

	COMERCIALIZADORA RÁPIDO S.A DE C.V		
	Política Respuesta a Incidentes	Código:	PECRSI14_PO01(2)
		Página:	1 de 2

El objetivo de esta política es garantizar la respuesta a incidentes, incluyendo la evaluación del alcance, aplicando procedimientos internos y con terceros, para mitigar el incidente, aplicable a todas las áreas, actividades y procesos de Comercializadora Rápido S.A. de C.V.

1. Responsabilidades y procedimientos.

El Comité de Riesgos debe estar conformado por personal de Comercializadora Rápido S.A. de C.V. con conocimientos técnicos y operativos de las infraestructuras de sucursales 7/24 e instalaciones administrativas de la Organización.

El Comité de Riesgos es responsable de elaborar y dar mantenimiento al procedimiento para la respuesta a incidentes de seguridad, el cual debe ser avalado por Alta Dirección.

El Comité de Riesgos debe conocer los procedimientos **Evaluación de incidentes de seguridad de la información PECSI14**, que considera al menos etapas de:

- Identificación y análisis.
- Estimación del riesgo.
- Valoración del riesgo.
- Control del riesgo.
- Reevaluación.

El Comité de Riesgos debe coordinar las acciones para solucionar los incidentes que afecten los servicios de información, para la operación de Comercializadora Rápido S.A. de C.V., en corresponsabilidad con las áreas afectadas e involucradas en la operación.

Es responsabilidad de todo el personal de Comercializadora Rápido S.A. de C.V. involucrarse y concientizar los procedimientos para la detección y prevención de fraude para evitar la posibilidad de actos malintencionados dentro de la organización.

2. Informar eventos de seguridad de la información.

Los usuarios y colaboradores deben notificar de forma inmediata al Comité de Riesgos y Alta Dirección, de todos los incidentes o amenazas detectados que puedan causar la degradación en los niveles de servicios, en las infraestructuras catalogadas como esenciales de Comercializadora Rápido S.A. de C.V.

Es responsabilidad de todo el personal de Comercializadora Rápido S.A. de C.V. reportar los incidentes de seguridad de la información que tengan una probabilidad de materializar un riesgo.

Algunos ejemplos de incidentes son, sin ser limitativos:

- Accesos físicos no autorizados.
- Accesos lógicos no autorizados.
- Negación o degradación de servicios a sistemas de información.
- Recepción de correo basura.
- Robo de información.
- Incumplimiento a las políticas de seguridad de la información.
- Falla en la identificación o etiquetado de la información (de acuerdo a su clasificación).
- Ataques de virus.
- Incumplimiento con leyes sobre protección de datos personales.

	COMERCIALIZADORA RÁPIDO S.A DE C.V		
	Política Respuesta a Incidentes	Código:	PECRSI14_PO01(2)
		Página:	2 de 2

- Amenazas al personal para entregar información confidencial de clientes internos y externos.
- Fraudes y/o extorsión

3. Informar sobre puntos débiles de seguridad de la información.

El monitoreo de la seguridad debe llevarse a cabo por el área de Sistemas IT.

El Comité de Riesgos puede solicitar la información necesaria, que permita identificar incidentes de seguridad relacionados con el ambiente de red y sistemas, así como, herramientas de monitoreo de seguridad en redes (IPS, firewalls, entre otros.)

El Gerente de Sistemas IT deberá notificar sobre las amenazas detectadas en la Organización.

4. Respuesta a incidentes de seguridad.

Los miembros del Comité de Riesgos deben estar capacitados para el uso de las herramientas adquiridas por Comercializadora Rápido S.A. de C.V. para el análisis y la respuesta a incidentes.

Se deben llevar a cabo sesiones de análisis de los incidentes conforme a la criticidad identificada, para la prevención y su solución.

Los procedimientos de respuesta a incidentes de seguridad se deben ser actualizados periódicamente.

5. Recolección de evidencia

Es responsabilidad del Comité de Riesgos recolectar y documentar la evidencia relativa a los incidentes de seguridad que se identifiquen. Es responsabilidad de la Gerencia de Sistemas de la Información verificar que se encuentre el resguardo de toda documentación y evidencia de los incidentes relativos a la seguridad de la información dentro de un repositorio para su análisis.