MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE SERVEI PÚBLIC D'OCUPACIÓ ESTATAL

MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES

Generalitat de Catalunya

SOC Servei d'Ocupació de Catalunya

IRON HACK SPAIN

Seguridad en equipos informáticos

IFCT0109 – Seguridad informática

MF0486_3 (90 horas)

Robustecimiento de sistemas

Introducción
Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información
Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios
Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles
Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible
Actualización de parches de seguridad de los sistemas informáticos
Protección de los sistemas de información frente a código malicioso
Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema
Monitorización de la seguridad y el uso adecuado de los sistemas de información
Resumen

Introducción

Introducción

Reducir las Vulnerabilidades para Minimizar el Riesgo

- Un incidente de seguridad ocurre cuando una amenaza explota una vulnerabilidad del sistema.
- Reducir las vulnerabilidades (robustecimiento o securización) reduce el riesgo de un ataque.
- El robustecimiento se aplica principalmente a la seguridad lógica del sistema.
- Las vulnerabilidades son como puertas abiertas que permiten a los atacantes acceder al sistema.
- Reducir las vulnerabilidades es una forma efectiva de prevenir ataques.
- El robustecimiento debe ser específico para cada sistema y función.

Minimizar la superficie de ataque:

- Un sistema con menos funciones es menos vulnerable.
- Eliminar aplicaciones y servicios innecesarios.

Reducir el número de usuarios:

- Eliminar usuarios innecesarios.

Revisión continua:

- Mantenerse actualizado con parches de seguridad.
- Usar software antivirus.

Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información

Usuarios y contraseñas por defecto

Seguridad de los sistemas: Cambiar usuarios y contraseñas por defecto

- Los sistemas de información utilizan cuentas de usuario para controlar el acceso.
- Las contraseñas por defecto son un riesgo para la seguridad, pq son conocidas por los atacantes
- La norma ISO 27001 exige cambiar las contraseñas por defecto, además de ser una medida básica de seguridad.

Riesgos asociados a las cuentas por defecto

- Acceso no autorizado: Los atacantes pueden usar las cuentas por defecto para acceder al sistema.
- Elevación de privilegios: Los atacantes pueden usar las cuentas por defecto para obtener permisos más altos.
- Malware: Las cuentas por defecto pueden ser utilizadas para instalar malware.

Las cuentas por defecto son un blanco fácil para los atacantes y pueden usar las cuentas por defecto para causar daños al sistema. Es importante proteger las cuentas por defecto para evitar estos riesgos.

Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información

Usuarios y contraseñas por defecto

Buenas prácticas para la gestión de cuentas

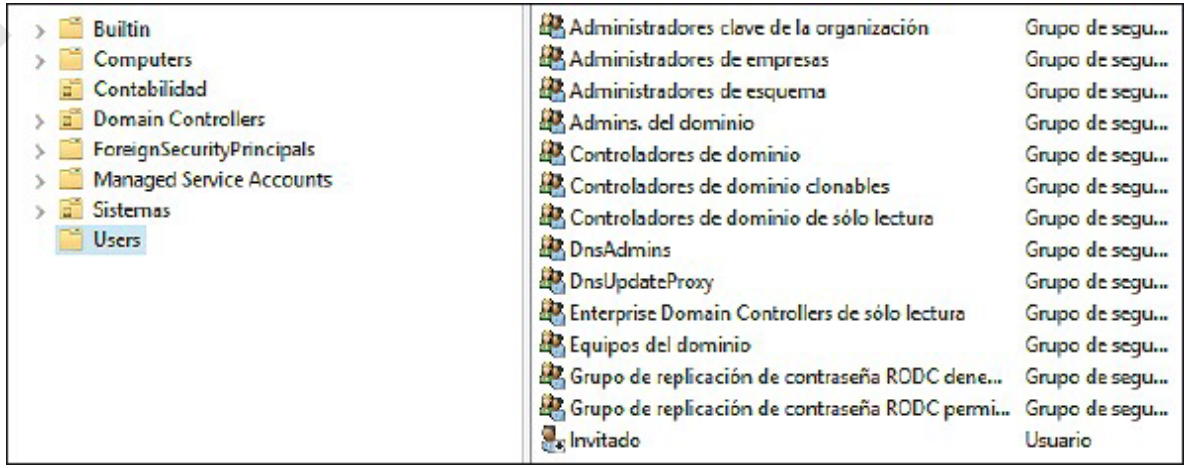
- Cambiar las contraseñas por defecto: Usar contraseñas seguras y únicas.
- Deshabilitar las cuentas no utilizadas: Eliminar las cuentas que no se necesitan.
- Restringir los permisos: Otorgar a los usuarios solo los permisos que necesitan.
- Monitorizar la actividad: Vigilar la actividad del sistema para detectar accesos sospechosos.

Implementar buenas prácticas de gestión de cuentas es fundamental para la seguridad y cambiar las contraseñas por defecto es el primer paso.

En sistemas Microsoft Windows, los identificadores de seguridad (SID) de usuarios y grupos por defecto son conocidos públicamente. Un atacante con acceso al sistema podría usar este conocimiento para:

- Averiguar el nombre de usuario de una cuenta modificada.
- Potencialmente obtener acceso a la cuenta.

Cuenta invitada deshabilitada



Modificación de los usuarios y contraseñas por defecto de los distintos sistemas de información

Referencias y directrices

Existen diversas fuentes acreditadas para el robustecimiento de sistemas. Entre las más destacadas se encuentran:

- INCIBE: Guías para servidores web:
- CCN: Guías para sistemas operativos (buscamos por sistema operativo)
- NIST: Biblioteca sobre seguridad de la información (Serie 800).
- CIS: Guías de comparación y robustecimiento (Benchmarks).

Estas guías proporcionan información y recomendaciones para fortalecer la seguridad de los sistemas y Es importante consultarlas y adaptarlas a las necesidades específicas de cada organización.

Directrices CIS para Cuentas y Contraseñas

- Asegurar el uso de cuentas administrativas dedicadas.
- Usar contraseñas únicas.
- Usar autenticación multifactor para accesos administrativos.
- Registrar y alertar los inicios de sesión fallidos a cuentas administrativas.

Estas directrices son esenciales para proteger los sistemas contra accesos no autorizados y es importante implementarlas de forma adecuada y monitorizar su eficacia.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Introducción

Importancia de la Gestión de Contraseñas y Privilegios

- Introducción a la Gestión de Seguridad: La correcta configuración de las políticas de gestión de contraseñas y privilegios es esencial para salvaguardar la seguridad de los sistemas de información.
- Requisitos para Contraseñas Seguras: Las contraseñas deben cumplir con requisitos mínimos, como longitud adecuada, variedad de caracteres, periodo de vigencia y la no repetición de claves anteriores.
- Directivas de Gestión de Contraseñas: Estas condiciones se agrupan en directivas que deben aplicarse a los usuarios para prevenir vulnerabilidades.
- Gestión de Privilegios: Además, es fundamental gestionar los privilegios mediante la inclusión o exclusión de usuarios en grupos con permisos específicos sobre ficheros o programas.

Principios Fundamentales de Autenticación de Usuarios

- Principios de Autenticación: La autenticación se basa en algo que el usuario tiene, algo que es y algo que sabe, como tarjetas de identificación, características biométricas y contraseñas, respectivamente.
- Relación con la Seguridad: Estos principios son fundamentales para garantizar la seguridad de los sistemas de información y prevenir accesos no autorizados.
- Norma ISO 27002: Esta norma establece controles relacionados con la gestión de derechos de acceso y privilegios como marco de referencia para asegurar la autenticación de usuarios de manera segura.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Introducción

Proceso de Gestión de Derechos de Acceso y Privilegios

- Identificar a qué usuarios deben concederse accesos a recursos específicos es crucial para garantizar la seguridad de los sistemas.
- Los privilegios deben asignarse cuidadosamente en función de la necesidad de saber de cada usuario, evitando otorgar permisos innecesarios.
- Es fundamental mantener un proceso de autorización y registro completo antes de conceder privilegios, garantizando así una trazabilidad adecuada.
- Se recomienda el uso de rutinas o mecanismos automáticos del sistema para evitar la necesidad de otorgar privilegios manualmente, lo que puede reducir el riesgo de errores humanos.
- Asimismo, se aconseja el uso de programas que minimicen la necesidad de ejecutarse con privilegios, lo que puede contribuir a mejorar la seguridad del sistema.
- Finalmente, es importante asignar los privilegios a un identificador de usuario diferente al utilizado en el uso diario de la empresa, lo que ayuda a mitigar posibles riesgos de seguridad y a mantener una segregación adecuada de funciones.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Introducción

Condiciones para Contraseñas Seguras según ISO 27002

- Las contraseñas deben ser de calidad y tener una longitud suficiente.
- Deben ser fáciles de recordar pero no basarse en información fácilmente adivinable.
- No deben incluir palabras que se encuentren en diccionarios comunes.
- Deben estar libres de caracteres consecutivos idénticos, ya sean numéricos o alfanuméricos.
- Se recomienda cambiarlas regularmente o en base al número de accesos, evitando la reutilización de claves anteriores.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Directrices en guías NIST

Directrices de Seguridad según NIST 800-123

- La guía NIST 800-123 establece directrices específicas para la seguridad de servidores, destacando la importancia de las políticas de contraseñas.
- Estas políticas deben incluir aspectos como la longitud mínima, complejidad, periodo de validez, reutilización y seguridad en el almacenamiento de contraseñas.
- Reflexión sobre Seguridad y Conveniencia. Es crucial encontrar un equilibrio entre seguridad y conveniencia al establecer estos valores, ya que una longitud excesiva puede dificultar su memorización y llevar a prácticas inseguras, como apuntarlas en lugares no seguros.
- Se debe garantizar que el periodo de vigencia de las contraseñas esté equilibrado con un periodo mínimo para evitar la repetición de contraseñas anteriores.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Directrices en guías NIST

Prevención de Ataques y Medidas de Seguridad Adicionales

- La guía NIST 800-123 también recomienda medidas para prevenir ataques de fuerza bruta y la adivinación de contraseñas por repetición.
- Se sugiere incrementar el tiempo entre intentos de inicio de sesión después de fallos sucesivos y bloquear cuentas temporal o permanentemente después de un número determinado de intentos fallidos.
- Es importante considerar el compromiso entre seguridad y conveniencia, ya que un exceso de medidas de seguridad podría afectar negativamente la experiencia del usuario.
- Otras medidas adicionales, como el uso de tarjetas inteligentes, lectores biométricos o sistemas de contraseña de un solo uso, pueden ser necesarias dependiendo del valor de la información almacenada y el nivel de seguridad requerido.

Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios

Directrices en guías CIS

Directrices CIS para Microsoft Server

- Para Microsoft Server, las directrices del Centro de Seguridad CIS incluyen elementos clave para configurar políticas de contraseñas a través del Directorio Activo.
- Estos elementos incluyen la longitud mínima de contraseñas, la edad máxima y mínima de las mismas, la complejidad requerida y el historial de contraseñas a recordar.

Elementos de Configuración para Linux

- Para el subsistema de contraseñas en Linux, se establecen directrices específicas que extienden el sistema de contraseñas por defecto y son integrables con OpenLDAP.
- Estas directrices incluyen requerir autenticación para el modo de arranque de un solo usuario, ajustar los periodos de expiración y vigencia de las contraseñas, asegurar que no haya contraseñas vacías y deshabilitar configuraciones obsoletas como ".rhosts" en la configuración de PAM.

Configuraciones Adicionales y Recomendaciones

- Además de las directrices anteriores, se deben revisar la configuración de PAM y librerías extendidas para evitar el uso de contraseñas débiles.
- Se recomienda deshabilitar el almacenamiento de contraseñas con cifrado reversible y asegurar que no queden entradas obsoletas en archivos de contraseñas o grupos, provenientes de sistemas antiguos.
- Estas medidas son fundamentales para garantizar la seguridad de los sistemas y prevenir posibles vulnerabilidades relacionadas con contraseñas débiles o configuraciones obsoletas.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Herramientas y otras aplicaciones

Principios de Robustecimiento del Sistema

- El robustecimiento busca reducir la superficie de ataque de un sistema, lo que implica eliminar herramientas, utilidades, aplicaciones y servicios no necesarios.
- La norma ISO 27002 establece procedimientos para añadir o quitar aplicaciones del sistema como un cambio, mediante controles como "Responsabilidades y procedimientos de operación" y "Gestión de cambios".

Normativas y Medidas Organizativas

- La norma ISO 27002 incluye objetivos de control relacionados con el cumplimiento legal y la revisión de la seguridad de la información para disuadir el uso no autorizado de herramientas.
- proporciona apéndices con normativas de referencia, como la "Normativa general de utilización de los recursos y sistemas de información del organismo (NG00)", que establece medidas organizativas sobre la instalación de software y el uso de aplicaciones dentro de la empresa.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Herramientas y otras aplicaciones

Medidas Específicas de Seguridad

La guía CCN-STIC 821 dice

- Solo el personal de soporte técnico autorizado puede instalar software en los equipos de los usuarios, excepto las herramientas de uso común descargables desde servidores internos.
- Los usuarios pueden solicitar la inclusión de aplicaciones, que deben ser evaluadas por el personal técnico de seguridad.
- Se prohíbe la instalación de software sin licencia o que infrinja la legislación de propiedad intelectual.
- Está prohibida la reproducción, modificación, cesión o uso fuera de la empresa de programas instalados en los equipos de la empresa.
- Las aplicaciones instaladas por la empresa, especialmente las relacionadas con la seguridad, no pueden ser deshabilitadas ni eliminadas.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Herramientas y otras aplicaciones

Medidas Específicas de Seguridad

La guía CCN-STIC 821 recoge en sus apéndices 7 normativas:

- Uso de los sistemas de información.
- Acceso a internet.
- Uso de correo electrónico.
- Normas para trabajar fuera de las instalaciones.
- Uso de contraseñas.
- Confidencialidad para terceros.
- Buenas prácticas para terceros.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Comunicaciones y puertos de red

Control de Acceso a las Redes y Servicios

- La norma ISO 27002 establece en su objetivo de control "9.1.2 Control de acceso a las redes y servicios asociados" la necesidad de proporcionar a los usuarios acceso solo a lo autorizado.
- Es fundamental identificar los servicios accesibles desde fuera de la empresa y habilitar el tráfico entrante exclusivamente en los puertos necesarios para esos servicios.

Procedimientos de Control y Normativas de Uso de Internet

- Es importante implementar un procedimiento formal para controlar los puertos abiertos y establecer contramedidas organizativas que fomenten el buen uso del sistema de comunicación e internet.
- La guía CCN-STIC 821- Apéndice 2(NP10) propone una normativa de referencia para el control del uso de internet, que incluye medidas como el uso de internet para fines profesionales, evitar páginas de contenido poco ético o ilegal, y mantener actualizado el navegador y las herramientas de seguridad.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Comunicaciones y puertos de red

Puertos Autorizados y Procedimientos de Evaluación

- Los puertos autorizados deben ser un conjunto mínimo estándar, como ~~HTTP~~, HTTPS, FTP, y servicios varios de la empresa identificados y definidos.
- Cualquier inclusión de otros puertos debe solicitarse y analizarse por el personal técnico de seguridad para garantizar la seguridad de la red y prevenir posibles riesgos de seguridad.

Medidas del Apéndice 2(NP10) de la Guía CCN-STIC 821

- Uso de internet para fines profesionales.
- Evitar visitar páginas de contenido poco ético, ofensivo o ilegal, así como páginas no fiables o sospechosas.
- Cuidar la información publicada en internet y observar las restricciones legales aplicables.
- Realizar descargas solo con autorización y asegurar la autenticidad de las páginas visitadas.
- Comprobar la seguridad de la conexión, cerrar sesiones al finalizar la conexión y utilizar herramientas contra código dañino.
- Mantener actualizado el navegador y las herramientas de seguridad, utilizar niveles de seguridad del navegador y desactivar las cookies.
- Eliminar la información privada y evitar la instalación de complementos desconocidos.
- Limitar y vigilar la ejecución de programas en el navegador, como applets y scripts.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Pasarelas de seguridad

Concepto de Pasarelas de Seguridad

- Las pasarelas, puertas de enlace o puertas de acceso son equipos de comunicaciones que conectan redes con arquitecturas diferentes, realizando funciones de traducción de protocolos.
- En el contexto de internet y redes TCP/IP, las pasarelas a menudo funcionan como routers, simplificando el equipo a funciones de la capa de interred.

Funciones y Características de las Pasarelas de Seguridad

- Las pasarelas de seguridad extienden las funciones de un router y suelen incorporar servicios de antivirus o detección de intrusos para tomar decisiones sobre las conexiones permitidas.
- El router, al decidir el encaminamiento de la comunicación, permite filtrar conexiones y proporciona servicios de traducción de direcciones de red (NAT).

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Pasarelas de seguridad

Importancia y Referencias de Seguridad

- El NIST, en su manual "An Introduction to Computer Security: The NIST Handbook (1995)", recomienda el uso de pasarelas de seguridad o firewalls para bloquear y filtrar el acceso entre la red privada de la empresa e internet.
- El uso de firewalls implica un equilibrio entre funcionalidad y seguridad, y la decisión debe basarse en una política de seguridad que permita implementar medidas adecuadas al nivel requerido por cada empresa.

Funciones del Router en la Red

- El router, al decidir el encaminamiento de la comunicación, permite filtrar conexiones según reglas establecidas.
- Las reglas pueden basarse en el puerto, el protocolo y/o la dirección IP de los extremos.
- Además, proporciona servicio de traducción de direcciones de red (NAT) para optimizar el uso de direcciones IP públicas en la conexión a internet.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Directrices en guías NIST

Estrategias de Instalación de Aplicaciones de Servidor

- La guía NIST 800-123 sugiere que una aplicación de servidor idealmente debería residir en un equipo dedicado a esta única función.
- Se recomienda realizar una instalación mínima del sistema operativo y luego agregar los servicios y aplicaciones necesarios.
- En caso de no poder realizar una instalación mínima, se debe desinstalar todas las aplicaciones, servicios y protocolos de red innecesarios después de la instalación estándar.

Desinstalación y Bloqueo de Servicios

- La desinstalación es preferible a desactivar o bloquear servicios, ya que lo que no existe no puede ser vulnerable.
- Si un servicio no puede ser desinstalado, se puede bloquear de forma que su reactivación requiera intervención física intencionada.
- Se deben revisar servicios como el de compartir archivos, comunicaciones inalámbricas, control y acceso remoto no cifrado, entre otros.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Directrices en guías NIST

Ventajas y Directrices Adicionales

- Deshabilitar servicios innecesarios aumenta la seguridad al reducir la superficie de ataque y posibles problemas de compatibilidad.
- Además, libera recursos del sistema para los servicios esenciales y reduce la necesidad de espacio en disco.
- Otras directrices incluyen eliminar documentación y archivos de ejemplo del fabricante y configurar servicios para aceptar conexiones solo en puertos específicos.

Los servicios que se deben revisar expresamente, según la guía NIST 800-123, son:

- Servicios para compartir archivos e impresoras.
- Servicios de comunicaciones inalámbricas.
- Servicios de control y acceso remoto, especialmente los no cifrados, como Telnet.
- Servicios de directorio, como LDAP.
- Servidores web.
- Servidores de correo electrónico.
- Compiladores y librerías de lenguajes.
- Herramientas de desarrollo.
- Herramientas y utilidades de gestión de red, como el protocolo SNMP.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Directrices en guías CIS

Para sistemas operativos Linux, CIS recomienda instalar paquetes de robustecimiento o hardering.

Algunas herramientas modernas y activamente mantenidas que se utilizan para fortificar sistemas Linux incluyen:

- CIS-CAT Pro: Esta herramienta de evaluación de seguridad proporciona evaluaciones automatizadas de cumplimiento con las pautas de seguridad CIS (Center for Internet Security) para una variedad de sistemas operativos, incluidas varias distribuciones de Linux.
- OpenSCAP: Es una herramienta de cumplimiento de políticas y evaluación de seguridad que implementa los estándares SCAP (Security Content Automation Protocol). OpenSCAP puede escanear sistemas Linux en busca de vulnerabilidades y configuraciones inseguras, y proporcionar recomendaciones para mejorar la seguridad.
- Tiger: Tiger es una auditoría de seguridad del sistema para sistemas Unix y Linux. Realiza numerosas verificaciones de seguridad en el sistema, incluida la configuración de seguridad, los permisos de archivos y directorios, las cuentas de usuario y más.
- OSSEC: Es una plataforma de detección de intrusos de código abierto que monitorea logs de sistemas, archivos de configuración y actividad del sistema en busca de signos de intrusiones o actividad maliciosa.
- Fail2Ban: Esta herramienta se utiliza para proteger servidores Linux contra ataques de fuerza bruta al bloquear automáticamente direcciones IP que intentan acceder repetidamente con credenciales incorrectas.

Eliminación y cierre de las herramientas, utilidades, servicios y puertos prescindibles

Directrices en guías CIS

Desactivación de servicios innecesarios en sistemas LINUX

Se recomienda desactivar dos grandes grupos de aplicaciones:

- Servicios basados en el servicio xinitd (FTP, TFTP, Telnet, POP, IMAP, RLOGIN, entre otros).
- Servicios innecesarios en el arranque del sistema (sendmail, login gráfico, X Font server, SMB, NFS, NIS, RPC, NETFS, SNMP, entre otros).

Básicamente solo hay que tener activados los servicios que se necesiten para trabajar, porque sino estamos activando más vulnerabilidades.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Introducción

Muchos servicios comunes en internet no son seguros ya que la información enviada no está cifrada.

Herramientas como WireShark pueden capturar tramas de tráfico, revelando información como la dirección web visitada.

La confidencialidad es inexistente si se captura el tráfico: las peticiones al servidor web y sus respuestas pueden ser capturadas y visualizadas sin problemas.

Mejorando la Seguridad en Internet

Para mejorar la confidencialidad de los servicios en internet (una red pública no fiable), se utilizan mecanismos que cifran la información intercambiada.

Si un atacante obtiene acceso al tráfico, tendría que descifrar la información para acceder a ella, lo que protege la información y ofrece resistencia a su descubrimiento.

En el extremo receptor de la comunicación, el destinatario descifra la información y accede al contenido.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Criptosistemas de clave secreta y criptosistemas de clave pública

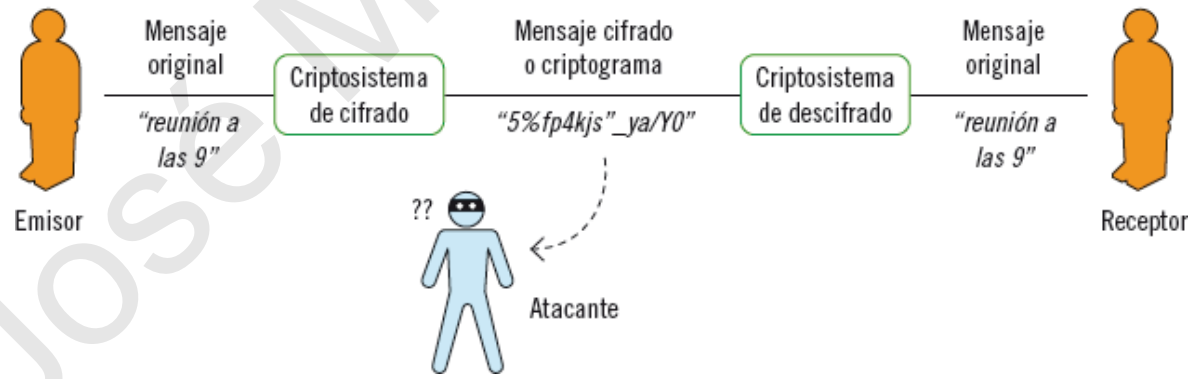
- La criptografía es la ciencia que proporciona comunicaciones seguras a través de canales inseguros.
- El texto se cifra para que resulte ilegible para quien no sepa descifrarlo y recuperar el texto original.
- El proceso completo de cifrado y descifrado se realiza mediante un criptosistema.

Criptosistemas

Los criptosistemas definen los algoritmos y las claves necesarios para transformar una información en otra.

Para dificultar el descifrado de la información, se mantiene secreto el algoritmo o procedimiento, y/o sus claves o parámetros.

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



Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Criptosistemas de clave secreta y criptosistemas de clave pública

Criptosistemas de Clave Simétrica

- En los criptosistemas de clave simétrica, la clave que se emplea para cifrar y descifrar la información es la misma y debe ser conocida por el emisor y el receptor del mensaje.
- La clave debe permanecer secreta, porque de conocerse se puede descifrar la información.
- Estos sistemas son sencillos y se usan frecuentemente, pero no se emplean habitualmente en procesos de autenticación.

Criptosistemas de Clave Asimétrica

- En los criptosistemas de clave asimétrica, se emplea una clave pública para cifrar la información y una clave privada para descifrarla. Se utiliza un par de claves. La pública es y debe ser conocida ampliamente, mientras que la clave privada es conocida únicamente por quien la crea.
- Cualquier persona que tenga la clave pública puede enviar datos cifrados al propietario de la clave privada, pero solo el propietario de la clave privada puede descifrar estos datos.
- Este mecanismo se emplea muy habitualmente para las comunicaciones por internet, porque no necesita ninguna vía segura. Se adapta perfectamente al uso exclusivo de internet.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Criptosistemas de clave secreta y criptosistemas de clave pública

Firma Electrónica y su Regulación

- La firma electrónica es equivalente a una firma manual y aporta la identidad del propietario de la firma al documento.
- En España, la firma electrónica está regulada por la Ley 06/2020, que deroga la antigua Ley 59/2003 debido a su incompatibilidad con el Reglamento Europeo 910/2014.
- Este reglamento regula la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Firma Digital y sus Características

- La firma digital es un caso específico de la firma electrónica que utiliza una clave pública.
- El emisor emplea su clave privada para cifrar un resumen del documento y lo envía junto con el documento.
- El receptor utiliza la clave pública del emisor para descifrar el resumen y luego lo compara con el resumen del documento que él calcula para confirmar la integridad del documento y la autenticidad del remitente.
- La firma digital asegura la integridad del documento pero no aporta confidencialidad, ya que cualquiera que intercepte el mensaje puede descifrarlo con la clave pública del remitente.
- La identidad del remitente y el no repudio solo quedan asegurados de forma débil, ya que la autenticidad del remitente no está respaldada por un tercero.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Criptosistemas de clave secreta y criptosistemas de clave pública

Certificado digital vs Certificado electrónico

- En España, los términos "certificado digital" y "certificado electrónico" se usan con frecuencia de forma intercambiable, lo que puede generar confusión. Aunque están estrechamente relacionados, existen algunas diferencias sutiles:

Certificado digital:

- Es un concepto más amplio que abarca cualquier documento electrónico que vincule una identidad a una clave pública. No tiene un marco legal específico en España.
- Se utiliza en diversos contextos, como el comercio electrónico, la firma electrónica y la autenticación de usuarios.

Certificado electrónico:

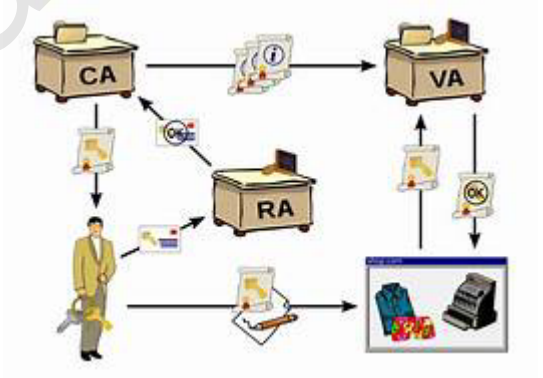
- Es un tipo de certificado digital que cumple con los requisitos establecidos en la Ley 59/2003 de Firma Electrónica.
- Posee validez legal y puede ser utilizado para realizar trámites administrativos y comerciales de forma electrónica.
- Se emite por una Autoridad de Certificación (AC) reconocida, como la Fábrica Nacional de Moneda y Timbre (FNMT).

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Criptosistemas de clave secreta y criptosistemas de clave pública

Entidades de certificación:

- DNI electrónico (Dirección General de la Policía)
- Fábrica Nacional de Moneda y Timbre (FNMT)
- Generalitat Valenciana (ACCV)
- Agéncia Catalana de Certificació (CATCert)
- ANF Autoridad de Certificación (ANF AC)
- AC Camerfirma



Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Protocolos seguros

Un protocolo seguro es un conjunto de reglas y normas que rigen la comunicación entre dos o más sistemas informáticos con el objetivo de proteger la información y los datos que se intercambian. Estos protocolos son esenciales para garantizar la seguridad de las comunicaciones en Internet, especialmente cuando se trata de información sensible o confidencial.

Ejemplos de protocolos seguros:

HTTPS (Hypertext Transfer Protocol Secure):

Es la versión segura del protocolo HTTP, utilizado para navegar por la web.

Cifra la información que se intercambia entre el navegador web y el servidor web, protegiéndola de miradas indiscretas.

Se utiliza para acceder a sitios web que requieren autenticación, como bancos online o tiendas virtuales.

SSH (Secure Shell):

Es un protocolo para la administración remota de servidores.

Permite a los usuarios conectarse a un servidor de forma segura y ejecutar comandos como si estuvieran presentes físicamente en el servidor.

Cifra la información que se intercambia entre el cliente SSH y el servidor SSH, protegiéndola de ataques.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

Protocolos seguros

Ejemplos de protocolos seguros:

SFTP (Secure File Transfer Protocol):

Es un protocolo para la transferencia segura de archivos.

Permite a los usuarios transferir archivos entre dos servidores o entre un servidor y un cliente de forma segura.

Cifra la información que se intercambia entre el cliente SFTP y el servidor SFTP, protegiéndola de ataques.

TLS (Transport Layer Security):

Es un protocolo que proporciona seguridad a la capa de transporte de la red.

Se utiliza para proteger la comunicación entre dos aplicaciones, como un navegador web y un servidor web, o un cliente de correo electrónico y un servidor de correo electrónico.

Cifra la información que se intercambia entre las dos aplicaciones, protegiéndola de ataques.

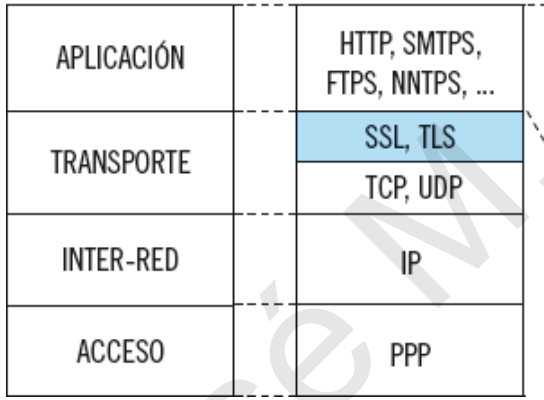
Es importante elegir el protocolo adecuado para cada caso, en función del tipo de información que se va a intercambiar y del nivel de seguridad que se requiere.

Configuración de los sistemas de información para que utilicen protocolos seguros donde sea posible

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)



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
...		

Actualización de parches de seguridad de los sistemas informáticos

Introducción

Gestión de Vulnerabilidades y Parches

- A pesar de minimizar los servicios implementados y usar protocolos seguros, las funciones prestadas pueden presentar vulnerabilidades.
- Estas vulnerabilidades, una vez descubiertas, representan un riesgo para el sistema de información.
- Los fabricantes suelen ser conscientes de las vulnerabilidades en una fase temprana y trabajan activamente para corregir estas debilidades.
- Los fabricantes proporcionan parches o correcciones que los usuarios deben aplicar para resolver el problema.

Actualización de parches de seguridad de los sistemas informáticos

Actualización de parches

Gestión de Vulnerabilidades y Parches

- A pesar de minimizar los servicios implementados y usar protocolos seguros, las funciones prestadas pueden presentar vulnerabilidades.
- Estas vulnerabilidades, una vez descubiertas, representan un riesgo para el sistema de información.
- Los fabricantes suelen ser conscientes de las vulnerabilidades en una fase temprana y trabajan activamente para corregir estas debilidades.
- Los fabricantes proporcionan parches o correcciones que los usuarios deben aplicar para resolver el problema.

Gestión de Vulnerabilidades según ISO 17799:2005

- La norma ISO 17799:2005 establece la gestión de la vulnerabilidad técnica como objetivo de control.
- Se debe obtener información oportuna sobre las debilidades de los sistemas de información en uso.
- Se recomienda establecer un procedimiento formal de gestión de vulnerabilidades, que incluya búsqueda activa de información, monitorización de nuevas vulnerabilidades y establecimiento de un cronograma de reacción.

Actualización de parches de seguridad de los sistemas informáticos

Actualización de parches

Evaluación de Riesgos y Aplicación de Parches

- Se debe evaluar el riesgo asociado a la vulnerabilidad para determinar las acciones a emprender, como la aplicación de un parche.
- Se debe considerar el riesgo de aplicar un parche frente al de no aplicarlo, y se debe probar y evaluar su efectividad antes de aplicarlo.
- Se pueden considerar controles alternativos a la aplicación de un parche, como desconectar servicios relacionados con la vulnerabilidad, agregar controles como firewalls, reforzar la monitorización y mantener registros de auditoría.

Atención a Sistemas de Mayor Riesgo y Cambio de Software

- Se debe atender primero a los sistemas de mayor riesgo.
- Es importante tener un entorno de prueba y evaluación del parche antes de aplicarlo en entornos productivos.
- La norma ISO señala la importancia de seguir un procedimiento formal en relación al cambio de software.

Actualización de parches de seguridad de los sistemas informáticos

Directrices en guías NIST

Aplicación de Parches según la Guía NIST 800-123

- Una vez instalada la aplicación del servidor, es esencial aplicar parches para corregir vulnerabilidades conocidas antes de que el sistema sea accesible o entre en producción.
- Los administradores del servidor deben seguir un procedimiento organizado para aplicar actualizaciones, reducir las vulnerabilidades y aplicar parches oportunos.

Protección del Servidor durante la Aplicación del Parche

- Durante la aplicación del parche, los administradores deben asegurarse de que el servidor esté protegido.
- Se recomienda desconectar el servidor de la red o mantenerlo solo conectado a una red segura mientras se instalan los parches.
- Los parches deben copiarse mediante un mecanismo fuera de línea, como un CD o una unidad de almacenamiento USB.

Actualización de parches de seguridad de los sistemas informáticos

Directrices en guías NIST

Prueba de Parches y Configuración del Servidor

- Los parches deben probarse antes de aplicarse, especialmente en servidores de producción.
- Se debe disponer de un entorno de prueba idéntico al de producción para verificar que el parche no genera problemas adicionales.
- Aunque los servidores pueden configurarse para descargar automáticamente los parches, no deben configurarse para instalarlos automáticamente para permitir su prueba previa.

Actualización de parches de seguridad de los sistemas informáticos

Directrices en guías CIS

Directrices de CIS para Linux

- La guía de comparación de seguridad v.1.0.5 de CIS para Red Hat Linux recomienda instalar los últimos parches al sistema operativo.
- Esta es una medida fundamental para robustecer un servidor y se destaca entre las primeras medidas.

Directrices de CIS para Microsoft Server

- La guía v.2.1 de CIS para Microsoft Server recomienda configurar el sistema para que se apliquen automáticamente las actualizaciones.
- Esto abarca tanto los paquetes de mejoras y correcciones de mayor envergadura, como los parches y correcciones menores que el fabricante haga disponibles.

Protección de los sistemas de información frente a código malicioso

Ataque de código malicioso

- El código malicioso es una amenaza constante para los sistemas de información.
- Para que la amenaza se materialice, el código malicioso debe llegar a un equipo de la red y ser ejecutado por el mismo.
- Las salvaguardas se aplican de manera preventiva para evitar que el código entre al sistema y sea ejecutado.

Detección y Ejecución de Código Malicioso

- La detección de códigos maliciosos es compleja y debe realizarse en todos los puntos de conexión a internet y en todos los equipos que admitan medios de almacenamiento externo.
- Para que la aplicación sea ejecutada, las instrucciones del programa deben estar en la memoria volátil del ordenador y el microprocesador debe ejecutarlas.
- Se debe analizar el espacio de memoria en busca de una secuencia de instrucciones conocidas, correspondientes a la actividad de los códigos maliciosos existentes.

Protección de los sistemas de información frente a código malicioso

Ataque de código malicioso

Protección contra el Código Malicioso según la Norma ISO 27002

- La norma ISO 27002 establece un objetivo de control dedicado a la protección contra el código malicioso.
- La protección se basará en una política formal que prohíba el uso de software no autorizado, la realización de revisiones regulares de las aplicaciones y archivos de los sistemas críticos, y la instalación y actualización regular de software específico para la detección de código malicioso.
- Se recomienda el empleo de aplicaciones de detección y prevención de código malicioso, preferiblemente en diferentes niveles (servidor y cliente).

Protección de los sistemas de información frente a código malicioso

Tipos de código malicioso

- El código malicioso, o malware, es cualquier aplicación que genera un daño intencionado al sistema sin el conocimiento ni la autorización del usuario.
- Los tipos de malware se clasifican generalmente por su forma de propagación y por el daño que producen.
- Casi todo el malware comparte una característica común: son aplicaciones capaces de copiarse a sí mismas de manera similar a un virus.

Tipos de Malware según su Capacidad de Propagación

- Virus: Infectan a otros archivos ejecutables y se activan cuando se ejecuta el archivo donde están incluidos. Intentan propagarse a otros archivos ejecutables y causar daño intencionado.
- Gusanos: No infectan a otros archivos ejecutables sino que constituyen un archivo por sí mismo. Persiguen como objetivo su máxima propagación, empleando para ello vías como el correo electrónico, redes de intercambio de archivos, 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.

Protección de los sistemas de información frente a código malicioso

Tipos de código malicioso

Tipos de Código Malicioso según el Daño que Producen

- Adware: Aplicaciones que muestran publicidad no deseada al usuario, generalmente basándose en funcionalidades de espía.
- Bloqueador: Impiden la ejecución de determinados programas, como antivirus u otros programas de seguridad, o impiden el acceso a determinadas páginas web.
- Bombas lógicas: Actúan bajo una circunstancia programada, por ejemplo una fecha, o bajo control remoto.
- Joke: Al ejecutarse hace pensar al usuario que el ordenador se va a borrar, que está averiado, etc.
- Hoax: En forma de correo electrónico engañan al destinatario en relación a la existencia de un nuevo virus, o alguna otra información.
- Keylogger: Registra todas las pulsaciones logrando así obtener las claves de acceso a los servicios.
- Clicker: 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.
- Ransomware: Cifran un fichero y coaccionan al usuario a que pague un rescate para descifrarlos.
- Downloader: Acceden a internet para descargar otros programas normalmente maliciosos.

Protección de los sistemas de información frente a código malicioso

Tipos de código malicioso

Tipos de Código Malicioso según el Daño que Producen

- Spyware: Envían información del equipo a un equipo remoto, bien sean las páginas visitadas y otra información sobre hábitos de uso, o documentos completos.
- Exploit: Explotan una vulnerabilidad, generalmente para tener control remoto del sistema infectado, o tener acceso no autorizado al sistema.
- Fraude: Simulan un comportamiento anormal, e incitan a la compra. Generalmente, un falso antivirus u otra aplicación, que informa que se tiene un virus, y puede eliminarse comprando la aplicación.
- Dropper: Permite la instalación de otros códigos maliciosos en el sistema.
- Password Stealer: Accede a ficheros conocidos del sistema, donde se registran usuarios y sus contraseñas para enviarlos al atacante.
- Backdoor: Permite el acceso al sistema operativo, aplicación o página web, eludiendo los controles de acceso que haya.
- Rootkit: Permiten al atacante tomar el control del sistema como su administrador, permitiendo al atacante remoto hacer lo que desee.
- Browser Hijacker: 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.

Protección de los sistemas de información frente a código malicioso

Directrices en guías NIST

Medidas de Control según la Guía NIST 800-123

- Los sistemas operativos y las aplicaciones normalmente no incluyen las medidas de control necesarias para proteger el sistema de las aplicaciones maliciosas.
- Es necesario añadir al sistema medidas adicionales, como aplicaciones específicas contra software malicioso (antivirus, antiespías, detectores de rootkit) y aplicaciones de detección y prevención de intrusiones (IDPS).

Aplicaciones de Detección y Prevención de Intrusiones

- Las aplicaciones IDPS deben poder detectar ataques dirigidos contra el servidor, como los ataques de denegación de servicio (DoS).
- Los sistemas de detección de intrusión (IDS) advierten al administrador de una posible intrusión (carácter reactivo).
- Los sistemas de prevención de intrusiones (IPS) emplean algoritmos para decidir cortar una comunicación que corresponde a un intento de intrusión (carácter preventivo).

Protección de los sistemas de información frente a código malicioso

Directrices en guías NIST

Medidas de Seguridad Adicionales

- Se deben utilizar aplicaciones de chequeo de la integridad de los archivos, que detecten cuando un fichero crítico ha cambiado.
- Se deben instalar cortafuegos (firewalls) en el equipo para protegerlo de accesos no autorizados.
- Se deben utilizar aplicaciones de gestión de actualizaciones o correcciones para atender de manera temprana las nuevas vulnerabilidades.

Mejora de la Confidencialidad y Proporcionalidad del Riesgo

- Se puede mejorar la confidencialidad usando discos duros cifrados, completa o parcialmente.
- Todas las medidas de seguridad deben aplicarse siempre de manera proporcional al riesgo, ya que consumen recursos y pueden afectar el rendimiento del sistema.
- Para evitar un impacto negativo en el rendimiento, algunas medidas deben trasladarse del servidor a equipos de red dedicados exclusivamente a ello.

Protección de los sistemas de información frente a código malicioso

Directrices en guías CIS

- La guía v.1.0.5 de CIS para Red Hat Linux incluye recomendaciones sobre aplicaciones antivirus.
- Es altamente recomendable instalar aplicaciones antivirus, especialmente en los servidores de correo y en los servidores de archivos.
- El objetivo de estas recomendaciones es proteger a los clientes de los servicios de los servidores.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Introducción

- La infraestructura de comunicaciones en una empresa es como el sistema de carreteras que conecta diferentes puntos para facilitar el intercambio de información.
- Elementos Clave: Incluye estaciones de trabajo, servidores, clientes, impresoras y escáneres, todos ellos esenciales para el flujo de trabajo diario.
- Con las redes TCP/IP es posible conectar una amplia gama de dispositivos adicionales: desde cámaras web y reproductores multimedia hasta unidades de almacenamiento en red y equipos industriales compatibles con esta tecnología.
- Una infraestructura de comunicaciones robusta es fundamental para una empresa, ya que facilita la colaboración, la eficiencia operativa y el funcionamiento sin problemas de los sistemas empresariales.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Protección de las comunicaciones: separación y otras medidas

- **Protección de las comunicaciones** Es importante que los servicios, sistemas y usuarios estén separados en diferentes redes. Esto puede ser físicamente o a través de redes virtuales (VLAN). Esta medida básica aumenta la seguridad de los servicios en cada subred.
- **Estructura de red** Normalmente, la estructura de la red se organiza como un árbol, creando grupos según su ubicación. Todos los equipos están conectados a internet a través de un switcher principal y un firewall.
- **Seguridad de la red** La norma ISO 17799:2005, ahora reemplazada por la ISO/IEC 27002:2013, establece directrices para proteger la información en las redes y la infraestructura misma. Es importante proteger las redes de accesos no autorizados.
- **Medidas de seguridad** Se deben asignar responsabilidades separadas para la gestión de redes y equipos. También es necesario establecer medidas especiales para preservar la confidencialidad e integridad de los datos que usan redes públicas.
- **Aplicación de controles** Los controles deben ser consistentes en toda la infraestructura y deben estar en línea con el servicio que se debe proporcionar a la organización. Las medidas deben aplicarse siempre de manera proporcional.
- **Medidas efectivas** Asignar una dirección IP estática a los equipos facilita el seguimiento de las conexiones. También es importante asegurarse de que los usuarios no puedan modificar la dirección IP ni la dirección MAC de sus adaptadores de red. Para cifrar el tráfico de red, se pueden usar protocolos como TLS.

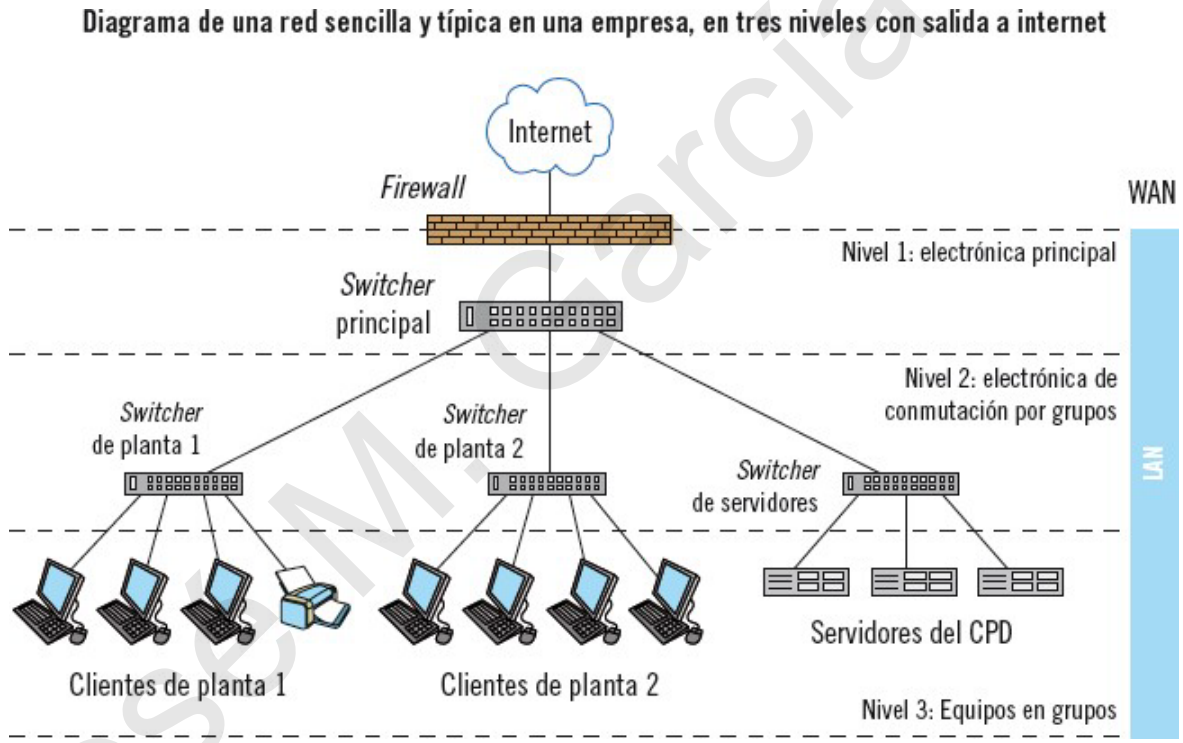
Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Protección de las comunicaciones: separación y otras medidas

- **Gestión de switchers** Es importante proteger el acceso a los switchers, que pueden ser gestionables a través de una interfaz web o mediante una conexión vía serie. Los switchers de gama media o alta suelen ser gestionables y permiten aplicar salvaguardas como la separación en VLAN o habilitar cada puerto para una MAC específica.
- **Protocolo 802.1X** Este protocolo permite proteger las conexiones a un puerto del switcher. Funciona impidiendo el uso del switcher a equipos no autorizados, basándose en una lista con las direcciones MAC de los ordenadores autorizados. Usar switchers que soporten este protocolo es una medida básica para garantizar que solo los equipos autorizados se conecten a la red.
- **Pasarela de seguridad** La pasarela de seguridad, o firewall, que conecta la red de la empresa a internet, puede tener medidas de seguridad muy extensas. Las detallaremos más adelante.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Protección de las comunicaciones: separación y otras medidas



Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Cifrado de las comunicaciones: Ipsec

- IPsec es un protocolo de la capa de internet que aporta seguridad al protocolo IP, añadiéndole posibilidades de cifrado.
- Aporta seguridad a todos los protocolos superiores (principalmente a los protocolos de transporte TCP/UDP), sin necesidad de modificación alguna.

Ventajas de IPsec

- IPsec tiene una ventaja notable frente a otros protocolos que permiten el cifrado, como SSL y TLS, ya que estos operan en la capa de transporte.
- Cualquier aplicación funcionará con IPsec, sin modificación alguna.

Modos de funcionamiento de IPsec

- Modo transporte: orientado a comunicaciones de ordenador a ordenador, solo se cifra el contenido del paquete.
- Modo túnel: orientado a comunicaciones red a red, se cifra completamente el paquete. Se emplea sobre todo para las comunicaciones a través de internet o entre routers para el establecimiento de redes privadas virtuales (VPN).

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Cifrado de las comunicaciones: Ipsec

Implementaciones de IPsec

- Existen múltiples implementaciones de IPsec, según el sistema operativo.
- Como cualquier operación de red, IPsec debe configurarse y probarse fuera del entorno de producción, y antes de implantarse.

Rendimiento de las comunicaciones

- Las operaciones de cifrado y descifrado exigen la ejecución de algoritmos matemáticos complejos, lo que penaliza el rendimiento de las comunicaciones.
- El empleo de microprocesadores multinúcleo permite que esta operación se realice de manera más eficiente.

Es importante mencionar que TLS (Transport Layer Security) ha reemplazado a SSL (Secure Sockets Layer) como el protocolo estándar para el cifrado de tráfico web. Además, aunque IPsec sigue siendo relevante, especialmente en redes corporativas y para VPNs, TLS es más comúnmente utilizado para el cifrado de tráfico en la web. Por último, aunque IPsec es obligatorio en IPv6, la adopción de IPv6 ha sido más lenta de lo esperado, y IPv4 sigue siendo ampliamente utilizado.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Cifrado de las comunicaciones

Existen varios protocolos similares a IPsec. Algunos de los más conocidos son:

1. IKEv2/IPSec:

Es una combinación de dos protocolos: IKEv2 para la gestión de claves y IPSec para la seguridad de datos.

Ofrece una alta seguridad y velocidad, lo que lo convierte en una opción popular para VPNs.

Está implementado en la mayoría de los sistemas operativos, lo que facilita su uso.

2. WireGuard:

Es un protocolo relativamente nuevo que se destaca por su alta velocidad y seguridad.

Es de código abierto y está siendo auditado constantemente por la comunidad de seguridad.

Se está ganando popularidad como una alternativa a OpenVPN.

3. OpenVPN:

Es un protocolo VPN de código abierto y muy configurable.

Ofrece una alta seguridad y flexibilidad, pero puede ser un poco más complejo de configurar que otros protocolos.

Es una opción popular para usuarios avanzados que necesitan un alto grado de control sobre su conexión VPN.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Cifrado de las comunicaciones

4. L2TP/IPSec:

- Es una combinación de dos protocolos: L2TP para la creación de túneles y IPSec para la seguridad de datos.
- Es una opción popular para redes corporativas debido a su buena compatibilidad con diferentes dispositivos.
- Sin embargo, no es tan rápido como IKEv2/IPSec o WireGuard.

5. SSTP:

- Es un protocolo VPN desarrollado por Microsoft.
- Es fácil de configurar y usar, pero no es tan seguro como otros protocolos.
- Se recomienda su uso solo en entornos donde la facilidad de uso es más importante que la seguridad.

Al elegir un protocolo VPN, es importante considerar sus necesidades específicas. Factores a tener en cuenta son:

Nivel de seguridad: ¿Necesita la máxima seguridad posible o una seguridad básica es suficiente?

Velocidad: ¿Es importante para usted tener una conexión VPN rápida?

Compatibilidad: ¿Qué dispositivos necesita conectar con la VPN?

Facilidad de uso: ¿Qué tan fácil de configurar y usar es el protocolo?

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Cifrado de las comunicaciones

Protocolo	Seguridad	Velocidad	Compatibilidad	Facilidad de uso
IKEv2/IPSec	Alta	Alta	Buena	Buena
WireGuard	Alta	Alta	Buena	Regular
OpenVPN	Alta	Media	Buena	Regular
L2TP/IPSec	Buena	Media	Buena	Buena
SSTP	Media	Baja	Buena	Fácil

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Carpetas, impresoras y otros recursos

- Medidas de Protección: Se deben aplicar medidas de protección para los recursos compartidos, como impresoras y carpetas.
- Privilegios de Instalación: Las impresoras deben ser instaladas solo por usuarios con privilegios adecuados, según la guía CIS v1.2.
- Gestión de Controladores: Es importante gestionar los controladores de impresoras de manera formal para asegurar la uniformidad de versiones y la distribución rápida de parches de seguridad.
- Conectividad de Impresoras: Se recomienda evitar la conexión de impresoras a internet, y si es necesario, restringir las comunicaciones a direcciones IP conocidas y predefinidas.
- Control de Acceso: Las impresoras deben contar con un sistema de control de acceso integrado con el sistema de información de la empresa para gestionar los permisos de impresión.
- Impresión Segura: Se debe implementar un modo de impresión segura que requiera la autenticación del usuario antes de iniciar el trabajo de impresión.

Gestión segura de comunicaciones, carpetas compartidas, impresoras y otros recursos compartidos del sistema

Carpetas, impresoras y otros recursos

- Protección de Carpetas Compartidas: Se deben utilizar mecanismos de control de acceso lógico a las carpetas compartidas, aprovechando las capacidades de los sistemas operativos para especificar privilegios a recursos y archivos individuales.
- Control de Acceso: Los administradores deben controlar tanto el acceso de la aplicación como el acceso de los usuarios a los recursos del servidor para protegerse contra ataques de denegación de servicio.
- Almacenamiento y Control de Ficheros: Se recomienda utilizar discos o unidades lógicas separadas para las carpetas compartidas y aplicar sistemas de cuota de disco para limitar el espacio consumido por los usuarios.
- Revisión de Archivos: Los archivos cargados por los usuarios deben ser revisados en busca de contenido malicioso o ilegal antes de estar disponibles para el servidor.
- Control Adicional: Se deben aplicar medidas adicionales como limitar el número de procesos y conexiones simultáneas, así como configurar cortafuegos para proteger los servidores de carpetas compartidas.

Nota sobre Vulnerabilidades: Se debe tener cuidado con limitar el número de conexiones para evitar vulnerabilidades. Se recomienda aplicar controles de tiempo para liberar conexiones automáticamente y reducir el riesgo de explotación.

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Monitorización y registro

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

Vulnerabilidades de seguridad

- Las medidas de seguridad aplicadas tendrán vulnerabilidades.
- Estas medidas podrían verse desactivadas o inutilizadas, comprometiendo el sistema sin que se sepa.

ISO/IEC 27002:2013

Establece el objetivo de control “12.4 Registro de actividad y supervisión”.

- Para detectar las actividades no autorizadas, se deben monitorizar los sistemas e investigar los eventos de seguridad registrados.

Registro y gestión de eventos de actividad

- Se debe registrar toda actividad de seguridad que suceda en el sistema.
- La monitorización y el registro deben observar los requisitos legales de privacidad y la política de seguridad de la empresa.

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Monitorización y registro

Protección de los registros de información

- Si los registros de información se pueden alterar, no habrá evidencia de un acceso no autorizado.
- Los registros serán un objetivo importante para un atacante.

Sincronización de relojes

- Es necesario sincronizar los relojes para tener precisión al revisar eventos en distintos sistemas.
- Se deben aplicar mecanismos de ajuste automático con servidores de hora de referencia.

Protocolo NTP o PTP

- El protocolo NTP (Network Time Protocol) o el PTP permite sincronizar los relojes de los equipos.
- Este protocolo corrige el retraso que pueda introducir la red de comunicaciones y emplea el puerto 123 del protocolo de transporte UDP.

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Recomendaciones NIST

Recomendaciones de Monitorización y Registro según NIST

La guía NIST 800-123 destaca la importancia del registro de actividad, especialmente de eventos de seguridad, para mantener la seguridad en los servidores. Es vital elegir los datos adecuados a registrar y monitorear para mantener la integridad de los sistemas de información.

Monitoreo de Red y Sistema

Los registros de red y sistema son cruciales, especialmente si las comunicaciones están cifradas, lo que dificulta la monitorización del tráfico. Revisar los registros no solo es reactivo, sino que también puede revelar actividades sospechosas, incluyendo intentos de ataque e intrusión.

Beneficios de los Registros

Los registros proporcionan alertas sobre actividades sospechosas, trazabilidad de actividades hostiles, ayuda en la recuperación de servidores y evidencia para investigaciones posteriores. Es importante sincronizar la hora en todos los sistemas y considerar el tamaño de los registros, que puede requerir espacio considerable.

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Recomendaciones NIST

Protección y Copias de Seguridad de Registros

Los registros deben protegerse contra modificaciones o eliminaciones, preferiblemente almacenándolos en un servidor dedicado y utilizando protocolos estándar como syslog. Se recomienda realizar copias de seguridad de los registros durante períodos específicos, considerando obligaciones legales, requisitos de la empresa y tamaño de los registros.

Análisis y Frecuencia de Revisión

El análisis de registros debe ser regular, aumentando la frecuencia ante actividades sospechosas. Además, se debe realizar un análisis a largo plazo para detectar ataques premeditados. Se recomienda el uso de herramientas de análisis automático como SIEM (Security Information and Event Management) para facilitar la detección y alerta de actividades sospechosas.

Selección de Soluciones SIEM y Referencias CIS

Existen diversas soluciones SIEM disponibles, incluyendo opciones de licencia gratuita y de código abierto. Se recomienda seleccionar una solución que se ajuste al alcance necesario y facilite la interpretación de los resultados. Las guías CIS para sistemas Linux y Windows también destacan la importancia de mantener registros de auditoría de la actividad del sistema referente a la seguridad.

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Uso inadecuado de los sistemas de información

Uso adecuado de los sistemas de información
Establecer medidas organizativas que dicten las condiciones de uso adecuado de los sistemas de información.
Aumentará la conciencia de seguridad de los usuarios y reducirá la posibilidad de incidentes.

Equilibrio entre seguridad y uso eficiente
Existen muchas referencias, criterios y consideraciones que deben tenerse en cuenta.
Se debe alcanzar un equilibrio entre seguridad y uso eficiente de los recursos.

Norma relativa al Esquema Nacional de Seguridad
Se recomienda considerar la aplicación de criterios recogidos en la norma relativa al Esquema Nacional de Seguridad,
Accesible desde la página web del CCN (Centro Criptológico Nacional).

Monitorización de la seguridad y el uso adecuado de los sistemas de información

Uso inadecuado de los sistemas de información

No se podrá acceder a los recursos informáticos y telemáticos para desarrollar actividades que persigan o tengan como consecuencia:

- Uso intensivo de recursos para usos no profesionales
- Degradación de los servicios.
- Modificación no autorizada y premeditada de información.
- Violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
- Deterioro intencionado del trabajo de otras personas.
- Uso de los sistemas de información para fines ajenos a los de la organización, salvo excepciones que se contemplen expresamente.
- Daño intencionado y actividades ilícitas
- Dañar intencionadamente los recursos informáticos de la organización o de otras instituciones.
- Incurrir en cualquier otra actividad ilícita, del tipo que sea.

En lugar de simplemente prohibir el “uso intensivo de recursos para usos no profesionales”, se podrían considerar políticas más flexibles que permitan cierto uso personal de los recursos de la empresa, siempre y cuando no interfiera con las operaciones empresariales. Esto puede ayudar a mejorar la satisfacción y la productividad de los empleados.

Resumen

Es crucial reducir las debilidades en los servidores que dan servicio a los ordenadores cliente para proteger los sistemas de las numerosas amenazas lógicas a las que están expuestos. Este proceso se conoce como robustecimiento y requiere un análisis detallado de cada sistema, ya que las debilidades variarán de uno a otro. Cuanto mejor se conozca el sistema en producción y se corrijan los fallos conocidos, menos probable es que una amenaza, que suele aprovechar un error específico, oculto y concreto del sistema, tenga efecto.

Existen guías proporcionadas por fabricantes y entidades como NIST y CIS que deben seguirse para robustecer un sistema. Sin embargo, algunas recomendaciones básicas de la norma ISO 27002 son esenciales:

- Modificar los usuarios y contraseñas por defecto del sistema y no mantener activas aquellas con identificador estándar.
- Configurar las directivas de contraseñas en términos de longitud, complejidad, histórico sin repetición, periodo máximo y mínimo de vigencia, además del bloqueo por intentos de acceso fallidos.
- Desinstalar todas las aplicaciones y servicios innecesarios para reducir la superficie de ataque de un sistema. Si es posible, usar sistemas para funciones únicas.
- Emplear servicios y protocolos seguros, generalmente mediante SSL y TLS, que añaden técnicas de cifrado para proteger las comunicaciones.
- Mantenerse informado de las vulnerabilidades descubiertas para aplicar los parches de corrección y seguridad que se liberen. Evitar la aplicación automática en entornos de producción sin probarse antes.

Resumen

- Proteger los sistemas de código malicioso con programas específicos, en las conexiones a internet, y donde se usen medios extraíbles.
- Gestionar de manera segura las comunicaciones, mediante la separación de redes, medidas de seguridad en la electrónica de red, y el uso de cortafuegos.
- Monitorizar la seguridad, usar los registros de auditoría del sistema con herramientas de análisis y alerta automático. Promover el uso correcto de los sistemas especificando usos prohibidos.

Estas medidas deben ser proporcionales al riesgo de los sistemas, pero siempre debería haber una aplicación mínima de los aspectos señalados.