

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRSI11

CONTROL DE CAMBIOS

Cambio en Formato a partir del PGCRC02 Elaboración de información Documentada
Organización de la información

1. OBJETIVO

Establecer los métodos estándar para mantener actualizados y habilitados los controles de seguridad en el sistema operativo de Comercializadora Rápido S.A. de C.V., así como identificar y gestionar el hardening de los activos de la información con el fin de minimizar los riesgos de seguridad.

2. ALCANCE

Aplica el alcance de endurecimiento de servidores, equipos de trabajo administrativos, operativos y dispositivos de sistema Punto de Venta.

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
<u>Cid Palacios Jesús David</u> Administrador de infraestructura	<u>Pitol Pimentel Carlos Adrián</u> Gerente de Sistemas	<u>Martínez Ponce Janely</u> Gestión de Calidad	<u>Montes Barrera Elliioth Abdel</u> Gerente General

3. REFERENCIAS

ISO/IEC 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

4. DEFINICIONES Y ABREVIATURAS

4.1 Hardening:

Acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de los equipos.

4.2 VPN:

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

4.3 Firewall:

Es un sistema cuya función es prevenir y proteger a una o varias redes, de intrusiones o ataques de otras redes, bloqueándole el acceso

5. RESPONSABILIDADES

5.1 Gerente General


Aprobar la información documentada del SGC, asegurando que los recursos necesarios estén disponibles para lograr sin problema la implementación efectiva del documento.

5.2 Administrador de infraestructura

Es responsabilidad de Administrador de Infraestructura de establecer mecanismos para la protección de datos e información sensible o reservada.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 1 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRS111

5.3 Jefe de Sistemas

Es responsabilidad de Jefe de Sistemas IT implementar y cumplir las políticas, metodologías y procedimientos definidos en las operaciones de seguridad de la información.

5.4 Gestión de Calidad

Gestionar el cumplimiento documental según lo establecido en el SGC, asegura su adecuada implementación, manteniendo la eficacia, así como la mejora continua de estas, resguardando y emitiendo la documentación controlada.

5.5 Auxiliar de Sistemas IT

Es responsabilidad de Auxiliar de Sistemas aplicar los procedimientos de Hardening en los equipos de trabajo administrativos, operativos y dispositivos de sistema Punto de Venta de Comercializadora Rápido S.A. de C.V.

6. DESARROLLO

6.1 Generalidades

El Administrador de infraestructura y/o auxiliar de sistemas IT, son los responsables del seguimiento de la instalación de cada uno de los equipos hasta le mantenimiento continuo de cada uno de estos, a continuación, se describe el proceso para mantener el Hardening:


- **Instalación de sistema operativo:** Esta actividad consiste en el despliegue de los sistemas operativos en los equipos administrativos, operativos (POS) y servidores.
- **Configuración del Sistema operativo inicial:** Se asigna un nombre a cada equipo conectado a la red de 724.
- **Deshabilitar servicios necesarios:** A partir de este punto se inicia con los parámetros de seguridad básica a aplicar en los servidores, aplicativo de políticas y controles de conexión.
- **Remover aplicaciones innecesarias:** Si existen aplicaciones que se hayan instalado en el despliegue de los sistemas operativos, este debe ser inmediatamente desinstalado.
- **Actualización del Sistema Operativo Windows:** Todo equipo de red existentes dentro de 724 y desarrollos de programas (POS) deben encontrarse actualizado con las versiones más recientes.
- **Instalación de antivirus:** Todos los servidores, equipos administrativos y operativos de la Organización deben contar con ESET ENDPOINT ANTIVIRUS instalado y con licencia vigente.
- **Proceso de respaldo (backups):** Todo equipo en la red de Comercializadora rápido S.A. de C.V. debe contar con backup de datos.
- **Aplicar seguridad complementaria:** Se aplica herramienta WinGuard para aplicar políticas de bloqueos, fondos de pantalla y seguridad en estaciones de trabajo y servidores, definidos por Sistemas IT de Comercializadora Rápido S.A. de C.V. según políticas de seguridad y administración del directorio activo y sistemas operativos.
- **Mantenimiento de los dispositivos:** Para el aseguramiento del funcionamiento y correcto uso de los dispositivos se realiza la revisión de los equipos en campo.

6.2 Uso de Firewall (fortigate)

Todos los equipos que se manejan dentro de la red de Comercializadora Rápido cuentan con el firewall del sistema operativo activo y con las políticas que permitan solo el uso de las aplicaciones que el usuario estará

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 2 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRS11

manejando. Esta herramienta permite a Comercializadora Rápido S.A. de C.V. controlar el tráfico de red que llegan y salen en conexión con el Host. para mayor información del procedimiento actual de firewall ver **Reglas Firewall PECRS12**

6.3 Cifrado

Actualmente se cuenta con la herramienta Bitlocker habilitada en todos los equipos para cifrar la información de todos los equipos de cómputo de comercializadora Rápido, ver **Cifrado de Datos y Resguardo de llaves PECRS15**.

6.4 Buenas Prácticas en Sistemas Operativos

Mantener actualizado el sistema operativo y las aplicaciones con sus correspondientes parches de seguridad como buena práctica para evitar intrusiones a través de fallas dentro de los sistemas operativos.

También se siguen recomendaciones para robustecer la seguridad como son:

- Evitar utilizar servicios que no son seguros
- Deshabilitar las carpetas compartidas
- Utilizar contraseñas fuertes
- Crear un perfil de usuario con privilegios restringidos
- Deshabilitar la ejecución automática de dispositivos USB
- Configurar la visualización de archivos ocultos
- Configurar la visualización de las extensiones de archivos.
- Revisión del programa de antivirus ESET ENDPOINT ANTIVIRUS

6.5 Protección en el correo electrónico

Se cuenta con la configuración del filtro dentro del servicio de Telmex para detección de correo SPAM y la detección de correos maliciosos, adicional a la protección que proporciona el programa ESET Endpoint Antivirus para la detección en línea del correo electrónico.

6.6 Backup's

Se realizan todos los días por las noches un respaldo de los equipos de los usuarios para mantener la información importante salvaguardada en caso de ocurrir algún contratiempo con el equipo.


6.6.1 Backup Correo Electrónico

Los equipos administrativos, y equipos POS de la organización cuentan con un respaldo de correo electrónico; específicamente para los casos especiales de cambio del equipo se hace un traspaso de la información empleando la siguiente metodología:

- El usuario se dirige a Panel de control del equipo al que inicialmente se encontraba en operación y se desea realizar el back up de correo. Selecciona el marcador de Correo
- En la ventana emergente configuración de correo, seleccione Archivo de datos.
- Seleccionar la pestaña Abrir ubicación de archivos
- Se transfieren datos a unidad externa de datos al disco duro Unidad C:\ Nombre del usuario\documentos\archivos Outlook\Nombre del correo electrónico .pst

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 3 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRSI11

- Copia a respaldo y se finaliza el proceso.

6.7 Antivirus ESET endpoint antivirus

Utilizado en las computadoras de forma global dentro de las instalaciones y oficinas de Comercializadora Rápido S.A. de C.V. para el monitoreo diario de las condiciones generales de los equipos, así como la valoración de la amenaza, este proceso se describe en el **Configuración y Administración de antivirus PECRSI07**

Todos los equipos se centralizan en un servidor para poder mostrar un reporte de los equipos.

Se considera que los equipos deben reiniciarse, cada vez que se actualiza el antivirus, esta tarea es propia del antivirus ya que detecta que puede presentar una vulnerabilidad en los mecanismos de esta.

El periodo que tiene de utilidad es por un año, se observa en administración de licencias para asegurar la cobertura del tiempo activo del antivirus.

Las actividades de monitoreo y verificación de las actividades que puedan presentar alguna amenaza en la funcionalidad y operatividad de los equipos recae en el auxiliar de Sistemas de IT.

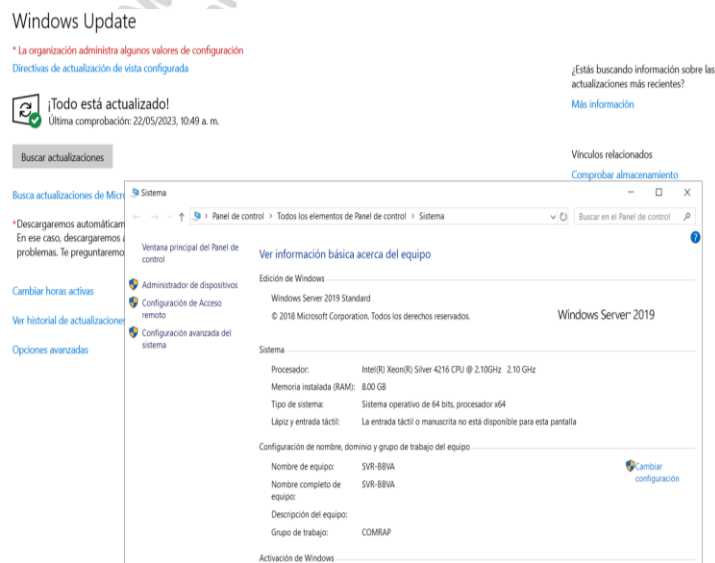
6.8 Actualización del sistema operativo

Actualmente se consideran dentro de las actividades de endurecimiento de la seguridad de la información; tiene como objetivo que los sistemas operativos cumplan con los criterios que puedan comprender toda la extensión de operación. Los equipos de operación que se encuentran en las sucursales de 7/24 MIX cumplen con este punto de actualización derivado del compromiso de la organización en mantener seguras las computadoras de oficinas y sucursales.

6.8.1 El servidor de base de datos


Se encuentra las con actualizaciones al día y con sistema operativo dentro del ciclo de vida del proveedor.

Ejemplo: Base de datos



Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 4 de 6
--	-----------------------	--------------------------

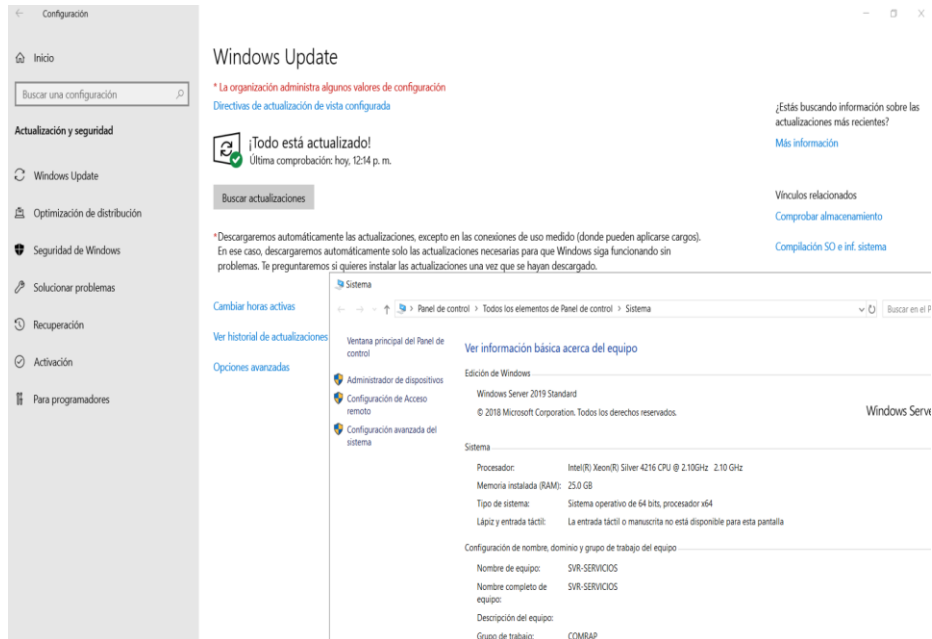
"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRSI11

6.8.2 El servidor del Web Service (Servicios)

Se encuentra con actualizaciones al día y con sistema operativo dentro del ciclo de vida del proveedor.

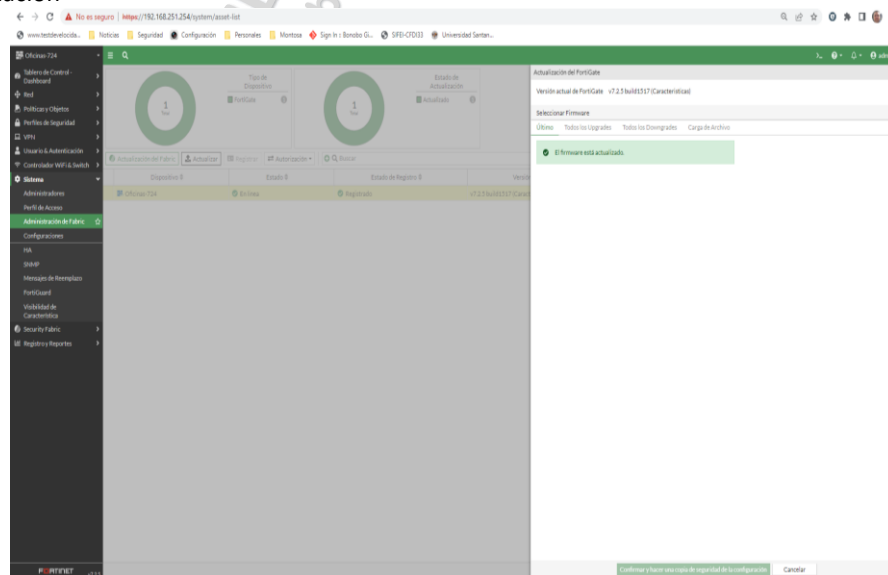
Ejemplo: Actualizaciones



6.8.3 Firewall de acceso de sucursales


Se encuentra dentro del ciclo de vida del proveedor y con la última actualización recomendada por el fabricante.

Ejemplo: Actualización



Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 5 de 6
--	-----------------------	--------------------------

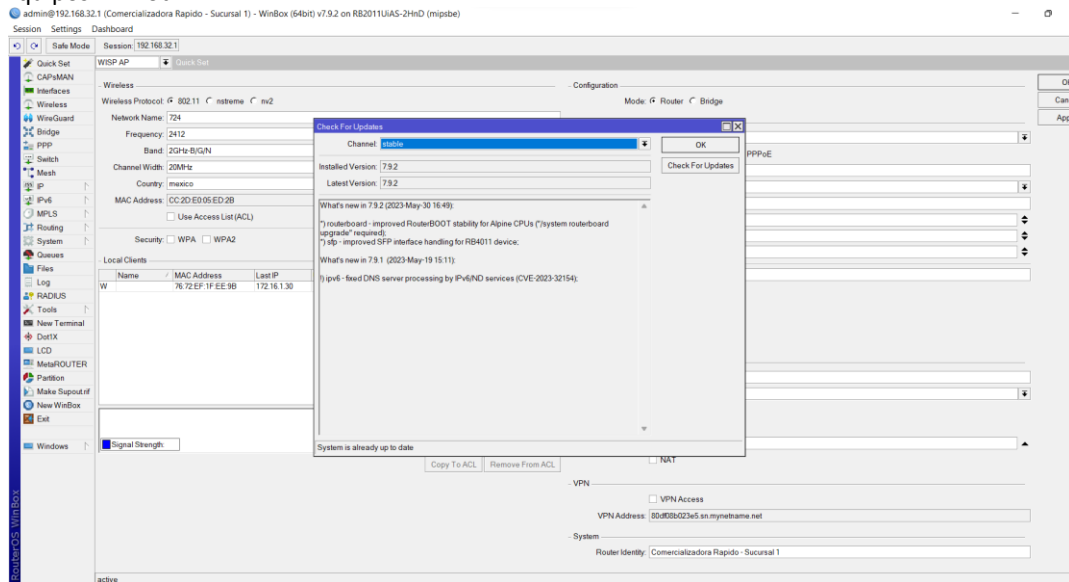
"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"

	COMERCIALIZADORA RÁPIDO S.A DE C.V	
	Tipo de documento:	Procedimiento específico
	Título:	Hardening
	Código:	PECRSI11

6.8.4 Equipos Mikrotik

En sucursales se encuentran dentro del ciclo de vida del fabricante y con la última actualización recomendada por el fabricante.

Ejemplo: Equipos Mikrotik



7. DIAGRAMA DE FLUJO

Puesto involucrado	Puesto involucrado	Puesto involucrado	Puesto involucrado
NA	NA	NA	NA

8. ANEXOS

TIPO	CODIGO	TITULO
Formato	NA	NA
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	PECRSI12	Reglas Firewall
	PECRSI15	Cifrado de Datos y Resguardo de llaves
	PECRSI07	Configuración y Administración de antivirus

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 6 de 6
--	-----------------------	--------------------------

"Cualquier documento impreso diferente del original y cualquier archivo electrónico que se encuentre fuera del Portal de Gestión de Calidad será considerado como Copia No Controlada"