	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRSI20</b>

#### CONTROL DE CAMBIOS

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

### 1. OBJETIVO

Establecer el procedimiento que garantice a los activos de la información, la continuidad y ejecución de las operaciones para la prevención y tratamiento de vulnerabilidades en los componentes de las TIC's que; soportan los procesos de información de Comercializadora Rápido S.A de C.V y que puedan representar un riesgo.

### 2. ALCANCE

El alcance del presente procedimiento contempla los sistemas de la infraestructura informática de Comercializadora Rápido S.A. de C.V, y dirigido a los interesados y responsables de la infraestructura tecnológica y de la seguridad de la información de la Organización.

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

### 3. REFERENCIAS

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

ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información

### 4. DEFINICIONES Y ABREVIATURAS

#### 4.1 Ataque:

Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo

#### 4.2 Activo:


Componente físico o lógico relacionado con la información y sus procesos de tratamiento, y que tiene valor para la empresa. La entidad asigna un valor a cada activo que representa el nivel de importancia que tiene el activo en el proceso del negocio.

#### 4.3 Activo de la información:

Se refiere a toda la información o elemento de información que la entidad recibe o produce en el ejercicio de sus funciones. Incluye la información que se encuentre presente en forma impresa, escrita, en papel, transmitida por cualquier medio electrónico o almacenado en equipos de cómputo, incluyendo software, hardware, recurso humano, datos contenidos en registros, archivos, bases de datos, videos e imágenes, que tengan valor para la entidad.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>1 de 8</b>
--	-----------------------	--------------------------

"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"

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRS120</b>

#### 4.4 Amenaza de seguridad de la información:

Surgen a partir de la existencia de vulnerabilidades, es decir, que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

#### 4.5 Análisis Forense de Seguridad de la Información (Information Security Forensics):

Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.

#### 4.6 Arquitectura de red:

Descripción, especificación y configuración de los componentes físicos o lógicos en una conexión de dispositivos que comparten recursos.

#### 4.7 Autenticación:

Garantía de que una característica reivindicada de una entidad es correcta

#### 4.8 Ciberataque:

En computadoras y redes de computadoras un ataque es un intento de exponer, alterar, desestabilizar, eliminar para obtener acceso sin autorización o utilizar un activo. Está asociado a cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo tomar el control, desestabilizar o dañar un sistema informático (ordenador, red privada etc.)

#### 4.9 Código malicioso:

Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

#### 4.10 Control

Medida que modifica un riesgo.

### 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 Gerente de Sistemas IT


Es responsable de garantizar la adecuada implementación del presente procedimiento para la aplicación del tratamiento de vulnerabilidades.

#### 5.3 Administrador de la Infraestructura

Es responsable de la detección temprana de las vulnerabilidades en de las TIC's para evitar riesgos que afecten el seguimiento de las actividades de Comercializadora Rápido S.A. de C.V. Dar difusión y aviso con el Comité de Riesgos de las vulnerabilidades encontradas para activar los controles de seguridad y solución que mitiguen el riesgo. Evaluar el riesgo e implementar las medidas/controles correspondientes a las

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>2 de 8</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRS120</b>

vulnerabilidades detectadas. Documentar las evidencias del tratamiento de vulnerabilidades y los tiempos de recuperación de los sistemas.

#### 5.4 Auxiliar de Sistemas IT.

Mantener un inventario de activos de información debidamente actualizado y vigente, como base para el tratamiento eficaz de las vulnerabilidades. Cuenta con la información de los servicios especializados y técnicos internos/externos suficientes para apoyar en el proceso de gestión de vulnerabilidades, tales como los proveedores de HW y SW, empresa de telecomunicaciones y otros.

#### 5.5 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

La gestión de vulnerabilidades es el proceso en el que se identifican las vulnerabilidades en TI y se evalúan los riesgos que éstos representen; esta evaluación ayuda a detectar y aplicar los controles de forma temprana para minimizar o mitigar el riesgo, se desarrolla la detección de vulnerabilidades de acuerdo a la siguiente imagen.


**Ejemplo:** Gestión de Vulnerabilidades 724



- a) Para la programación y tratamiento de vulnerabilidades es necesario que se utilice la herramienta de seguimiento, para ello se asignan responsables de las actividades y controles.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>3 de 8</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRS120</b>

- b) Contar con el inventario de activos actualizado y utilizado en toda la red de Comercializadora Rápido S.A. de C.V, esto para identificar quien es el usuario vigente y cuál es la ubicación.
- c) Ejecutar las pruebas de vulnerabilidad involucra escaneos y agentes autenticados, proporciona información de datos sobre vulnerabilidades.
- d) Analizar las vulnerabilidades: ante un gran hallazgo de vulnerabilidades, será necesario definir cuáles son las primeras que deben repararse y centrarse en los activos con mayor probabilidad de ser explorados.
- e) Remediar (Acciones Preventivas/Correctivas): Una vez identificados y priorizados los hallazgos se ejecuta el plan de acción que mitigará o eliminará las vulnerabilidades en este documento se deberá contar con el responsable de las acciones adecuadas.
- f) Por ello se realizará el registro de las acciones correctivas de acuerdo a la planeación que se proyecte periódicamente o las necesidades identificadas durante el cumplimiento de las funciones de administración de las TIC's.

## 6.2 Programación y tratamiento de vulnerabilidades.

Dentro de esta fase principal se establecen los requerimientos para la gestión de la vulnerabilidad identificada, los responsables de seguimiento, los recursos necesarios, las actividades implicadas y el nivel de riesgo que representan para Comercializadora Rápido S.A. de C.V., el objetivo principal es la identificación de los requerimientos para el análisis y alcance de la vulnerabilidad, en dónde se aplicarán los controles de mitigación incluyendo pruebas, el alcance de las TIC's afectadas, tipo de pruebas que se ejecutaran por ejemplo:


- Escaneos contratados con externos, pruebas de penetración caja negra, caja gris o caja blanca.
- Las solicitudes explícitas de escaneo de vulnerabilidades solicitud del área responsable, cumplimientos regulatorios, solicitudes de auditoría, apoyo a proyectos previo a su puesta en producción, etc.
- Resultados de análisis de vulnerabilidades o pruebas de penetración realizados con anterioridad.
- Validar con Gerente de Sistemas IT y Administrador de Infraestructura de los sistemas el alcance del análisis y de las pruebas de vulnerabilidad con el fin de determinar los tiempos de ejecución, horarios, recursos, restricciones, requisitos o cualquier tema relacionado con la disponibilidad o criticidad de los dispositivos seleccionados.
- Identificar la herramienta que se empleará para la realización de las pruebas, esta debe ser una herramienta específica para la detección de vulnerabilidades, pueden ser tanto de software para correr sobre sistemas operativos tradicionales con ZenMap 7.91. A nivel de Hardware, los principales fabricantes que comercializan este tipo de tecnología son: Fortinet y Eset Point.

## 6.3 Inventario de activos actualizado.

Para la identificación y protección general de los equipos y recursos informáticos que se encuentren disponibles para algún posible ataque y represente una amenaza a los dispositivos de HW y SW de Comercializadora Rápido; se debe contar con un inventario para identificar cada uno de los dispositivos utilizados en la infraestructura que soportan los procesos del negocio; para tal fin, debe iniciarse con el inventario de los servicios prestados, continuar con la relación de los procesos asociados a estos servicios y de allí, determinar el listado de los activos o dispositivos que soportan estos procesos.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>4 de 8</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRS120</b>

La lista de Equipos y aplicativos está administrada por el departamento de Sistemas de Tecnología de la Información. Dicha lista de la infraestructura tecnológica debe estar continuamente actualizada y completa para el análisis y el tratamiento de las vulnerabilidades, ver **Ejemplo Reporte de activos informático724 PECRS120\_AV01(2)**.

La revisión del inventario debe ser verificada continuamente para evitar que se haya descartado algún activo de información considerado como crítico y que representen una vulnerabilidad severa. Se considera potencialmente expuestos a amenazas: los servidores, base de datos, routers, firewall, switches, y fortinet.

#### 6.4 Pruebas de vulnerabilidad.

En esta tercera fase se llevará a cabo la prueba para el análisis de vulnerabilidad, una vez realizada, se analizan los datos resultantes y finaliza con la entrega de reportes técnicos de la ejecución de la prueba, a continuación, se desglosan los aspectos a considerar:

- Programación adecuada de pruebas (considerar que se realicen en horarios y día de bajo tráfico red)
- Dimensionar el impacto que pueda representar.
- Implementar estrategias de contingencia para activos críticos con los responsables del Plan de Continuidad del Negocio.
- Considerar antes de la prueba realizar respaldos de la información de los activos involucrados.
- Registro del tiempo de respuesta excesivos o incidentes en el restablecimiento de los servicios.
- Utilización de CPU en servidores críticos
- Informar a los usuarios críticos de la realización de las pruebas.
- Analizar si las medidas adoptadas han disminuido la exposición y el nivel de riesgo.
- Realizar las pruebas utilizando herramientas de código abierto para analizar la vulnerabilidad de la aplicación, base de datos, de la red y/o dispositivos móviles.
- Hacer pruebas de caja negra y caja blanca para encontrar los agujeros de seguridad al menos una vez por año.

#### 6.5 Clasificación de activos o dispositivos con base en la confidencialidad de la información.

- **Información sensible:** Se considera todo documento que contiene información personal y privada de un individuo, empresa, números de cuenta, datos personales, contraseñas, claves privadas de acceso a los sistemas y/o algún dato que pueda presentar una vulnerabilidad a la seguridad de la información.
- **Información de confidencialidad:** Información que se encuentra únicamente accesible a personal u organizaciones autorizadas a dicha información. Garantizar que la información solo es accesible para aquellos autorizados a tener acceso.


La información que se considera crítica para la continuidad del proceso debe encontrarse almacenada en los activos y estos deben clasificarse de acuerdo a la importancia del contenido.

Su clasificación:

- **Confidencial (C).** Aplica a toda información de gran relevancia para Comercializadora Rápido S.A. de C.V.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>5 de 8</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRSI20</b>

- **Restringido (R).** Accesible únicamente para determinado personal de la organización y sin la cual no pueden desempeñar su trabajo.
- **Uso interno (I).** Accesible para todo el personal de la empresa exclusivamente.

Posteriormente se debe crear un esquema de priorización teniendo en cuenta los impactos sobre la continuidad del servicio agrupando los servidores o estaciones de trabajo, siempre y cuando se cuente con la certeza que aquellos seleccionados para esta agrupación. A continuación, se deben seleccionar la(s) aplicaciones y artefactos tecnológicos que, por su sensibilidad e impacto pudieran tener una consecuencia negativa para la entidad en caso de que pudiese materializarse una vulnerabilidad. Finalmente, en esta etapa se realizan análisis de los datos, redes, aplicaciones, bases de datos y dispositivos móviles con servicios de escaneo de vulnerabilidades.

ACTIVOS DE LA INFORMACIÓN 724	CLASIFICACIÓN	IMPACTO
Base de datos de clientes de corresponsalías	<b>C</b>	<b>ALTO</b>
Equipos POS	<b>I</b>	<b>MEDIO</b>
SW POS	<b>R</b>	<b>MEDIO</b>
Servidores	<b>C</b>	<b>ALTO</b>
API's	<b>C</b>	<b>ALTO</b>
Correo Organizacional	<b>I</b>	<b>MEDIO</b>
Sistema administrativo	<b>R</b>	<b>MEDIO</b>
Contratos	<b>I</b>	<b>BAJO</b>
Documentación SGSI	<b>R</b>	<b>MEDIO</b>


## 6.6 Análisis y reportes

Basado en los resultados de las diferentes herramientas utilizadas sobre las pruebas y/o la extracción de información obtenida de las mismas, se deben desarrollar informes tanto técnicos como ejecutivos teniendo en cuenta aspectos definidos en el programa de trabajo y aspectos como los descritos a continuación:

- Se debe analizar cada uno de los resultados teniendo en cuenta los activos de información y el nivel de criticidad establecidos de acuerdo al análisis interno y al contratado externamente.
- Se debe realizar análisis y validación de resultados con el objetivo de identificar falsos positivos; este ítem aplica exclusivamente sobre el análisis de vulnerabilidades debido a que las pruebas de penetración garantizan la confirmación de la vulnerabilidad.
- Realizar comparaciones con los análisis anteriormente realizados.
- Se deben organizar las vulnerabilidades de acuerdo con su nivel de criticidad conforme a la escala mostrada a continuación y el impacto para el negocio de lo cual se obtiene la priorización de las vulnerabilidades más críticas:

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>6 de 8</b>
--	-----------------------	--------------------------

*"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"*

	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRSI20</b>

VALOR	NIVEL CRÍTICO	MEDIDAS A TOMAR
15 a 25	URGENTE	El daño derivado de la materialización de la amenaza tiene consecuencias GRAVES para la organización.
6 a 12	MEDIO	El daño derivado de la materialización de la amenaza tiene consecuencias MODERADAS para la organización.
1 a 5	MINIMO	El daño derivado de la materialización de la amenaza NO tiene consecuencias relevantes para la organización.

- Realizar recomendaciones y elaborar informes para cada uno de los grupos o seccionales identificadas en el plan de trabajo.

### 6.7 Remediación

La última fase donde se establecen las acciones correctivas para mitigar las vulnerabilidades identificadas, las cuales serán registradas y deberán ser detalladas para crear los procedimientos de mitigación, para tal efecto se empleará el uso de herramientas de mejora continua como la **Matriz de vulnerabilidades PECRSI20\_F01(2)**

En el formato deberá incluir el nivel de la criticidad de cada una de las vulnerabilidades encontradas y se anexa la tabla de tiempos máximos para ejecución de acciones correctivas las cuáles deben ser aplicadas en el corto, mediano o largo plazo. Además, cada uno de los hallazgos deberá registrarse lo siguiente: los responsables de las acciones correctivas y seguimiento, los tiempos de revisión, los recursos o la capacidad de las TIC's.

### 6.8 Acciones implicadas en la gestión de vulnerabilidades

Acción	Registros	Responsable
Identificación de amenaza.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Administrador de la infraestructura.
Determinar alcance de la vulnerabilidad.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Gerente de Sistemas IT
Mantener continuidad de las operaciones.	Plan de Continuidad de Negocio.	Comité de Riesgos.
Contención de amenaza.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Administrador de infraestructura
Erradicar la amenaza.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Administrador de infraestructura
Recuperación.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Administrador de infraestructura/Comité de Riesgos.
Registro y almacenamiento documental.	Matriz de vulnerabilidades. <b>PECRSI20_F01(2)</b>	Comité de Riesgos


### 6.9 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

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>7 de 8</b>
--	-----------------------	--------------------------

*"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"*



	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Gestión de la vulnerabilidad</b>
	Código:	<b>PECRSI20</b>

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.

#### 6.10 Gestión de actualizaciones y parches.

La identificación de activos informáticos y las actualizaciones del sistema administrativo en Punto de Venta 724 y otros SW utilizados, así como el nivel de parches es una tarea de mejora y robustecimiento a la seguridad y operaciones, por lo tanto es importante disponer de una base que permita realizar los cambios en sistema sin que estos generen un riesgo a futuro.

#### 6.11 Recolección de evidencia y documentación

Para fines de recolección de datos históricos, los hallazgos de las vulnerabilidades identificadas, así como las actividades de remediación deben contar con un repositorio digital y ubicación conocida, el cual pudiera ocuparse como evidencia forense en caso de necesitarse. El responsable de la trazabilidad de los registros será el departamento de Sistemas IT y deben documentar todas las actividades realizadas y las lecciones aprendidas de cada fase definido en el presente procedimiento para la gestión de vulnerabilidades.

### 7. DIAGRAMA DE FLUJO

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

### 8. ANEXOS

TIPO	CODIGO	TITULO
Formato	PECRSI20_F01(2)	Matriz de vulnerabilidades
Ayuda visual	PECRSI20_AV01(2)	Ejemplo Reporte de activos informático724
Políticas	NA	NA
Otros (documento externo)	NA	NA

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>8 de 8</b>
--	-----------------------	--------------------------

*"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"*