	<b>COMERCIALIZADORA RÁPIDO S.A. DE C.V.</b>	
	Tipo de documento:	<b>Procedimiento específico</b>
	Título:	<b>Informática Forense</b>
	Código:	<b>PECRSI22</b>

#### CONTROL DE CAMBIOS

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

### 1. OBJETIVO

Determinar el análisis digital forense considerando las fases de: Identificación, preservación (no modificando la evidencia), obtención, la documentación y el análisis de información

### 2. ALCANCE

A todos los equipos que son parte de Comercializadora Rápido, S. A. de C. V., que están bajo el control del área de sistemas.

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

### 4. DEFINICIONES Y ABREVIATURAS

#### 4.1 Informática forense:

La informática forense proporciona la recopilación, identificación, preservación y análisis de datos de computadoras personales, computadoras portátiles y dispositivos informáticos de almacenamiento.

#### 4.2 Análisis forense de red:

El análisis forense de red tiene como objetivo monitorear, registrar y analizar cualquier actividad de la red.

### 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 Comité de riesgos


Responsables de la gestión del proceso para el seguimiento a la investigación forense y se requiera de pruebas para procesos legales.

#### 5.3 Administrador de la Infraestructura

Es responsable de la identificación y recolección de evidencia suficiente de las TIC's para su análisis forense. Preparar copia de la evidencia digital, examinar la copia obtenida con la finalidad de recuperar la información, analizar la información recuperada y crear un reporte describiendo los datos obtenidos en el procedimiento de análisis.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>1 de 4</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>Informática Forense</b>
	Código:	<b>PECRSI22</b>

#### 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 Prevenir incidentes de seguridad de la información

Establecer acciones para prevenir los incidentes de seguridad de la información, a través de las siguientes actividades:

- Establecer contacto con el equipo de seguridad informática.
- Analizar los comunicados emitidos por los servicios de seguridad de redes.
- Implementar las medidas preventivas necesarias.
- Aplicar **Prevención de Fuga de Datos (DLP) PECRSI17.**

#### 6.2 Identificación

La primera etapa identifica las fuentes o los medios informáticos de trabajo que representen evidencia de gran valor / información relevante (dispositivos), así como los custodios clave y la ubicación de los datos.

Los cuales se encuentran registrados en los procedimientos y protocolos de tecnología de información de Comercializadora Rápido S. A. de C. V. a cargo del área de sistemas

Ver **Matriz de vulnerabilidades PECRSI20\_F01(2)**

#### 6.3 Preservación

El proceso de preservar la información relevante almacenada electrónicamente debe protegerse integralmente de la escena del incidente, capturando imágenes visuales de la escena y documentando toda la información relevante sobre la evidencia y cómo se adquirió.

Lo anterior se lleva a cabo por el responsable designado por el gerente de sistemas, asegurando mantener la integridad de las evidencias, las cuales se resguardan en el servidor del sistema de Comercializadora Rápido S. A. de C. V.

#### 6.4 Recopilación


La recopilación de información digital que puede ser relevante para la investigación. Implica el resguardo del dispositivo electrónico de la escena del crimen o incidente y luego la obtención de imágenes, copias o impresión de su contenido. Y se resguarda en el área de sistemas de Comercializadora Rápido S. A. de C. V., bajo la custodia del gerente de sistemas.

#### 6.5 Análisis

Búsqueda sistemática en profundidad de evidencia relacionada con el incidente que se está investigando. Los resultados del examen son objetos de revisión de datos que se encuentran en la información recopilada; pueden incluir archivos generados por el sistema y el usuario. El análisis tiene como objetivo establecer conclusiones basadas en la evidencia encontrada. El reporte queda bajo resguardo del área de sistemas de

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>2 de 4</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>Informática Forense</b>
	Código:	<b>PECRSI22</b>

Comercializadora Rápido S. A. de C. V. y se comunica al gerente general y en caso de indicarse, al área de recursos humanos para un seguimiento con las partes interesadas o bien para un seguimiento legal.

## 6.6 Informes

Los informes se basan en técnicas y metodologías probadas, por parte de personal de sistemas de Comercializadora Rápido S. A. de C. V., con la verificación de parte del gerente de sistemas, a fin de cumplir criterios de examinación forense, para poder duplicar y reproducir los mismos resultados.

## 6.7 Administración documental

Mantener un sistema automatizado de documentación de expedientes con una cuota de seguridad y control, para salvaguardar los resultados con el debido cuidado y los investigadores deben prepararse para declarar ante Comercializadora Rápido S. A. de C. V. o en caso de ejercerse una situación legal, se hará frente a una entidad de jurídica o legal, municipal, estatal o federal.

El administrador de infraestructura es responsable de la detección de incidentes de seguridad de la información y es el encargado de hacer el registro del incidente en la herramienta de apoyo al sistema **Matriz de vulnerabilidades PECSI20\_F01(2)** para lo cual debe documentar el impacto del incidente, ingresar la información de descripción del incidente e indicar los requisitos de la norma ISO 27001 efectuados a través de:

- Dirigir los campos de registro en la herramienta de apoyo al sistema de gestión.
- Identificar los requisitos de la norma ISO 27001 afectados por el incidente.

### 6.7.1 Verificación de las copias de los medios informáticos

Las copias que fueron efectuadas en los medios previos, deben ser idénticas al original. La verificación debe estar asistida por métodos y procedimientos que establece la completitud de la información traspasada a la copia y es preciso que el software o la aplicación soporte de la operación ya haya sido probado y analizado por el departamento de Sistemas de Comercializadora Rápido S. A. de C. V. para que; sea válido en un procedimiento ante una diligencia legal.

### 6.7.2 Documentación de los procedimientos, herramientas y resultados sobre los medios informáticos analizados

La persona que hace la investigación es del área de sistemas de Comercializadora Rápido S. A. de C. V., o en caso de ser necesario se contara con los servicios de un externo con la competencia requerida y cumpliendo los criterios de confidencialidad establecidos por Comercializadora Rápido S. A. de C. V.


El Gerente De Sistemas, asegura contar con los pasos realizados, herramientas utilizadas, resultados de análisis, y todo claramente documentado para que cualquier persona diferente pueda revisar dichos datos.

### 6.7.3 Mantenimiento de cadena de custodia de las evidencias digitales

Va ligado al punto 6.3, se debe documentar cada uno de los eventos que se hayan realizado con la evidencia en su poder como quién la entregó, cuándo se entregó, entre otras cosas.

Vigente a partir de: <b>30-ABR-2024</b>	Revisión: <b>3</b>	Página: <b>3 de 4</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>Informática Forense</b>
	Código:	<b>PECRSI22</b>

#### 6.7.4 Informe y presentación de los análisis de los medios informáticos

Pueden presentarse falsas expectativas cuando existe una inadecuada presentación de los resultados. Los elementos críticos a la hora de defender un informe de las investigaciones son: la claridad del uso del lenguaje, una buena redacción sin juicios de valor, y una ilustración lógica de los hechos y resultados. Existen dos tipos de informes: técnicos, con los detalles de una inspección realizada; y ejecutivos, para la gerencia y dependencias de Comercializadora Rápido S. A. de C. V.

#### 6.7.5 Solucionar el incidente de seguridad de la información

Definir las acciones para contener el incidente e implementar la solución definitiva, a través de:

- Definir la solución del incidente de seguridad de la información.
- Implementar la solución al incidente de seguridad de la información.
- Notificar la solución del incidente.
- Establecer contacto con las autoridades.
- Identificar las lecciones aprendidas.

Registrar las soluciones a partir del **Matriz de vulnerabilidades PECSI20\_F01(2)** y cumplir con las acciones prevista en tiempo y forma

#### 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)	PECSI17	Prevención de Fuga de Datos (DLP)
	PECSI20_F01(2)	Matriz de vulnerabilidades

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