


| | | |
|---|---|--|
|  | COMERCIALIZADORA RÁPIDO S.A. DE C.V. | |
| | Tipo de documento: | Procedimiento específico |
| | Título: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

CONTROL DE CAMBIOS

Cambio en Formato a partir del PGCRGC02 Elaboración de información Documentada
Organización de información

1. OBJETIVO

Gestionar los mecanismos que nos permitan poder responder de forma centralizada ante las posibles amenazas y monitoreo de los equipos para detectar vulnerabilidades y tomar acciones de corrección y mejora.

2. ALCANCE

Aplica a todos Equipo de software conectados al servidor dentro de las ubicaciones de Comercializadora Rápido S.A. de C.V.

| | | | |
|--|--|--|---|
| Elaboró: | Vo. Bo. | Revisó: | Aprobó: |
| <u>Romero Girón Carmen Belem</u> Auxiliar de Sistemas | <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 27001:2022 Sistemas de gestión de la seguridad de la información (SGSI)

4. DEFINICIONES Y ABREVIATURAS

4.1 Virus informático:

Es una amenaza que daña los archivos del ordenador.

4.2 Gusanos informáticos:

Es un programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red.

4.3 Troyanos:

Software que se presenta como un programa útil, engañando a los usuarios para permitir la ejecución.

4.4 Adware:

Forma abreviada de software relacionado con publicidad.

4.5 Spyware:

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento del usuario.


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.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 1 de 9 |
|--|-----------------------|--------------------------|

"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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

5.2 Gerente de sistemas

Garantizar el cumplimiento de la gestión de antivirus, manteniendo el monitoreo de los equipos para detectar vulnerabilidades y la efectiva solución de cada una de las vulnerabilidades.

5.3 Auxiliar Sistemas IT

Es el responsable de la ejecución del procedimiento y monitoreo de los equipos, la revisión y verificación de las políticas del antivirus.

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.

6. DESARROLLO

6.1 Generalidades en el Uso del antivirus

Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario en Comercializadora Rápido S.A. de C.V, se monitorean diariamente los estados de los equipos ante virus posibles, garantizando la funcionalidad y protección de los mismos.

Las actualizaciones y configuraciones quedaran registradas en el formato **Actualización/configuración ESET Endpoint antivirus PECRSI07_F01(2)**.

6.2 Manual de usuario

Para establecer las políticas del antivirus y hacer uso de la herramienta de seguridad de información; los equipos deben contar con la instalación del software ESET ENDPOINT ANTIVIRUS versión. 8.01 en conjunto del agente Management Agent 8.02.

Todos los equipos que se utilizan en la Organización cuentan con la aplicación de protección ante amenazas; diseñado para ayudar a detectar, prevenir y eliminar el malware en los dispositivos, tales como virus, gusanos bots, troyanos, etc.


En el manual de usuario de **ESET Endpoint Antivirus PECRSI07_EEA01(1)**, el cual sirve de referencia para la configuración y toma de acciones. El ingreso a este software, el responsable del monitoreo y de los cambios deberá ingresar su identificación como usuario y su respectiva contraseña.

6.3 Instalación

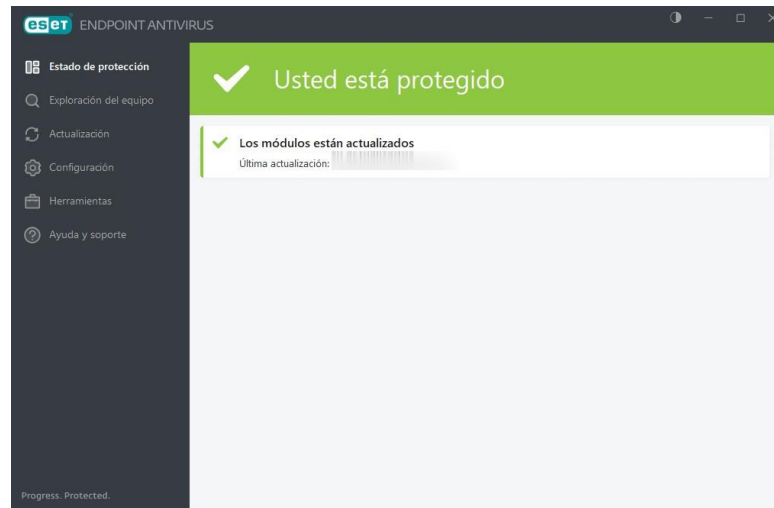
Los equipos de Comercializadora Rápido S.A. de C.V, deberán contar con la instalación, licencia vigente y actualización del antivirus; así como establecer políticas de seguridad para aminorar la vulnerabilidad de ataques por virus informáticos; estableciendo mecanismos de protección y obstruir todos los medios de acceso que generen amenazas al sistema de la información.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 2 de 9 |
|--|-----------------------|--------------------------|

"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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |




Ejemplo: Instalación



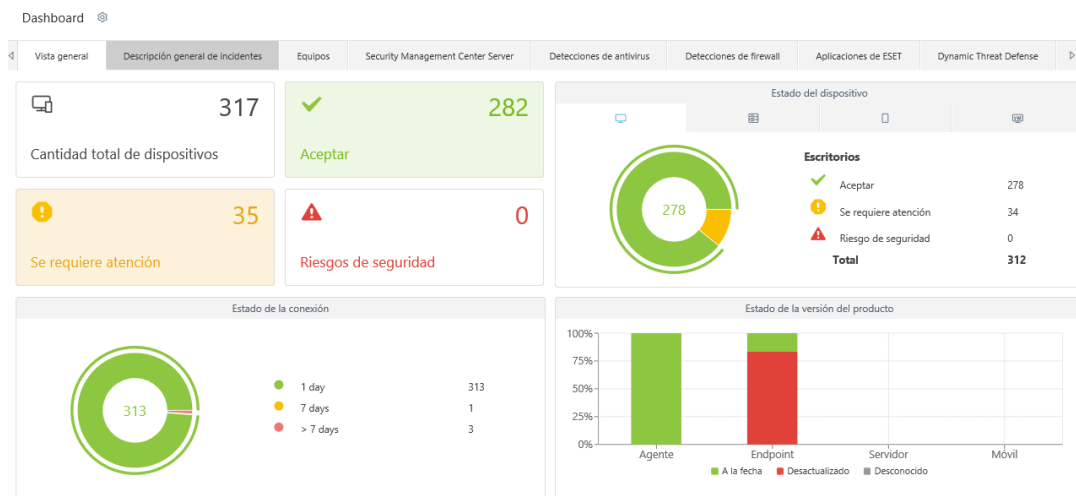
6.4 Información general de estado

La herramienta cuenta con un desglose del análisis de las vulnerabilidades posibles; cuenta con una herramienta útil y detallada: el dashboard con el que cuenta permite observar en concreto las licencias activas en los equipos de la organización.

Así como las alertas de peligrosidad que son representadas por un semáforo de colores siendo el usuario alertado de la amenaza latente en el equipo:

| | |
|---|---------------------------|
|  | Aceptado |
|  | Notificación de seguridad |
|  | Riesgo de seguridad |


Ejemplo: Desglose del análisis de las vulnerabilidades Dashboard



El usuario puede observar: Vista general; el estatus actual de todos los equipos que han sido escaneados.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 3 de 9 |
|--|-----------------------|--------------------------|

"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"

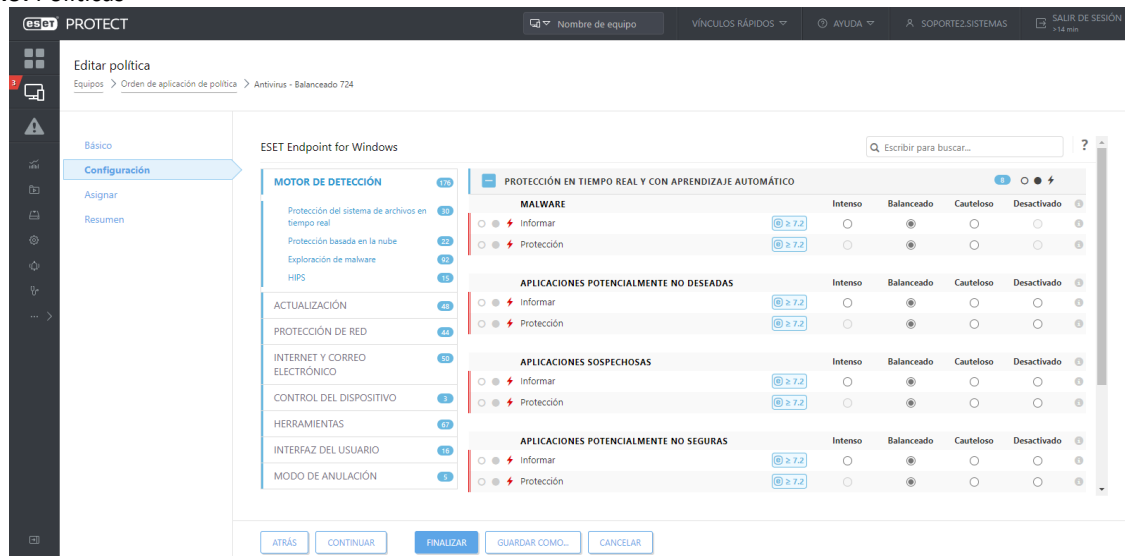
| | | |
|---|---|--|
|  | COMERCIALIZADORA RÁPIDO S.A. DE C.V. | |
| | Tipo de documento: | Procedimiento específico |
| | Título: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

Para las tareas del usuario; el auxiliar de sistemas se dirige a la opción mencionada y puede visualizar el avance de la protección de los equipos. Tiempo estimado de la operación cerca de 10 minutos para el escaneo de los 317 equipos actuales aproximadamente de Comercializadora Rápido S.A. de C.V.

6.5 Políticas.

Para el proceso de las políticas que se han creado en Comercializadora Rápido S.A. de C.V. se personaliza de acuerdo a los criterios convenientes para la protección de los equipos que se encuentran activos en 7/24.

Ejemplo: Políticas



Se atribuye el nombre de “El balanceado 724” para la política vigente de la Organización.

El software analiza las unidades locales (Disco Duro interno), de igual forma analiza cada unidad extraíble, unidades de red (esto se ejecuta al ingreso de carpetas compartidas para el análisis de algún virus). La forma de analizar algún archivo lo va a realizar al abrirse dicho documento, así como explorar un archivo creado o modificado, cuando se ejecuta o cuando explora un sector de inicio de medios extraíbles tras conectarse a un dispositivo.

Para la detección de: Malware /Aplicaciones potencialmente no deseadas/aplicaciones sospechosas/Aplicaciones potencialmente no segura; se realiza la edición de política:


6.5.1 Metodología para editar política

Se ingresa en configuración avanzada y en Motor de detección, por default vienen las opciones de INFORMAR Y PROTECCIÓN, el auxiliar escoge las opciones de acuerdo a las necesidades de detección que se desean: Intenso/Balanceado/Cauteloso/desactivado.

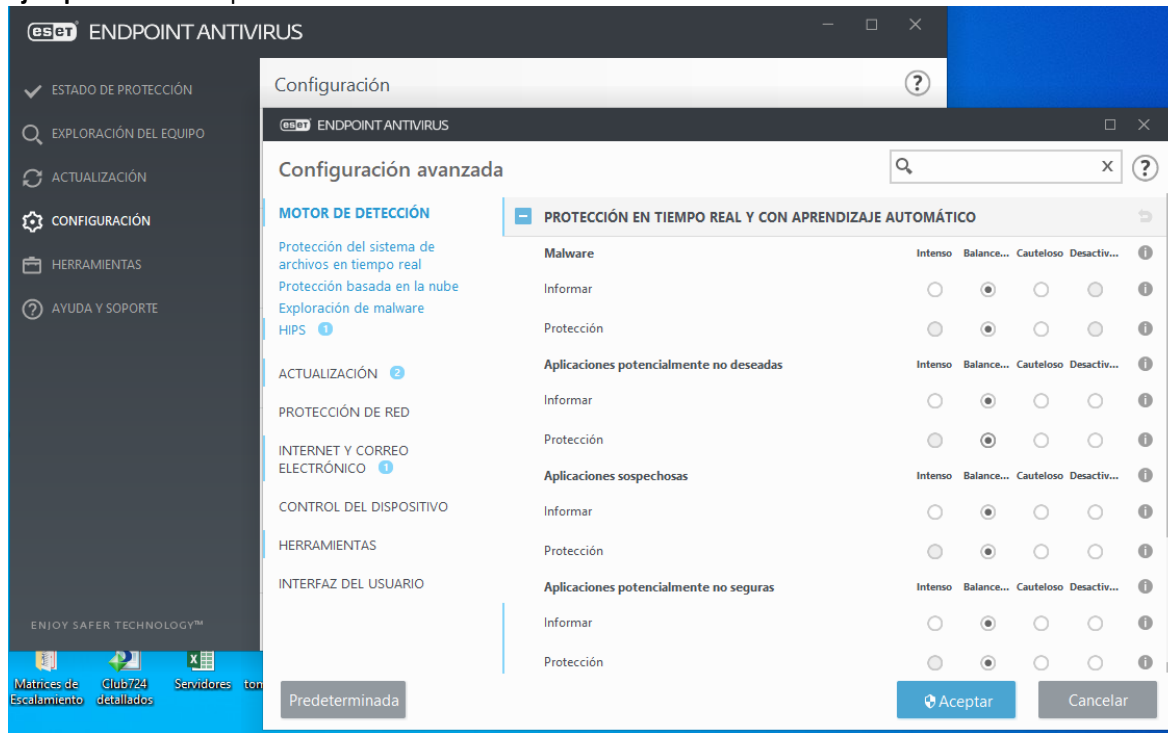
NOTA: La política actual de 724, se tiene activo la opción de balanceado

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 4 de 9 |
|--|-----------------------|--------------------------|

“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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

Ejemplo: Edición de políticas




6.1 Riesgos de seguridad.

Actualmente, el software de seguridad ESET Endpoint Antivirus utilizado contra códigos maliciosos permite identificar un porcentaje muy elevado de este tipo de amenazas informáticas. Sin embargo, en ausencia de estas soluciones existen altas posibilidades de padecer un incidente por malware, ya sea por falta de actualización del software, una configuración errónea o malas prácticas aplicadas a la Seguridad Informática. Esto representa una dificultad para saber de manera precisa si se está ante una infección, puesto que la mayoría de las amenazas buscan pasar inadvertidas. Sin embargo, esto no aplica en todos los casos, ya que existe malware que se hace evidente al usuario cuando infecta su equipo, es importante que se identifiquen ciertos criterios que a continuación se presentan:

- Bajo desempeño en el procesamiento de tareas en el equipo.
- Aparición de ventanas y anuncios emergentes que no han sido solicitadas por el usuario.
- Aparición de programas instalados en el equipo sin el conocimiento y consentimiento del usuario.
- Comportamiento anormal del sistema operativo, como reinicio o apagado repentino.
- Fallas durante la descarga de actualizaciones del sistema operativo o de programas instalados.
- Funcionalidades deshabilitadas del sistema operativo o de programas.
- Lentitud al navegar por Internet o durante la descarga de archivos.
- Alertas de seguridad por parte del sistema operativo o de supuestas soluciones antivirus.
- Imposibilidad de iniciar el sistema operativo tanto en “modo normal” como en “modo seguro”.
- Cambio de página de inicio de Internet o redirección a sitios web desconocidos.
- Cambio del fondo de escritorio u otro aspecto del sistema.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 5 de 9 |
|--|-----------------------|--------------------------|

“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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

- Mensajes intimidatorios para el usuario o solicitud de pagos para recuperar información.
- Conexiones de red entrantes y salientes por puertos y protocolos comúnmente no utilizados.

De manera general, este tipo de comportamientos podrían determinar que uno o más equipos se encuentran infectados. Ante las dudas, el método más fehaciente es el análisis y exploración que pueda realizar una solución de seguridad contra códigos maliciosos.

6.2 Riesgos de seguridad asociados al malware

Relacionados con una infección, existen una infinidad de riesgos de seguridad asociados con los códigos maliciosos, que pueden ir desde robar o dañar información, hasta afectar los sistemas, equipos o redes.

En otras palabras, todo aquel programa que atenta contra la confidencialidad, integridad o disponibilidad de la información perteneciente a los usuarios u organizaciones debe ser identificado como malware.

Por ello, más allá del robo de información sensible, las consecuencias derivadas de una afectación a alguna de las propiedades de los datos antes mencionadas, pueden magnificar los efectos negativos como la fuga de datos teniendo impactos e implicaciones.

6.3 Gestión de vulnerabilidades.

Documentos asociados: **Política Respuesta a Incidentes PECRSI14_PO01(2), Evaluación de incidentes de seguridad de la información PECRSI14 y PECRSI20_F01(2) Matriz de vulnerabilidades.**

6.3.1 Identificar la infección

Un incidente de seguridad relacionado con malware puede ser detectado de diferentes maneras y con distintos niveles de detalle, y para hacerlo se pueden utilizar desde herramientas de detección automatizadas (escaneo actual) como **consolas** que centralizan la información relacionada con amenazas identificadas en los equipos administrados hasta medios manuales, así como un **reporte de falla** de un usuario que considere un comportamiento anormal en su sistema.

Algunos incidentes muestran signos que facilitan la detección, no obstante, se pueden presentar ocasiones en donde es casi imposible detectarlos si no se cuenta con herramientas adecuadas. Por lo tanto, reconocer los indicios de infección es fundamental para conocer los equipos infectados y la información que puede estar en riesgo.


Las actividades de detección de malware pueden aplicarse a distintos niveles dentro de la organización:

- Nivel de host (en los sistemas operativos de servidores y estaciones de trabajo)
- Nivel de aplicaciones de servidor (correo electrónico o proxy) y,
- Nivel de aplicaciones de cliente (correo electrónico).

Independientemente de la manera en la cual se lleve a cabo, la detección es el paso inicial para atender un incidente por malware.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 6 de 9 |
|--|-----------------------|--------------------------|

"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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

6.3.2 Determinar el alcance de la infección

Luego de la identificación de una infección por malware, es necesario determinar la cantidad de sistemas que han sido comprometidos y de qué manera, con el propósito de conocer el alcance de la infección y el impacto que puede representar. Por ejemplo, si está limitada a un único equipo, un conjunto de ellos, una subred o, en casos más graves, a toda la red corporativa.

Conocer el alcance de una infección permite calcular los recursos que serán necesarios para solucionar los inconvenientes que haya generado. Además, permite saber los sistemas que han sido comprometidos, junto con la criticidad de la información que almacenan, procesan o transmiten.

Por otro lado, a partir del tipo de malware y su comportamiento, también es posible determinar saber si se ha filtrado información sensible, si se han visto comprometidos datos corporativos o privados de los empleados y/o de clientes. En general, es necesario identificar la información y los sistemas que han sido dañados para estimar las consecuencias negativas.

6.3.3 Mantener la continuidad de las operaciones

En el caso de incidentes por malware, luego de conocer el alcance de la infección, se podrá determinar si información sensible o equipos críticos se han visto afectados. En función de este resultado, se podrán tomar decisiones para continuar correctamente con las operaciones de Comercializadora Rápido S.A. de C.V.

6.3.4 Contención de acciones maliciosas.

Las estrategias de contención pueden variar en función del incidente y de los lineamientos establecidos por los equipos de respuesta, lo que a su vez depende del tipo de malware que afecte a la organización.

- Aislamiento del equipo: Una manera de iniciar esta fase está relacionada con el aislamiento de los equipos que se sabe que están comprometidos.
- Segmentación de las redes: La suspensión de los segmentos de red de los cuales forman parte evita que la infección pueda propagarse a través de la red corporativa e interrumpe cualquier conexión que pueda establecerse con el atacante para el robo de información.
- Identificación del ataque: La identificación del vector de ataque resulta fundamental para contener los estragos generados por un código malicioso y evitar su propagación.

Es importante la previsión para manejar incidentes que utilizan los vectores más comunes: propagación e infección a través de medios externos y removibles, explotación de vulnerabilidades en el software y sitios web, archivos adjuntos a correos electrónicos y enlaces a sitios que alojan malware.


Los ataques por malware pueden deberse a una campaña masiva de propagación que infectan los equipos de manera casual, quizá por malas prácticas de los usuarios, o bien puede tratarse de un ataque dirigido y con un propósito específico. En todos estos casos, una vez que se haya identificado el vector de ataque, se podrán aplicar distintas acciones en función de las características de la muestra de malware.

6.3.5 Erradicar la infección.

A partir de la identificación del método de propagación, es obligatorio llevar a cabo algunas acciones que mitiguen de manera específica el vector, por ejemplo el filtrado de correo electrónico y análisis de los mensajes y adjuntos, la modificación de los sistemas operativos para evitar la ejecución de programas de manera automática cuando se introduce un dispositivo removable, la actualización de software necesario

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 7 de 9 |
|--|-----------------------|--------------------------|

"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: | Configuración y Administración de antivirus |
| | Código: | PECRS107 |

para evitar la explotación de alguna vulnerabilidad que permita el ingreso de malware a la red corporativa, entre otras acciones.

Es necesario definir si la infección fue el simple resultado de un descuido en la Web o si, por el contrario, constituye el eslabón exitoso dentro de una cadena de ataques persistentes y dirigidos. Si se determina que la infección tuvo como objetivo específico a la organización, entonces se debe tener en mente que un nuevo ataque puede ser inminente. Por ello, el análisis de las piezas maliciosas debe orientarse a determinar las acciones específicas del malware, cómo puede ser detectado en la red, así como también medir y contener su daño.

6.3.6 Recuperación.

La fase de recuperación se presenta luego de que un incidente por malware ha sido contenido y de que se han identificado y mitigado las vulnerabilidades que fueron explotadas.

Llegado este punto, se confirma que los sistemas se encuentran funcionando de manera normal y que el malware ha sido removido para evitar incidentes similares. La recuperación puede incluir acciones como la restauración de sistemas operativos y respaldos, el reemplazo de archivos infectados, la instalación de parches de seguridad y actualizaciones, el cambio de contraseñas en los sistemas, el refuerzo de la seguridad perimetral a través de nuevas reglas de firewall, la creación de listas de control de acceso o el desarrollo de nuevas firmas de malware.

A partir de los patrones identificados, es posible determinar que si un ataque cumplió su cometido malicioso y si se intentarán nuevos casos de una manera similar. Por este motivo, es fundamental eliminar de raíz los problemas para mantener la seguridad; cabe destacar que esto logra con el conocimiento pleno del código malicioso.

6.3.7 Registro.

Realizar una investigación de lo acontecido permite mejorar los procesos dentro de la organización y que los equipos de respuesta evolucionen para enfrentar nuevas amenazas. El análisis puede llevarse a cabo por el comité de riesgos encargado de atender las incidencias.

Con la investigación y posterior mitigación de vulnerabilidades que eran desconocidas, surge la oportunidad de fortalecer el perímetro de las redes y de identificar otros potenciales puntos de acceso a los sistemas que antes no habían sido considerados.

6.3.8 Tiempo de respuesta


El tiempo de recuperación dependerá en gran medida de las consecuencias generadas por la infección, por lo que no se puede establecer un periodo para alcanzarla, aunque siempre se busca que sea en el menor tiempo posible.

6.3.9 Acciones de mejora.

En los eventos detectados, se lleva un registro de las situaciones de ataque presentado y el comité de riesgos deberá verificar el cumplimiento de las normas, procedimientos y controles establecidos mediante auditorías técnicas y registros de actividad de los sistemas como base para la monitorización del estado del riesgo en los sistemas y descubrimiento de nuevos riesgos.

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 8 de 9 |
|--|-----------------------|--------------------------|

"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: | Configuración y Administración de antivirus |
| | Código: | PECRSI07 |

7. DIAGRAMA DE FLUJO

| Puesto involucrado | Puesto involucrado | Puesto involucrado | Puesto involucrado |
|--------------------|--------------------|--------------------|--------------------|
| NA | NA | NA | NA |

8. ANEXOS

| TIPO | CODIGO | TITULO |
|---------------------------|-------------------|---|
| Formato | PECRSI07_F01(2) | Actualización/configuración ESET Endpoint antivirus |
| Ayuda visual | NA | NA |
| Políticas | NA | NA |
| Otros (documento externo) | PECRSI07_EEA01(1) | ESET Endpoint Antivirus |
| | PECRSI14_PO01(2) | Política Respuesta a Incidentes |
| | PECRSI14 | Evaluación de incidentes de seguridad de la información |
| | PECRSI20_F01(2) | Matriz de vulnerabilidades |

DOCUMENTO CONTROLADO
Prohibida su reproducción

| | | |
|--|-----------------------|--------------------------|
| Vigente a partir de: 29-ABR-2024 | Revisión: 3 | Página: 9 de 9 |
|--|-----------------------|--------------------------|

"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"