



SEGURIDAD INFORMÁTICA

JOSÉ PABLO
HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.8.0. Capítulo 8
Parte 1 de 2

Robustecimiento de sistemas

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Reducir la vulnerabilidad de un sistema (robustecimiento o securización de sistemas) permite reducir el riesgo de una amenaza, aplicándose casi en exclusividad a la seguridad lógica del sistema.

Dependerá de la función, servicio, protocolo, o aplicación concreta que corra en el sistema y requiere conocerla, al menos tan exhaustivamente como el atacante.

Debe aplicarse el principio de proporcionalidad.

Tres directrices:

- **Minimizar la superficie de un ataque lógico eliminar aplicaciones y servicios innecesarios.**
- **Eliminar usuarios innecesarios.**
- **Revisión continua.**

2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN

Si los sistemas operativos y las aplicaciones incorporan cuentas de usuario, y contraseñas creadas por el fabricante y públicamente conocidas, el control de acceso lógico a esos productos no es eficaz, hasta modificar las contraseñas para recuperar su confidencialidad.

ISO 17799 en relación a credenciales.

2.1. USUARIOS Y CONTRASEÑAS POR DEFECTO

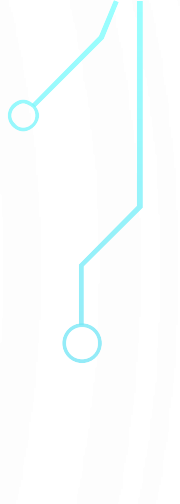
El control “11.2.3 Gestión de claves secretas de los usuarios”, fija que:

- **Los usuarios deben firmar un compromiso para mantener la confidencialidad de las claves.**
- **Cuando se proporcione una contraseña temporal a los usuarios, debe ser segura, y deben estar obligados a cambiarla.**
- **Al entregar una clave secreta a un usuario, se debe hacer de modo que se verifique su identidad.**
- **Las claves deben entregarse a los usuarios de manera segura.**
- **Las claves temporales serán seguras y únicas.**
- **Los usuarios deben reconocer la recepción de claves temporales.**
- **Las claves no se almacenarán sin protección.**
- **Las claves predeterminadas deben cambiarse tras la instalación del sistema o aplicación.**



2.1. USUARIOS Y CONTRASEÑAS POR DEFECTO

No solo deben modificarse las contraseñas de los usuarios por defecto, de manera que la autenticación sea factible, sino que siempre que sea posible, deben deshabilitarse los usuarios que el sistema incorpora por defecto.



2.2. REFERENCIAS Y DIRECTRICES

- **INTECO (Instituto Nacional de Tecnologías de la Comunicación)**, que proporciona guías para securizar servidores web, etc.
- **CCN (Centro Criptológico Nacional)**, que bajo registro proporciona guías para securizar sistemas operativos
- **NIST (National Institute of Standards and Technology)**, que proporciona una extensa biblioteca sobre seguridad de la información. Se puede descargar libremente la serie 800 de: <http://csrc.nist.gov>.
- **CIS (Center for Internet Security)**, que proporciona una extensa colección de guías de comparación o benchmarking, de robustecimiento de distintos sistemas (Windows, Linux, etc.).
- Puede buscar las guías gratuitas de comparación de seguridad (Security benchmarking) <https://benchmarks.cisecurity.org/>.

3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

Las contraseñas deben cumplir unos requisitos mínimos:

- **la longitud**
- **la variedad de caracteres empleados**
- **el periodo de vigencia**
- **no permitir la coincidencia con las claves anteriores**

3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

La autenticación de un usuario se basa en que este aporte al sistema:

- **Algo que se tiene (como una tarjeta de identificación).**
- **Algo que se es (una característica biométrica).**
- **Algo que se sabe (una contraseña).**

3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

La norma ISO 17799:2005 establece en su control “11.2.2 Gestión de privilegios”, que se debe restringir y controlar la asignación y uso de privilegios mediante un proceso de autorización formal, que contemple:

- Identificar a que usuarios hay que dar acceso a cada recurso.
- Los privilegios deben otorgarse en base a la necesidad de saber.
- Mantener proceso de autorización y registro, y no otorgarlos hasta que se complete.
- Es preferible el empleo de rutinas, u otros mecanismos automáticos del sistema, que eviten la necesidad de otorgar privilegios.
- Es preferible usar programas que eviten la necesidad de ejecutarse con privilegios.
- Los privilegios deben otorgarse a un identificador de usuario, diferente del utilizado en el uso normal y diario de la empresa.

3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS

la norma ISO 17799:2005 establece en el control “11.3.1 Uso de claves secretas”, que deben ser de calidad, con longitud suficiente, y que además, cumplan:

- Que sean fáciles de recordar.
- Que no se basen en nada fácilmente adivinable como información de la persona.
- Que no incluyan palabras incluidas en diccionarios.
- Que estén libres de caracteres consecutivos idénticos, todos numéricos o alfanuméricos.
- Que se cambien regularmente, o en base al número de accesos, evitando reutilizar de claves anteriores.

3.1. DIRECTRICES EN GUÍAS NIST

NIST 800-123 punto 4.2.2 indica que las reglas o política de contraseñas debe fijar:

- (a) la longitud mínima.
- (b) la complejidad, empleando mezcla de diferentes tipos de caracteres para reducir el posible éxito de un ataque de ensayo de error de palabras contenidas en diccionarios.
- (c) el periodo de validez de una contraseña.
- (d) la reutilización de contraseñas que evite emplear las anteriores.
- (e) la autoridad para cambiar o restablecer las contraseñas.
- (f) la seguridad de las contraseñas en lo referente a que se almacenen cifradas en el servidor, e incluso que se usen claves diferentes para la administración del servidor, y para otras labores de administración.

3.2. DIRECTRICES EN GUÍAS CIS

Para Windows se establecen los siguientes elementos a configurar, desde las políticas de grupo del directorio activo para los requisitos de las contraseñas:

(1.1.1.5.2.2) Longitud mínima de la contraseña de 8 caracteres, salvo en entornos de alta seguridad, donde se recomiendan 14 caracteres.

(1.1.1.5.2.3) Edad máxima de la contraseña de 60 días.

(1.1.1.5.2.5) Edad mínima de la contraseña de 1 día.

(1.1.1.5.2.6) Complejidad de la contraseña requerida.

(1.1.1.5.2.4) Histórico de contraseñas a recordar, para no repetir ninguna de las últimas 24 contraseñas empleadas.

(1.1.1.5.2.1) Deshabilitar almacenamiento de contraseñas con cifrado reversible.

3.2. DIRECTRICES EN GUÍAS CIS

Para Linux, se establecen los siguientes elementos a configurar para el subsistema de contraseñas PAM, que extiende el sistema de contraseñas por defecto, e integrable con OpenLDAP:

(7.9) Requerir autenticación para el modo de arranque de un solo usuario (que con acceso a la consola local, permite arrancar el sistema sin contraseña, y operativo como el usuario root), configurando la aplicación de arranque LILO o GRUB para ello.

Nota: LILO son las iniciales del gestor de arranque Linux Loader, y GRUB son las iniciales del gestor de arranque Grand Unified Bootloader.

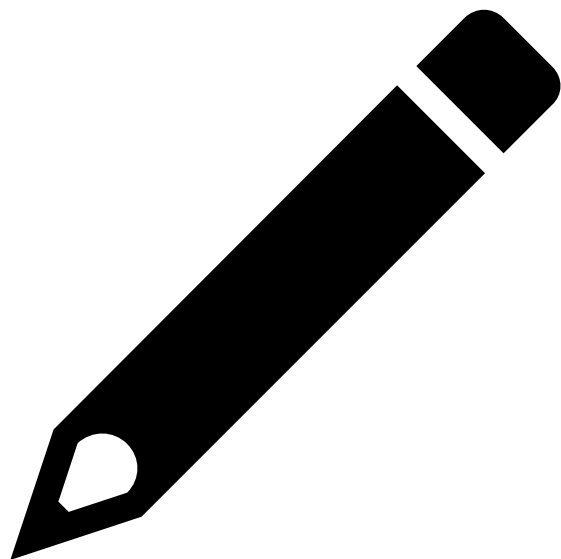
Ambas aplicaciones permiten modificar el modo en que arranca el sistema, incluidas opciones referentes al sistema de ficheros, o al inicio en modo multiusuario o monousuario.

(8.2) Verificar que no hay cuentas con contraseñas vacías.

(8.3) Ajustar el periodo en que expiran las contraseñas así como el periodo mínimo de vigencia.

(8.4) Asegurar que no quedan entradas “+” en archivos de contraseñas o de grupos, procedentes de sistemas antiguos.

(7.1) Deshabilitar “.rhosts” de la configuración PAM.



Actividades

LA POLÍTICA DE CONTRASEÑAS DE UNA EMPRESA, DONDE SE EMPLEA UN SERVIDOR WINDOWS, FIJA QUE TENGAN MÁS DE 12 CARACTERES, QUE NO COINCIDAN CON LAS 3 ANTERIORES, QUE SE USEN MAYÚSCULAS, MINÚSCULAS, Y NÚMEROS, Y QUE SE CAMBIEN AL MENOS CADA 15 DÍAS. ESTAS MEDIDAS GENERAN DESCONTENTO ENTRE LOS USUARIOS QUE LAS APUNTAN, SE LAS INTERCAMBIAN, Y LAS RESTABLECEN VARIAS VECES SEGUIDAS PARA MANTENER SIEMPRE LA MISMA. SE LE PIDE CORREGIR LA SITUACIÓN, DANDO PARÁMETROS CONCRETOS DE ACUERDO A LAS RECOMENDACIONES CIS PARA LOS REQUISITOS DE LAS CONTRASEÑAS.

Actividades



SOLUCIÓN

EMPLEANDO LAS RECOMENDACIONES CIS PARA WINDOWS:

LA LONGITUD DEBERÍA REDUCIRSE, A 8 CARACTERES.

EL PERIODO DE VIGENCIA DEBERÍA INCREMENTARSE A 60 DÍAS.

HAY QUE DISPONER UN PERIODO DE VIGENCIA MÍNIMO DE 1 DÍA.

SE DEBE AUMENTAR A 24 EL NÚMERO DE CLAVES SIN REPETIR.

4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES

Se aborda ahora el análisis de las consideraciones de seguridad que se deben observar en las aplicaciones que permanezcan instaladas en los sistemas, y específicamente, en las implicaciones para con las comunicaciones que ello pueda acarrear.

4.1. HERRAMIENTAS Y OTRAS APLICACIONES

El robustecimiento persigue minimizar la superficie de ataque de un sistema.

Es primordial eliminar todas las herramientas, utilidades, aplicaciones, y servicios que no sean estrictamente necesarios:

- **Medidas técnicas de revisión, y desinstalación de aplicaciones innecesarias.**
- **Medidas normativas que regulen la instalación de software.**

4.1. HERRAMIENTAS Y OTRAS APLICACIONES

Norma ISO 17799:2005

“12.5.1 Procedimientos de control del cambio”, se deben controlar los cambios con procedimientos formales para minimizar la corrupción de los sistemas. La introducción de nuevos sistemas, o las modificaciones de los existentes, deben hacerse según un proceso de: documentación, especificación, prueba, control de calidad, y puesta en marcha. Sobre todo, el software nuevo debe probarse en un entorno separado.

“12.5.4 Filtrado de información”, para el que deben evitarse oportunidades como las que ofrecen el uso y explotación de puertos o canales de manera disimulada, o encubierta por algunas aplicaciones. Se recomienda analizar el tráfico del equipo, y hacer uso de aplicaciones considerados de la más alta integridad, y siempre evaluadas previamente.

“15.1 Cumplimiento de los requerimientos legales”, aporta la contramedida **“15.1.5 Prevención del mal uso de los medios de procesamiento de la información”,** que fija que se debe disuadir a los usuarios de emplear los medios de procesamiento de la información para propósitos no autorizados, lo que incluye el empleo de utilidades no permitidas para fines no autorizados.

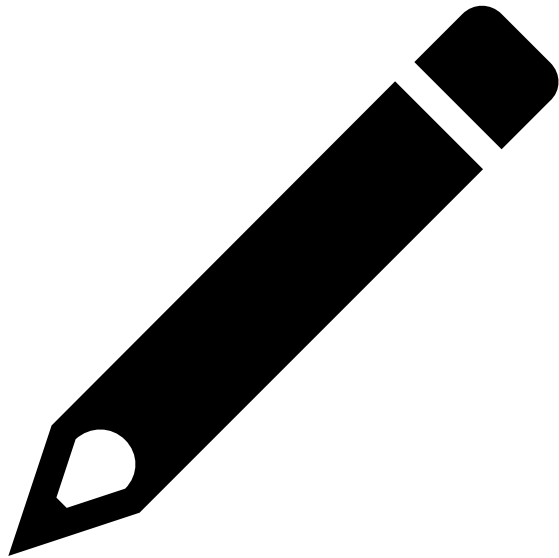
4.1. HERRAMIENTAS Y OTRAS APLICACIONES

Guía CCN-STIC 821

El apéndice I, desarrolla una “Normativa general de utilización de los recursos y sistemas de información del organismo (NG00)”:

- Solo el personal de soporte técnico autorizado podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios, con la excepción de las herramientas de uso común, que puedan ser descargables desde servidores internos.
- Los usuarios podrán solicitar la inclusión de una aplicación, lo que debe ser estudiado, al menos por el personal técnico de seguridad.
- No se podrá instalar software que no disponga de licencia correspondiente, o cuya utilización no sea conforme con la legislación vigente en materia de propiedad intelectual.
- Se prohíbe la reproducción, modificación, transformación, cesión, comunicación, o uso fuera de la empresa de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la empresa.
- No se podrán deshabilitar o eliminar las aplicaciones instaladas por la empresa, especialmente las relacionadas con la seguridad.

Actividades



EN UN SISTEMA WINDOWS, EJECUTE “SERVICES.MSC”, PARA CONSULTAR QUÉ SERVICIOS ESTÁN EN EJECUCIÓN, Y CUÁLES PODRÍAN INICIARSE DE MANERA AUTOMÁTICA. EXPLORE LAS PROPIEDADES DE UN SERVICIO PARA VER CÓMO DESHABILITARLO.

4.2. COMUNICACIONES Y PUERTOS DE RED

ISO 17799:2005. Objetivo de control “11.4 Control de acceso a la red”:

- “11.4.1 Política sobre el uso de los servicios de red”, resulta relevante, porque dicta que los usuarios sólo deberían tener acceso a los servicios para los cuales hayan sido autorizados.
- “11.4.2 Autenticación del usuario para conexiones externas”, ya que no basta con deshabilitar el resto de puertos, sino que en los puertos habilitados el acceso debe mantenerse autenticado (empleando técnicas de criptografía, dispositivos hardware o un mecanismo de desafío/respuesta, o redes privadas virtuales).
- “11.4.5 Segregación de redes”, que establece que los sistemas y/o grupos de usuarios deben separarse en diferentes redes.
- “11.4.6 Control de conexión a la red”, que establece que se debe restringir la capacidad de conexión de los usuarios a la red, empleando, por ejemplo, pasarelas de red o gateways, con tablas o reglas predefinidas para restringir el uso del correo, la transferencia de archivos, el acceso para iniciar una sesión interactiva remota, o el acceso a una aplicación concreta.

4.2. COMUNICACIONES Y PUERTOS DE RED

CCN-STIC 821-Apéndice 2(NP10):

- **Usar internet para fines profesionales.**
- **No visitar páginas de contenido poco ético, ofensivo o ilegal.**
- **No visitar páginas no fiables o sospechosas.**
- **Cuidar la información que se publica en internet.**
- **Observar las restricciones legales que sean de aplicación.**
- **Realizar descargas solo si se tiene autorización.**
- **No descargar código o programas no confiables.**
- **Asegurar la autenticidad de la página visitada.**
- **Comprobar la seguridad de la conexión.**

4.2. COMUNICACIONES Y PUERTOS DE RED

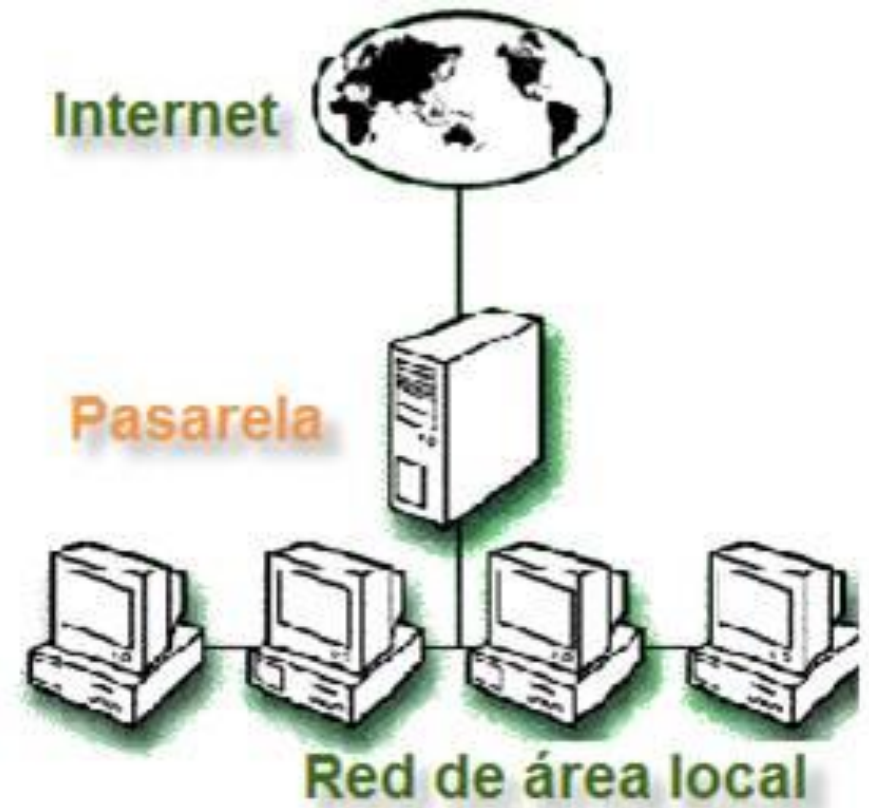
CCN-STIC 821-Apéndice 2(NP10):

- **Cerrar las sesiones al terminar la conexión.**
- **Utilizar herramientas contra código dañino.**
- **Mantener actualizado el navegador y las herramientas de seguridad. Utilizar los niveles de seguridad del navegador.**
- **Desactivar las cookies.**
- **Eliminar la información privada.**
- **No instalar complementos desconocidos.**
- **Limitar y vigilar la ejecución de programas en el navegador como applets y scripts.**

4.3. PASARELAS DE SEGURIDAD

Una pasarela, puerta de enlace o puerta de acceso (“gateway”) es un equipo de comunicaciones que interconecta redes con arquitecturas diferentes, realizando para ello funciones avanzadas de traducción de protocolos entre ambas redes.

Normalmente, la empresa empleará arquitectura de red TCP/IP, y estará conectada a internet, de manera que las pasarelas serán dispositivos que extiendan las funciones de un router. Tal es el caso de las pasarelas de seguridad, que añaden normalmente servicios de antivirus o de detección de intrusos, para tomar decisiones sobre las conexiones que se permiten.



4.4. DIRECTRICES EN GUÍAS NIST

NIST 800-123 Apartado 4.2.1

Una aplicación de servidor debería estar en un equipo u ordenador dedicado a esta única función.

Cuando se instale el sistema operativo, debe realizarse una instalación mínima, para posteriormente añadir todos los servicios y aplicaciones que se necesiten.

El enfoque contrario (si no es posible realizar una instalación mínima) consiste en eliminar todas las aplicaciones, servicios y protocolos de red innecesarios tras la instalación estándar.

Desinstalar es siempre preferible a desactivar o bloquear, porque aquello que no existe no tiene vulnerabilidad alguna. Sin embargo, algo deshabilitado o bloqueado puede volver a habilitarse, por error humano o intencionadamente

4.4. DIRECTRICES EN GUÍAS NIST

NIST 800-123 Apartado 4.2.1

Entre los servicios que se deben revisar expresamente, en esta guía señala los siguientes:

- **Servicios para compartir archivos e impresoras.**
- **Servicios de comunicaciones inalámbricas.**
- **Servicios de control y acceso remoto, especialmente los no cifrados, como es el caso de Telnet.**
- **Servicios de directorio (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.**

4.5. DIRECTRICES EN GUÍAS CIS

Para sistemas operativos Linux, CIS recomienda en su guía de comparación v.1.0.5 desactivar aquellos servicios que no son verdaderamente necesarios.

También se recomiendan desactivar dos grandes grupos de aplicaciones:

- **Los innecesarios, basados en el servicio xinitd (servicios basados en la conexión a internet como FTP, TFTP, Telnet, POP, IMAP, RLOGIN)**
- **Los servicios innecesarios en el arranque del sistema (sendmail, login gráfico, X Font server, SMB, NFS, NIS, RPC, NETFS, SNMP, demonio de impresión, procesos del servidor web, procesos de SNMP, servidor DNS, servidor SQL, procesos de Webmin, etc.).**

4.5. DIRECTRICES EN GUÍAS CIS

Para sistemas operativos Windows, CIS recomienda en su guía v2.1 revisar unos 160 aspectos sobre los servicios del sistema, detallados en la sección 1.1.1.1 (por ejemplo servicio de fax, de replicación de archivos, FTP, servicio de ayuda y soporte, el servicio HTTPS, servicio de indexación de contenidos, Messenger, POP3, servicio de impresión, etc.).