las comunicaciones SMTP no van protegidas por cifrado alguno, lo que ofrece un problema de confidencialidad e integridad.

Para solucionarlo, se define ESMPT (Enhanced Simple Mail Transfer Protocol), que en la RFC 3207 define cómo emplear SMTP sobre la capa de transporte seguro TLS, para ofrecer un servicio protegido.

Nótese que esto no soluciona el problema de la autenticidad del remitente, necesaria para protegerse del spam.

En este sentido existen muchas propuestas, como SMTP–AUTH, pero en general, su implementación no está estandarizada en los servidores SMTP, lo que dificulta una verdadera protección frente a esta amenaza.

5.2. PROTOCOLOS SEGUROS

Los protocolos de transporte seguro SSL y TLS permiten la implementación segura de los servicios de la capa de aplicación (HTTPS, SMTPS, NNTPS, etc.)

Modelo TCP/IP (RFC 1122)

APLICACIÓN	HTTP, SMTPS, FTPS, NNTPS, ...
TRANSPORTE	SSL, TLS
	TCP, UDP
INTER-RED	IP
ACCESO	PPP

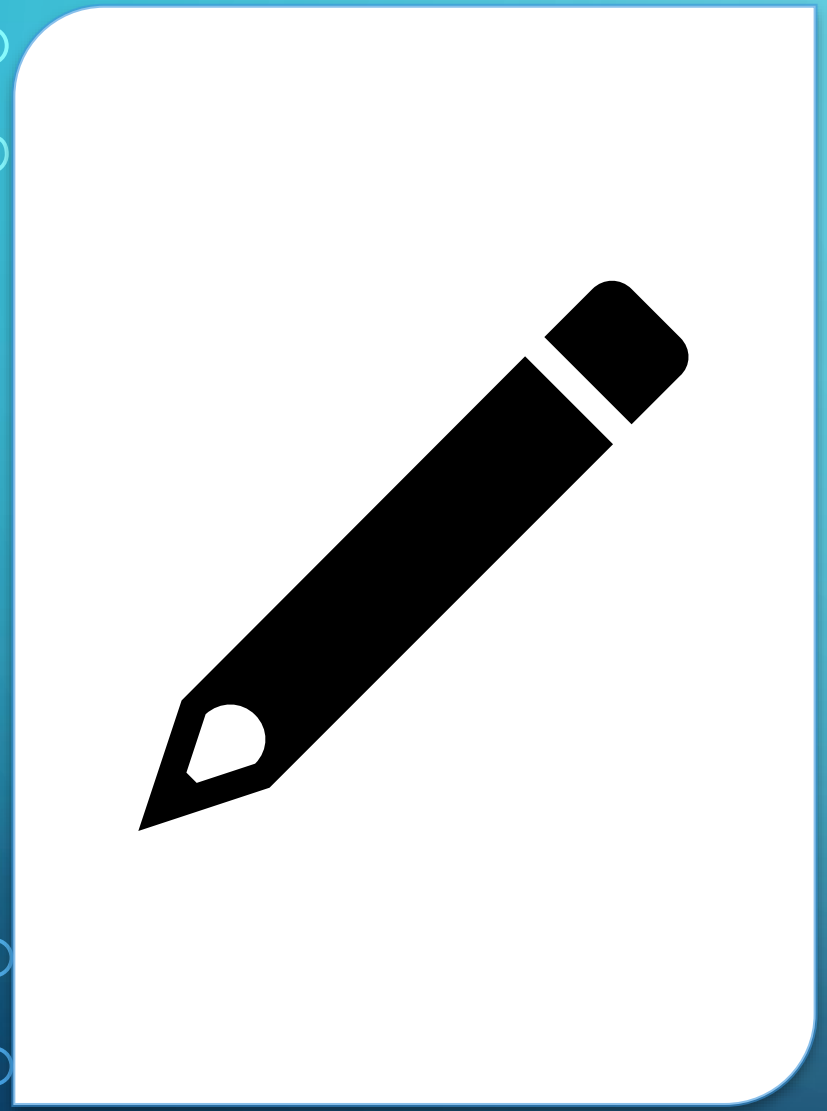
Protocolo	Comentario	Puerto
https	HTTP sobre SSL	TCP 443
smtps	SMTP sobre SSL	TCP 465
ftps	FTP sobre SSL	TCP 989,990
nntps	NNTP sobre SSL	TCP 563
ldaps	LDAP sobre SSL	TCP 646
...		

Actividades

EN EL DISEÑO DE UN SERVICIO DE EXTRANET (ES DECIR, DE ACCESO DESDE INTERNET A LA RED PRIVADA DE LA EMPRESA DESDE LA QUE RESULTEN ACCESIBLES LAS APLICACIONES CORPORATIVAS, GENERALMENTE A TRAVÉS DE UN PORTAL WEB), SE CONTEMPLAN DOS OPCIONES:

OPCIÓN 1. UN SERVIDOR HTTPS PARA PRESENTAR LA APLICACIÓN AL USUARIO, Y UN SERVIDOR SFTP PARA EL INTERCAMBIO SEGURO DE ARCHIVOS; Y ADEMÁS, MANTENER EL ACCESO A TRAVÉS DE UN PUERTO PRIVADO A LA BASE DE DATOS, EMPLEANDO USUARIOS Y CONTRASEÑAS SIN CIFRAR.

OPCIÓN 2. UN SERVIDOR HTTPS QUE INCORPORA UNA APLICACIÓN PARA SUBIR Y BAJAR ARCHIVOS (SIMULANDO UN SERVIDOR FTP), Y EMPLEAR SSH PARA QUE LOS USUARIOS ACCEDAN A LA RED INTERNA, Y DESDE AHÍ A LA BASE DE DATOS.



Actividades

SOLUCIÓN

LA OPCIÓN 1 ES SENCILLA, Y PROBABLEMENTE SEA MÁS RÁPIDA, PERO TIENE EL INCONVENIENTE DE EMPLEAR 3 SERVICIOS (UNO MÁS QUE LA OPCIÓN 2), Y SOBRE TODO, TIENE EL PROBLEMA DE QUE LAS CREDENCIALES DE ACCESO A LA BASE DE DATOS VIAJAN POR INTERNET SIN CIFRARSE, LO QUE LA DESCARTA.

LA OPCIÓN ELEGIDA ES LA 2, PORQUE SI BIEN ES MÁS COMPLEJA, OFRECE MÁS SEGURIDAD, YA QUE PARA ACCEDER A LA BASE DE DATOS SE EMPLEA EL PROTOCOLO SEGURO SSH, PARA CONECTARSE A LA BASE DE DATOS.

6. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS

Aunque se minimice el número de servicios implementados, y se empleen protocolos seguros, las funciones prestadas presentan vulnerabilidades.

Estas vulnerabilidades, cuando son descubiertas, suponen un riesgo para el sistema de información que lo implementa.

El fabricante trabaja activamente para corregir la debilidad de su producto, y poner a disposición de sus usuarios el parche o corrección que deben aplicar para subsanar el problema.

El usuario debe aplicar el parche para robustecer su sistema de información.

6.1. ACTUALIZACIÓN DE PARCHES

La norma ISO 17799:2005 establece:

Objetivo de control 12.6 la gestión de la vulnerabilidad técnica de manera sistemática y efectiva:

Única contramedida la 12.6.1, relativa al control de las vulnerabilidades técnicas.

Indica que se debe obtener información oportuna sobre las debilidades de los sistemas de información que se estén usando, porque es necesario para adoptar las medidas según los riesgos asociados.

Para ello, se debe partir de un inventario actualizado y completo de las aplicaciones que detalle el fabricante, las versiones, y las personas responsables de la aplicación.

6.1. ACTUALIZACIÓN DE PARCHES

La norma recomienda que se establezca un procedimiento formal de gestión de las vulnerabilidades:

- Búsqueda activa de información, y monitorización de aparición de nuevas vulnerabilidades
- Establecimiento de un cronograma, para reaccionar a las nuevas vulnerabilidades aparecidas.
- La evaluación del riesgo vinculado a la vulnerabilidad aparecida para determinar las acciones a emprender, como aplicar un parche, o corrección a la aplicación. Dependiendo de la urgencia según el procedimiento de cambios estándar de las aplicaciones (control 12.5.1), o actuando ante un incidente de seguridad (control 13.2).
- Se debe considerar el riesgo de aplicar un parche frente al de no aplicarlo. Antes de aplicarlo, preferiblemente se debería probar y evaluar su efectividad, y ausencia de efectos secundarios.
- Otros controles alternativos a la aplicación de un parche pueden ser:
  - Desconectar servicios relacionados con la vulnerabilidad.
  - Agregar controles como firewalls en el perímetro de seguridad.
  - Reforzar la monitorización para detectar o evitar ataques.
  - Mantener registros de auditoría de los procedimientos realizados.
  - Revisión y evaluación del proceso de gestión de vulnerabilidades.
  - Atender primero los sistemas de mayor riesgo.

6.2. DIRECTRICES EN GUÍAS NIST

La guía NIST 800-123, en su apartado 4.1, indica que una vez que la aplicación servidor ha sido instalada, es esencial aplicar los parches para corregir las vulnerabilidades conocidas, antes de que el sistema sea accesible o entre en producción. Para ello, los administradores del servidor deberían:

- Seguir un procedimiento organizado para aplicar actualizaciones.
- Reducir las vulnerabilidades como sea posible, hasta que haya un parche disponible.
- Identificar vulnerabilidades y aplicar los parches oportunos.
- Instalar correcciones de manera permanente (paquetes de mejora, mejoras
- Instalar correcciones de manera permanente (paquetes de mejora, mejoras del producto o upgrades, nuevas versiones, etc.)

6.2. DIRECTRICES EN GUÍAS NIST

Los administradores deben velar porque el servidor esté protegido durante el proceso de aplicación del parche, porque en esta fase podría verse especialmente comprometido. Para ello, la norma NIST recomienda:

- Desconectar el servidor de la red, o mantenerlo solo conectado a una red segura, mientras que los parches se copian e instalan.
- Colocar el servidor en una VLAN, donde los accesos al servidor sean los necesarios para llevar a cabo la aplicación del parche.
- No devolver el servidor a su funcionamiento en la red normal hasta que el parche y su verificación hayan terminado.
- Copiar los parches mediante un mecanismo fuera de línea, por ejemplo, usando un CD o una unidad de almacenamiento USB.
- Los parches deberían probarse antes de aplicarse, especialmente en servidores de producción. Para ello, se debe disponer de un entorno de prueba idéntico al de producción, donde chequear que el parche no genera problemas adicionales.
- Aunque los servidores se pueden configurar para que descarguen automáticamente los parches, no deberían configurarse para que los instalen automáticamente, para permitir que se prueben antes.

6.3. DIRECTRICES EN GUÍAS CIS

Para sistemas operativos Linux, CIS recomienda en la guía de comparación de seguridad v.1.0.5 para Linux, instalar los últimos parches al sistema operativo. Esto es un punto fundamental para robustecer un servidor, y se destaca entre sus primeras medidas (apartado 1.1).

También para sistemas operativos Windows, CIS recomienda en su guía v.2.1 configurar el sistema para que se apliquen automáticamente las actualizaciones automáticas (1.1.1.1.8), lo que abarca tanto los paquetes de mejoras y correcciones de mayor envergadura, como los parches y correcciones menores que el fabricante haga disponibles.

7. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO

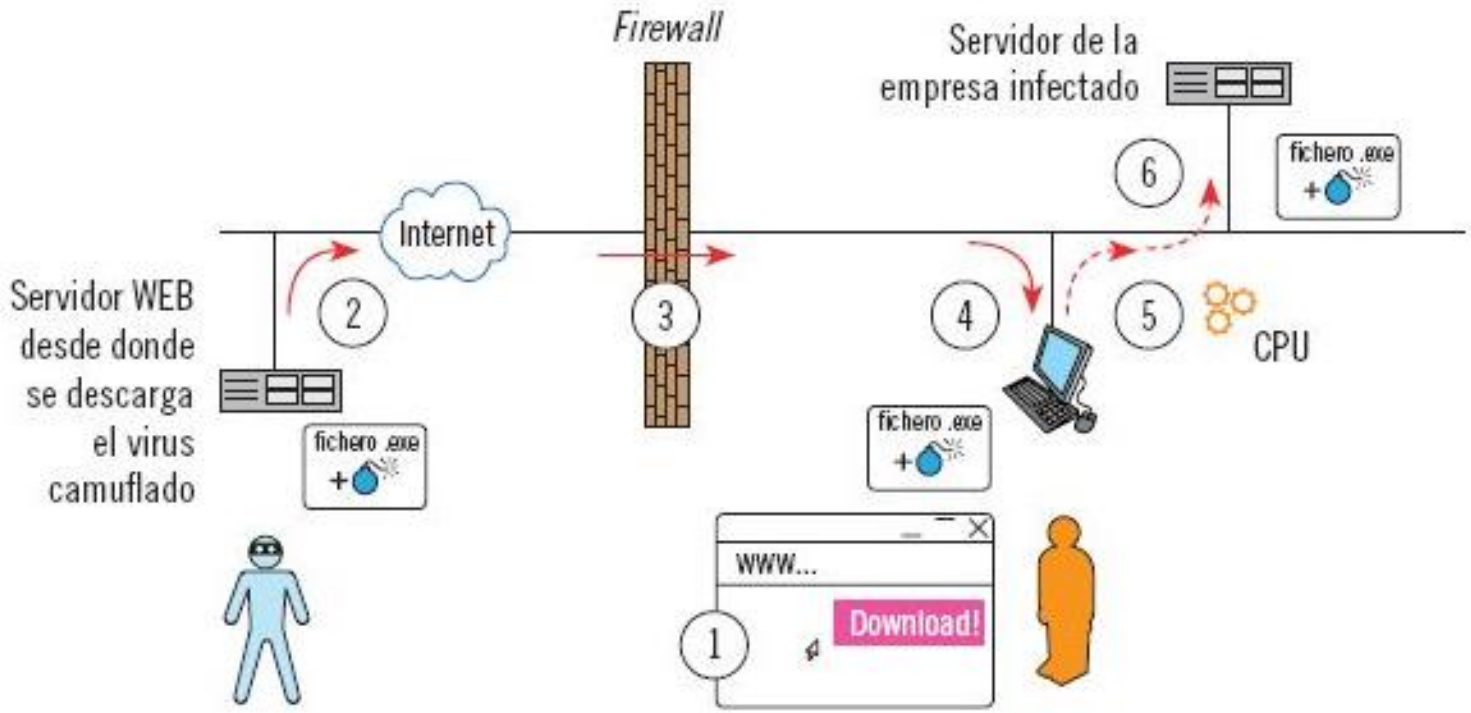
El código malicioso es una amenaza constante para los sistemas de información.

Se trata de aplicaciones que, una vez ejecutadas, producen un daño intencionado al sistema de información; por ejemplo, proporcionan una vía de acceso a un atacante, borran un archivo, o lo envían a un servidor remoto.

7.1. ATAQUE DE CÓDIGO MALICIOSO

Para que la amenaza del código malicioso se materialice, debe ocurrir que llegue a un equipo de la red, y que sea ejecutada por el mismo. Las salvaguardas se aplicarán con carácter preventivo, tanto para evitar que el código entre al sistema, como para evitar que una vez dentro sea ejecutado.

Infección por código malicioso: (1) el usuario descarga un archivo con un virus, (2) que se envía desde el servidor que propaga el virus, (3) que no es detectado por el firewall de la empresa. (4) El archivo se guarda en el disco duro, (5) es ejecutado, y el virus se activa, propagándose (6) al servidor de la empresa



7.1. ATAQUE DE CÓDIGO MALICIOSO

La vía de acceso al sistema de información puede ser

- la red externa o internet
- bien un medio de almacenamiento como un CD-ROM, o unidad USB

Deben aplicarse sistemas que detecten los códigos maliciosos en todos los puntos de conexión a internet, y en todos los equipos que admitan medios de almacenamiento externo.

Esta detección es compleja, porque el código malicioso puede formar parte de otra aplicación lícita, o bien transportarse de manera cifrada, a lo que se suma la dificultad de la enorme variedad de software malicioso existente.

Resulta inevitable penalizar el rendimiento del sistema que debe escudriñar un conjunto de instrucciones antes de su ejecución.

7.1. ATAQUE DE CÓDIGO MALICIOSO

ISO 17799:2005

Objetivo de control “10.4 Protección contra el código malicioso y móvil”, que persigue mantener la integridad del software, y la introducción de código no autorizado, articulando en particular el control “10.4.1 Controles contra código malicioso”:

- Una política formal, que prohíba el uso de software no autorizado.
- Establecer una política formal respecto a la obtención de software, desde redes externas u otros medios.
- Realizar revisiones regulares de las aplicaciones y archivos de los sistemas críticos, investigando la presencia de aplicaciones o modificaciones no autorizadas.
- La instalación y actualización regular de software específico, para la detección de código malicioso como medida preventiva, y los chequeos rutinarios de: cualquier archivo recibido antes de ejecutarlo, todos los adjuntos de los correos electrónicos (tanto en los servidores de correo como en las computadoras), y también de las páginas web, para detectar código malicioso.
- La definición de procedimientos y responsabilidades, para la protección frente a código malicioso.
- La preparación de planes apropiados, para la continuidad del negocio en caso de la materialización de un ataque por código malicioso.
- Mantenerse informado, por ejemplo, mediante subscripción a boletines de noticias de seguridad, de los códigos maliciosos nuevos.
- Verificar la información relacionada con códigos maliciosos nuevos, diferenciando, por ejemplo, amenazas reales de bromas pesadas.

7.2. TIPOS DE CÓDIGO MALICIOSO

Es código malicioso (malware) toda aplicación que sin conocimiento ni autorización del usuario genera un daño intencionado al sistema.

Su clasificación suele realizarse por su forma de propagación, y por el daño que producen.

Casi todo el código malicioso comparte una característica común: se trata de aplicaciones capaces de copiarse a sí mismas de manera similar a un virus.

7.2. TIPOS DE CÓDIGO MALICIOSO

En base a su capacidad de propagación se encuentran:

Virus, que infectan a otros ficheros ejecutables (aplicaciones convencionales, controladores de dispositivos), o con alguna capacidad de ejecución (algunos tipos de documentos que incluyen parte de información correspondiente a acciones ejecutables, como macros o repeticiones de tareas).

Gusanos, que no infectan a otros ficheros ejecutables sino que constituyen un fichero por sí mismo. Persiguen como objetivo su máxima propagación, empleando para ello vías como el correo electrónico, redes de intercambio de ficheros, aplicaciones de mensajería, y aplicaciones de conversación o chat.

Troyanos, carecen de mecanismo propio de replicación, y suelen propagarse al visitar una página web, estando incluidos en otras aplicaciones aparentemente inofensivas, o al ser descargados por un programa malicioso que ya exista en el sistema.

7.2. TIPOS DE CÓDIGO MALICIOSO

En base al daño que producen, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) ofrece la siguiente clasificación:

Aplicaciones que muestran publicidad no deseada (en inglés **adware**)

Bloqueador, que impiden la ejecución de determinados programas

Bombas lógicas, que actúan bajo una circunstancia programada, por ejemplo una fecha, o bajo control remoto.

Broma (en inglés joke), que al ejecutarse hace pensar al usuario que el ordenador se va a borrar, que está averiado, etc.

Bulo (en inglés hoax), que en forma de correo electrónico engaña al destinatario en relación a la existencia de un nuevo virus, o alguna otra información, solicitándole que lo reenvíe a todos sus contactos.

Capturador de teclado (en inglés **keylogger**), que registra todas las pulsaciones logrando así obtener las claves de acceso a los servicios.

Redireccionador (en inglés clicker), que redirecciona el navegador web del usuario a una página en concreto, por ejemplo, a una página falsa de un banco, u otros servicios, como el correo electrónico.

Criptovirus (en inglés **ransomware**), que cifran un fichero y coaccionan al usuario a que pague un rescate para descifrarlos.

Descargador (en inglés **downloader**), que acceden a internet para descargar otros programas normalmente maliciosos.

7.2. TIPOS DE CÓDIGO MALICIOSO

En base al daño que producen, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) ofrece la siguiente clasificación:

Espía (en inglés, **spyware**), que envían información del equipo a un equipo remoto

Que explotan una vulnerabilidad (en inglés **exploit**).

Fraude, que simulan un comportamiento anormal, e incitan a la compra.

Instalador (en inglés **dropper**), que permite la instalación de otros códigos maliciosos en el sistema

Ladrón de contraseñas (en inglés **password stealer**), que accede a ficheros conocidos del sistema, donde se registran usuarios y sus contraseñas para enviarlos al atacante.

Marcador (en inglés **dialer**), que aprovechan las conexiones a internet vía modem que hacen marcado telefónico, para hacer llamadas a números de cobro adicional.

Puerta trasera (en inglés **backdoor**), que permite el acceso al sistema operativo, aplicación o página web, eludiendo los controles de acceso que haya. La finalidad es obtener información, acceder a los ficheros, reiniciar el ordenador, etc.

Herramientas de control total (en inglés **rootkit**), que permiten al atacante tomar el control del sistema como su administrador (en Linux el usuario root), permitiendo al atacante remoto hacer lo que desee.

Secuestrador del navegador (en inglés browser **hijacker**), que modifica la página de inicio del navegador, añade barras de botones, modifica las direcciones de páginas más visitadas o favoritos, generalmente con la finalidad de aumentar las visitas a una página determinada.

7.3. DIRECTRICES EN GUÍAS NIST

La guía NIST 800-123, en su apartado 4.3, indica que normalmente los sistemas operativos y las aplicaciones no incluyen las medidas de control necesarias para proteger el sistema de las aplicaciones maliciosas, por lo que es necesario añadir al sistema medidas adicionales, en forma de:

- Aplicaciones específicas contra software malicioso, como aplicaciones antivirus, aplicaciones anti-espías, y detectores de rootkit, que permitan detectar y erradicar las infecciones que puedan ocurrir.
- Aplicaciones de detección y prevención de intrusiones (en inglés Intrusion detection and prevention software, IDPS) para detectar ataques dirigidos contra el servidor. Estas aplicaciones deben poder detectar, por ejemplo, ataques de denegación de servicio (en inglés Deny of Service, DoS) en los que el sistema se ve atacado porque recibe una cantidad de peticiones muy superior a su capacidad, lo que puede conllevar o su bloqueo, o su dedicación exclusiva a rechazar peticiones, sin poder atender ninguna.
- Aplicaciones de chequeo de la integridad de los archivos, que detecten cuando un fichero crítico ha cambiado.
- Aplicaciones de cortafuegos (firewalls) instalados en el equipo, para protegerlo de accesos no autorizados.
- Aplicaciones de gestión de actualizaciones o correcciones, que faciliten que las nuevas vulnerabilidades se atienden de manera temprana. Estas aplicaciones se pueden emplear para aplicar las correcciones y también para identificar las vulnerabilidades en el sistema operativo, servicios y aplicaciones.

7.4. DIRECTRICES EN GUÍAS CIS

CIS en la guía v.1.0.5 para Linux y dentro de su apartado 10, incluye recomendaciones sobre aplicaciones antivirus, indicando que es muy recomendable que se instalen, especialmente en los servidores de correo y en los servidores de ficheros, para proteger a los clientes de sus servicios

Actividades

LA RED DE UNA EMPRESA ESTÁ FORMADA POR UN FIREWALL QUE PROTEGE DE INTERNET A UN SERVIDOR Y 30 ESTACIONES DE TRABAJO. LA RED HA SUFRIDO UN ATAQUE DE CÓDIGO MALICIOSO MEDIANTE UN GUSANO, QUE SE HA REENVIADO POR CORREO DESDE LAS ESTACIONES DE TRABAJO A TODAS LAS DIRECCIONES DE LAS AGENDAS. EL FIREWALL SOLO HA DETECTADO EL INCREMENTO DE TRÁFICO SALIENTE, A RAÍZ DE LO CUAL HA CORTADO TODAS LAS CONEXIONES ENTRANTES Y SALIENTES.

INDICAR QUÉ OTRAS MEDIDAS PREVENTIVAS ESPECÍFICAS PARA EL CÓDIGO MALICIOSO DEBERÍAN APLICARSE EN LAS ESTACIONES DE TRABAJO, EN EL SERVIDOR, E INCLUSO EN EL FIREWALL.

Actividades

SOLUCIÓN

EL FIREWALL ESTABA BIEN CONFIGURADO, Y HA FUNCIONADO CORRECTAMENTE COMO MEDIDA DE DETECCIÓN Y COMO MEDIDA DE EMERGENCIA, EVITANDO QUE EL DAÑO GENERADO POR EL INCIDENTE FUERA MAYOR; POR EJEMPLO, SE HA LOGRADO CONTENER LA POTENCIAL PÉRDIDA DE IMAGEN DE LA EMPRESA.

SIN EMBARGO, SE DEBEN APLICAR MEDIDAS PREVENTIVAS, COMO LAS SIGUIENTES:

INSTALAR UN ANTIVIRUS EN EL FIREWALL, O SI NO ES POSIBLE, AÑADIR UN EQUIPO QUE HAGA ESTAS FUNCIONES DE ANTIVIRUS PARA LAS COMUNICACIONES.

INSTALAR UN ANTIVIRUS EN EL SERVIDOR.

INSTALAR UN ANTIVIRUS EN TODAS LAS ESTACIONES DE TRABAJO.

REVISAR LOS PERMISOS PARA CARGAR MEDIOS DE ALMACENAMIENTO EXTRAÍBLE (CD ROM Y USB) EN TODAS LAS ESTACIONES DE TRABAJO. SE DEBE REVISAR QUE LA CONFIGURACIÓN SE HAGA EXCLUSIVAMENTE EN BASE A LA OBLIGATORIA NECESIDAD DE HABILITAR ESTOS MEDIOS, PARA EL CUMPLIMIENTO DE LAS FUNCIONES DEL PUESTO.

8. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA

La red de comunicaciones de la empresa es la infraestructura que interconecta aquellos elementos que precisan intercambiar información, habitualmente estaciones de trabajo, clientes, servidores, impresoras para la salida de documentación impresa, y quizás escáner, para la entrada de documentos por red.

La generalización de las redes TCP/IP hace que se puedan conectar otros muchos dispositivos a la red, por ejemplo, cámaras web, dispositivos de reproducción multimedia, unidades de disco de red, y todo tipo de sistemas del ámbito industrial que admitan gestión TCP/IP.

8.1. PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

Como medida principal, conviene recordar el control “11.4.5 Segregación en redes”, que indica que los servicios, sistemas, y usuarios, se deben segregar en redes diferentes, que se pueden entender como redes físicamente separadas, o como redes lógicamente separadas, empleando redes virtuales diferentes (VLAN diferentes que se deben configurar en los switchers de red).

Esta medida es básica, y siempre debe observarse, porque aumenta la seguridad de los servicios de cada subred.

8.1. PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

Se pueden crear diferentes tipos de VLAN:

VLAN de nivel 1 por puerto: un conjunto de puertos del switcher forma la VLAN.

VLAN de nivel 2 por MAC: se definen los miembros por su dirección MAC.

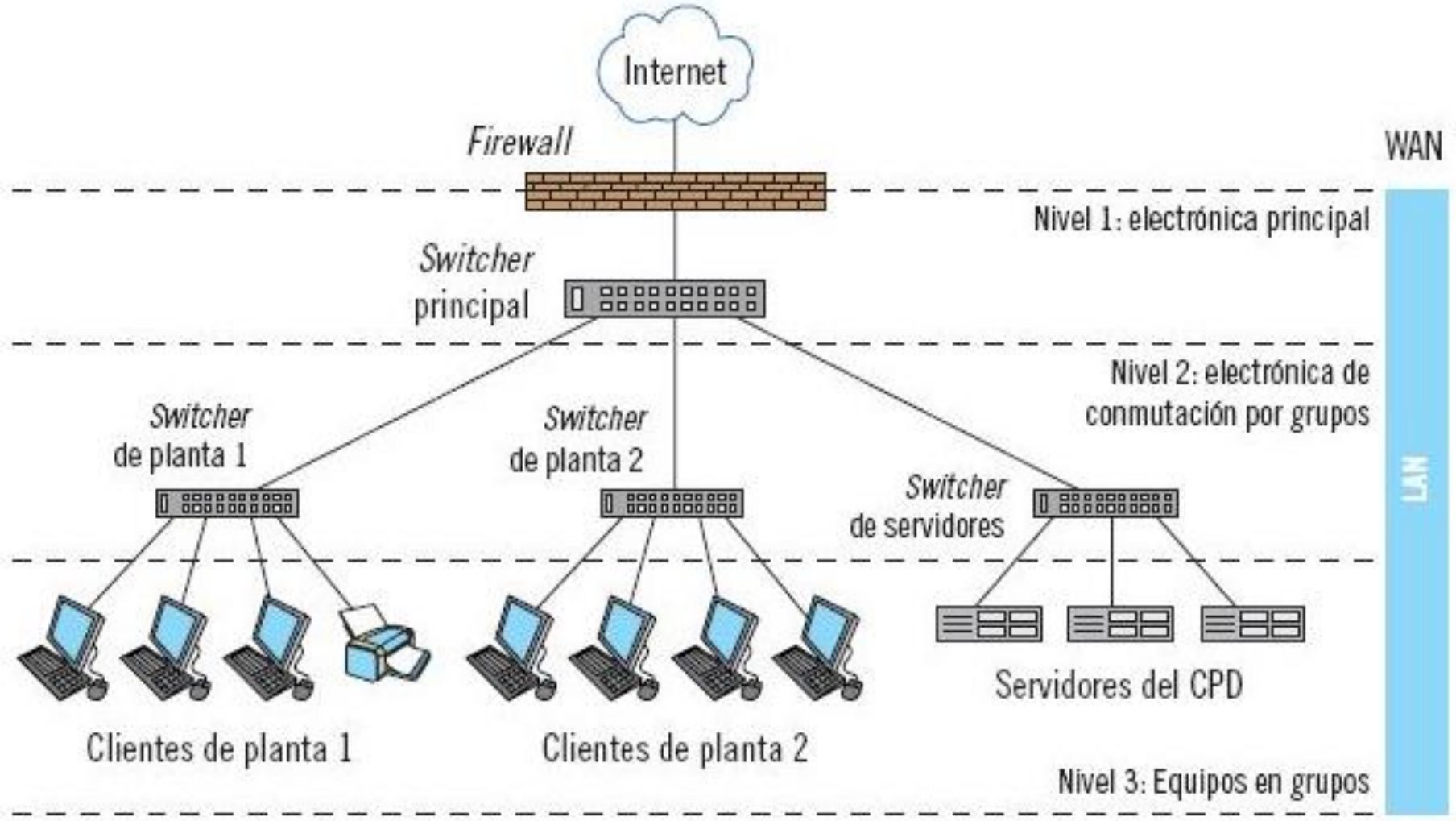
VLAN de nivel 2 por protocolo de red: los equipos que usan un mismo protocolo de red (IPv4, IPv6, etc.) forman una VLAN.

VLAN de nivel 3 por direcciones de red: un ordenador puede ser de distintas VLAN si tiene diferentes direcciones de red.

VLAN para niveles superiores: todos los equipos que usan FTP pertenecen a la misma VLAN, todos los que usan HTTP pertenece a la misma VLAN, etc.

8.1. PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

Diagrama de una red sencilla y típica en una empresa, en tres niveles con salida a internet



8.1. PROTECCIÓN DE LAS COMUNICACIONES: SEPARACIÓN Y OTRAS MEDIDAS

La norma ISO 17799:2005 establece el objetivo “10.6 Gestión de seguridad de red”, para asegurar la protección de la información en redes y la protección de la infraestructura.

El control “10.6.1 Controles de red”, en el que se indica que las redes se deben proteger de accesos no autorizados, mediante las siguientes medidas:

- Que haya responsables separados para la gestión de redes y para la gestión de los equipos de cómputo, cuando sea posible.
- Asignar responsabilidades y procedimientos para la gestión de los equipos remotos y las estaciones de trabajo que se conectan a la red.
- Establecer medidas especiales, de cara a preservar la confidencialidad e integridad de los datos que emplean redes públicas, y las medidas que correspondan para una adecuada disponibilidad de los equipos de red y computadoras conectadas.
- Realizar un registro y monitorización adecuada de las comunicaciones.
- La aplicación de controles debe ser consistente en toda la infraestructura, y ser acorde con el servicio que se debe entregar a la organización.

8.2. CIFRADO DE LAS COMUNICACIONES: IPSEC

Es un protocolo de la capa de inter-red, que aporta seguridad al protocolo IP, añadiéndole posibilidades de cifrado. Al operar en la capa de inter-red, aporta seguridad a todos los protocolos superiores (principalmente a los protocolos de transporte TCP/UDP), sin necesidad de modificación alguna, ya que todo se gestiona y configura a nivel de red.

Esta es una ventaja notable frente a otros protocolos que permiten el cifrado, como SSL y TSL, ya que estos operan en la capa de transporte, por lo que las aplicaciones y servicios deben estar programados y adaptados para ello.

Por el contrario, a priori cualquier aplicación funcionará con IPsec, sin modificación alguna.

IPsec soporta dos modos de funcionamiento:

- **El modo transporte**, orientado a comunicaciones de ordenador a ordenador, en el que solo se cifra el contenido del paquete, y la cabecera se mantiene intacta como en el protocolo IP. El empleo de este protocolo cuando los extremos están separados por encaminadores (routers), puede requerir de alguna configuración especial, en lo referente a la traducción de direcciones de red (NAT, Network Address Translation).
- **El modo túnel**, orientado a comunicaciones red a red, en el que se cifra completamente el paquete (incluida su cabecera) y el resultado se considera como la información útil de un nuevo paquete IP, que se procesa normalmente. Esto se emplea sobre todo para las comunicaciones a través de internet o entre routers para el establecimiento de redes privadas virtuales (VPN, Virtual Private Network).

8.3. CARPETAS, IMPRESORAS Y OTROS RECURSOS

Además de las medidas de protección que se pueden aplicar en la red que da acceso a los recursos compartidos, se deberían considerar las siguientes medidas específicas referentes a las impresoras:

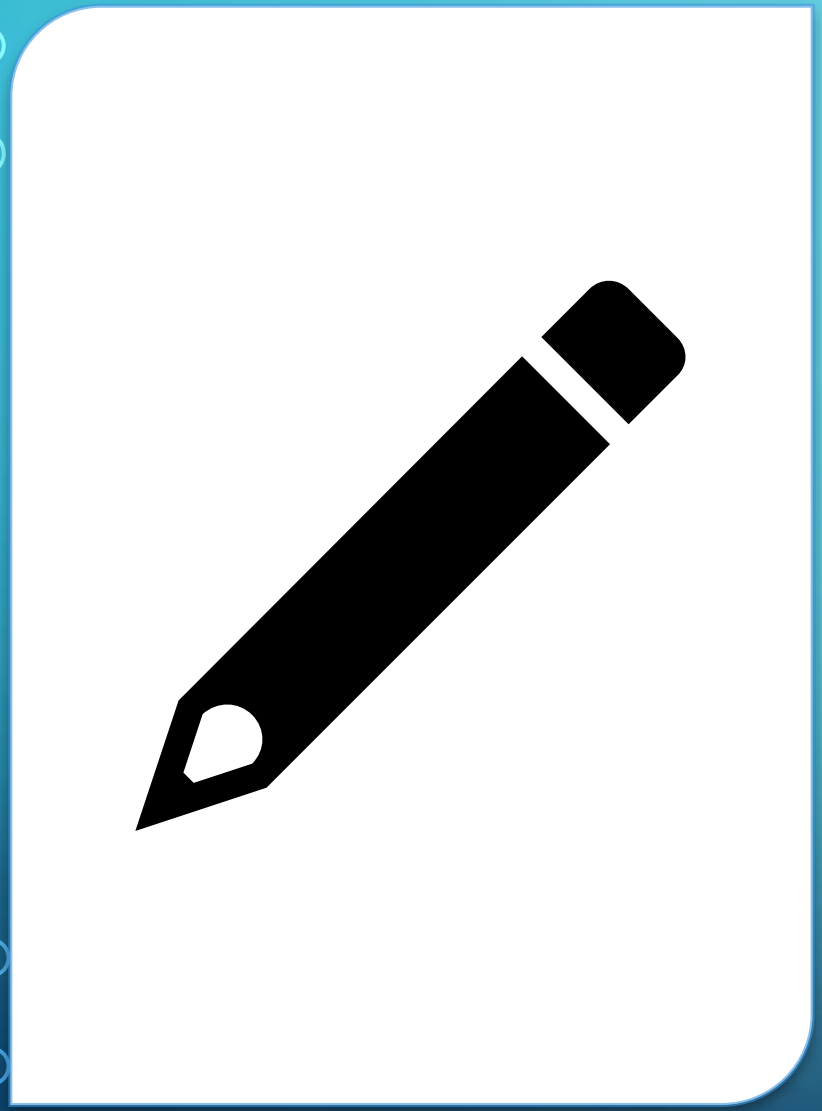
- Solo deben ser instalables por usuarios con privilegios para ello. Así se valora en la guía CIS v1.2 para sistemas Windows, en su punto 3.2.1.11, que también señala en la medida 4.1.19 que el servidor de impresión es uno de los servicios que solo deberían estar activos en caso de ser estrictamente necesario.
- Una medida organizativa es que los controladores de las impresoras deberían gestionarse según un procedimiento formal, para asegurar la homogeneidad de las versiones, y la rápida distribución de parches que solucionen vulnerabilidades.
- Siempre que sea posible, las impresoras no deberían tener conexión hacia o desde internet, y de ser necesarias, deberían restringirse las comunicaciones con direcciones IP conocidas y fijadas de antemano.
- Las impresoras deberían disponer de un sistema de control de acceso, preferiblemente integrado con el sistema de información de la empresa, para controlar qué usuarios tienen permisos de impresión.
- Las impresoras deberían tener un modo de impresión segura, de manera que no se inicie el trabajo de impresión hasta que el usuario esté delante de la máquina y aporte un código.

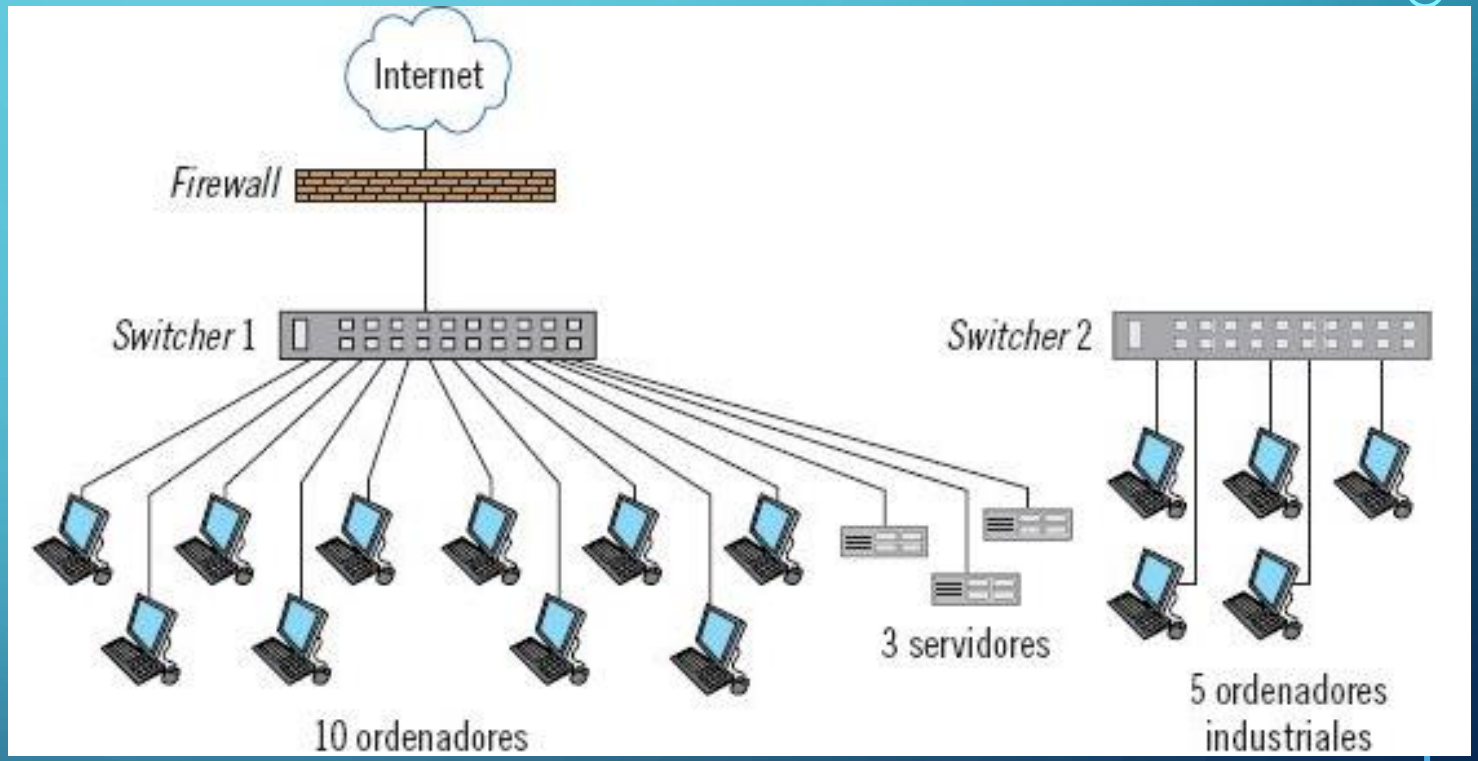
Actividades

LA RED DE UNA EMPRESA ESTÁ FORMADA POR 10 ORDENADORES DE OFICINA, 3 SERVIDORES PARA ESTOS ORDENADORES DE OFICINA Y 5 ORDENADORES INDUSTRIALES QUE SOLO NECESITAN ACCESO ENTRE ELLOS Y QUE CONTROLAN EL PROCESO DE FABRICACIÓN, CRÍTICO PARA EL NEGOCIO. SE DISPONE ADEMÁS DE 2 SWITCHERS, EL SEGUNDO DE LOS CUALES ES GESTIONABLE, Y DE 1 FIREWALL.

DIBUJAR LA RED PROPUESTA, JUSTIFICANDO LAS DECISIONES DE DISEÑO ADOPTADAS.

Actividades





9. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

Los sistemas de información deben monitorizarse, para medir la eficacia de las salvaguardas que los protegen y obtener evidencias que permitan valorar si estas salvaguardas son necesarias.

Además, las medidas de seguridad aplicadas tendrán vulnerabilidades, y podrían verse desactivadas o inutilizadas, permitiendo que el sistema esté comprometido sin saberlo.

9.1. MONITORIZACIÓN Y REGISTRO

La norma ISO 17799:2005 establece, en su objetivo de control “10.10 Monitorización”:

“10.10.1 Registro de Auditoría”, de toda actividad de seguridad que suceda en el sistema (cambios, aciertos, errores, eventos, alarmas, etc.).

“10.10.2 Uso del sistema de monitorización”, que debe realizarse de acuerdo con un procedimiento formal y documentado.

“10.10.3 Protección de los registros”, ya que si se pueden alterar, no habrá evidencia de un acceso no autorizado, de manera que los registros serán un objetivo importante para un atacante.

“10.10.4 Registros de los usuarios con privilegios y de los operadores del sistema”, que se deben revisar regularmente para detectar eventos de seguridad que sean indicio de un incidente.

“10.10.5 Registro de fallos y errores” detectados por el sistema, o notificados por los usuarios.

“10.10.6 Sincronización de relojes” de manera que haya precisión al revisar eventos en distintos sistemas con diferentes relojes.

9.2. RECOMENDACIONES NIST SOBRE MONITORIZACIÓN Y REGISTRO

La guía NIST 800-123, en su apartado 6.1, indica que el registro de la actividad, y en especial de los eventos de seguridad, es una labor vital para el mantenimiento continuo de la seguridad en los servidores. Elegir los datos correctos que se registren, y monitorizar los registros, es una tarea vital para el mantenimiento de los sistemas de información.

Los registros proporcionan:

- Un sistema de alerta sobre actividades sospechosas a investigar.
- La trazabilidad de una actividad hostil.
- Información de ayuda para recuperar un servidor.
- Información de ayuda en la investigación posterior a un incidente.
- Información que se pueda requerir legalmente.

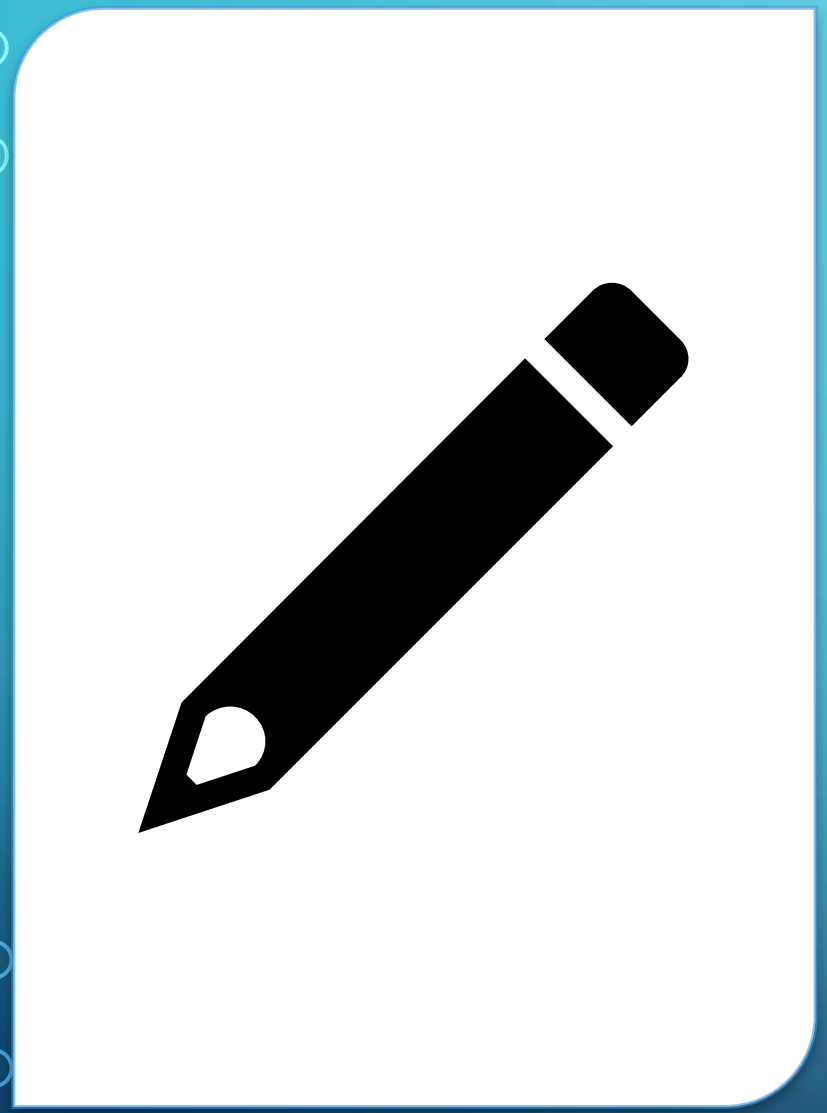
9.3. USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

Esquema Nacional de Seguridad, STIC-821 apéndice 1 (NG00), párrafo 102.

Vigilar:

- El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
- La degradación de los servicios.
- La modificación no autorizada y premeditada de información.
- La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
- El deterioro intencionado del trabajo de otras personas.
- El uso de los sistemas de información para fines ajenos a los de la organización, salvo excepciones que se contemplen expresamente.
- Dañar intencionadamente los recursos informáticos de la organización o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

Actividades



1.8.100.1.EJERCICIOSCAPITULO_8.DOCX