	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Evaluación de incidentes de seguridad de la información
	Código:	PECRS114

CONTROL DE CAMBIOS

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

1. OBJETIVO

Determinar los criterios de evaluación de la seguridad de la información de los Sistemas Tecnológicos de la Información de Comercializadora rápido S.A. de C.V. para su adecuada gestión de Riesgos, disponer de lineamientos de seguridad ante situaciones de emergencia, que nos apoyen a mitigar el impacto generado por la interrupción de los servicios críticos que afecten las operaciones normales de COMERCIALIZADORA RÁPIDO S.A. DE C.V.

2. ALCANCE

Se aplica para Sistemas IT de Comercializadora rápido S.A. de C.V.

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 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 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.

4.4 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.)

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 1 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRS114

4.5 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.

4.6 Evaluación de riesgos.

Actividad fundamental que la Ley establece que debe llevarse a cabo inicialmente y cuando se efectúen determinados cambios, para poder detectar los riesgos que pueden existir en todos y cada uno de los puestos de trabajo de la empresa y que puedan afectar a la seguridad de las operaciones y de los trabajadores.

4.7 Fraude

Uso de acciones ilegales, caracterizadas por el engaño, ocultamiento o la violación de la confianza.

4.8 Identificación de riesgos.

Proceso para encontrar, reconocer y describir los riesgos.

4.9 PC:

Puntos Críticos.

4.10 BIA

Análisis de Impacto del Negocio

4.11 DRP

Plan de recuperación de Desastres

5. RESPONSABILIDADES

5.1 Gerente de Sistemas IT

Responsable de verificar en la aplicación de este procedimiento.

5.2 Usuarios

Identificar y dar aviso al comité de riesgos de las posibles vulnerabilidades que se pudiesen llegar a presentar para ser evaluadas y controladas de forma y tiempos oportunos.

5.3 Comité de riesgos

Responsable de coordinar la ejecución de las actividades antes, durante y después de una incidencia, como también, velar por el cumplimiento de las disposiciones del Plan de continuidad.


6. DESARROLLO

6.1 Generalidades

Al evaluar la posible vulnerabilidad a la Seguridad de la información de Comercializadora Rápido S.A. de C.V, se deberá considerar una variedad de posibles autores que podrían llevar a cabo un ataque tanto dentro como fuera de las instalaciones. Estos incluirían tanto ataques oportunistas efectuados por un solo individuo como ataques premeditados llevados a cabo por un solo agresor o agresores organizados que serían amenazas provocadas por el Hombre, amenazas técnicas y amenazas ambientales.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 2 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14


En la siguiente imagen se presentan algunas de las amenazas:

Ejemplo: Ejemplos de amenazas

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PUNTUACIÓN RIESGO				
AMENAZAS PROVOCADAS POR EL HOMBRE	CRIMEN INFORMÁTICO	Lineas de comunicación no protegidas	1	2	3	4	5
		Arquitectura de Red insegura					
		Transferencia de contraseñas en operadores.					
		Falta de controles de autenticación					
		falta de Políticas de seguridad					
		Falta de monitoreo y registro de usuarios privilegiados					
		Falta de almacenamiento de red de trafico para investigaciones posteriores.					
	TERRORISMO-VANDALISMO	Ausencia de cámaras en todos las áreas administrativas	1	2	3	4	5
		Falta de vigilancia CCTV.					
	PERSONAL Y USUARIOS	Falta de procedimientos de contratación.	1	2	3	4	5
		Falta de capacitación respecto a la seguridad informatica					
		Falta de concientizacion respecto a la seguridad informática					
		Faltan clausulas de impacto legal y penalización en caso de uso indebido de la información					
	ALTA ROTACIÓN DE PERSONAL	No xisten controles en la seguridad de la confidencialidad y integridad de la información	1	2	3	4	5
	INCORRECTA ADMINISTRACIÓN DEL SISTEMA INFORMÁTICO	Mejoramiento de las políticas que regulen el uso de los Sistemas de Información de acuerdo al perfil de usuario.	1	2	3	4	5
		No existe documentación de políticas y procedimientos de la gestion de los servicios de Red					
ROBO	Falta de controles de acceso al centro de datos.	1	2	3	4	5	
	Falta de procedimiento para solicitud y acceso a las bitácoras						
TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PUNTUACIÓN RIESGO				
AMENAZAS ORGANIZACIONALES	INEXISTENCIA DE PLANES, POLÍTICAS Y PROCEDIMIENTOS ORGANIZACIONALES Y DE ADMINISTRACIÓN DE USUARIOS.	No se ha elaborado Plan de contingencias	1	2	3	4	5
		Falta de procedimiento formal para el registro y bloqueo de la eliminación de usuarios					
		Inexistencia de procedimientos de monitoreo de los recursos de procesamiento y almacenamiento de la informacion					
		Inexistencia de políticas que exijan la documentación de cambios en la configuración de los sistemas y recursos existentes.					
		No existe estandarización de los documentos.					
	FALTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	Incumplimiento de las políticas de seguridad informática.	1	2	3	4	5
		Falta de asignación adecuada de responsabilidades en la seguridad de la información					
		Falta de mecanismos de monitoreo					
		Falta de responsabilidades en la seguridad de la información.					

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 3 de 14
--	-----------------------	---------------------------

"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"

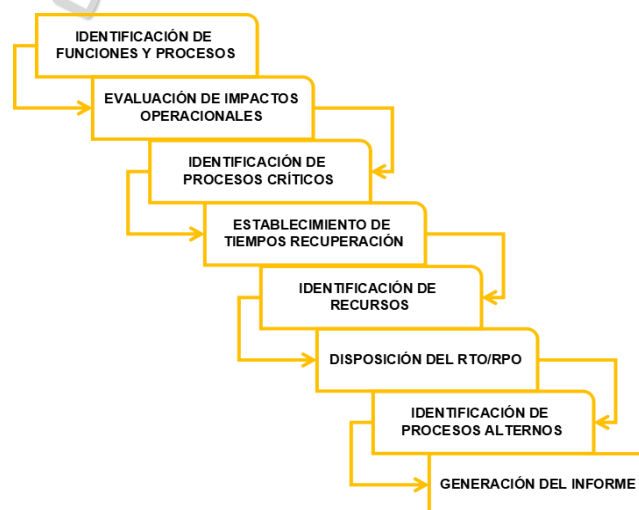
	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Procedimiento específico
	Título:	Evaluación de incidentes de seguridad de la información
	Código:	PECRS114

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PUNTUACIÓN RIESGO				
AMENAZAS TÉCNICAS	FALLA DE COMPONENTES ELECTRÓNICOS	Falta de capacitación del uso de los equipos de los usuarios	1	2	3	4	5
		No haber establecido políticas de reemplazo de piezas sensibles en el funcionamiento de los dispositivos electrónicos.					
		No se ejecutan pruebas periódicas de Hardware y Software.					
	FALLA DE SERVICIOS EN LOS PROVEEDORES	No se cuenta con un procedimiento en el que se indique la forma de operar en caso de la falta de internet.	1	2	3	4	5
	MALA IMPLEMENTACIÓN DE CONTROLES O INCUMPLIMIENTO DE LOS MISMOS.	Implementación de controles que no se encuentran acordes a la realidad del negocio.	1	2	3	4	5
		No se han monitoreado y /op evaluado el cumplimiento de los controles de seguridad.					
	FALLA/MAL FUNCIONAMIENTO DE LOS EQUIPOS.	Configuración incorrecta de parámetros.	1	2	3	4	5
		Cambios de configuración no documentados.					
		Falta de auditoría de la fallas de software (servidores, equipos, etc.)					
		Deficiencia en los procedimientos de respaldo periódicamente de la información.					
	SATURACIÓN DE LA RED.	Gestión inadecuada de la red (capacidad de recuperación de enrutamiento.	1	2	3	4	5
		Falta de políticas de uso de recursos de red como el buen uso de internet.					
		Deficiencia en los procedimientos de respaldo periódicamente de la información.					
		Falta de monitorización del tráfico de red.					

6.2 Metodología Del BIA


Define una serie de pasos interactivos con el objeto de identificar claramente los impactos de las interrupciones y tomar decisiones respecto a aquellos procesos que se consideran críticos para Comercializadora Rápido S.A. De C.V. y que afectan directamente el negocio ante la ocurrencia de un desastre, estos pasos son:

Ejemplo: Metodología BIA



Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 4 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRS114

6.2.1 Identificación de funciones y procesos

Las funciones de Comercializadora Rápido S.A. De C.V. que nos apoyan en los objetivos del Sistema de Gestión de Seguridad de Información, se describen en el siguiente listado:

ROL	PROCESOS	FUNCIONES
Gerente general	1. Revisión de los estados financieros 2. Coordinación de gerentes advos 3. Liderazgo frente al Comité de riesgos 4. Define dirección de la empresa.	Responsables de dirigir las acciones requeridas durante la contingencia.
Gerente de Sistemas IT	1. Respaldo de Información 2. Cifrado de datos 3. Protección antivirus 4. Recuperación de información del cliente 5. Recuperación de los servidores 6. Coordina y dirige los proyectos en desarrollo	Responsables de reunir los medios necesarios para llevar a cabo la activación del plan de continuidad (lugar alternativo de reunión, materiales necesarios, herramientas, etc)
Gerente de RH	1. Gestión de la seguridad de las instalaciones 2. Capacitación de nuevos usuarios e integrantes de la organización. 3. Filtra al personal de nuevo ingreso	Responsables de reunir los medios necesarios para llevar a cabo la activación del plan de continuidad (lugar alternativo de reunión, materiales necesarios, herramientas, etc)

6.2.2 Evaluación de impactos operacionales

Una vez identificados los elementos operacionales de Comercializadora Rápido S.A. De C.V., se requiere evaluar el nivel de impacto de interrupción dentro del negocio.

El impacto operacional permite evaluar el nivel negativo de una interrupción en varios aspectos de las operaciones en Comercializadora Rápido S.A. De C.V.; el impacto se puede medir utilizando un esquema de valoración, con los siguientes niveles: A, B o C.

Nivel A: Operación crítica para el negocio, indispensable esta operación.

Nivel B: Operación es una parte íntegra del negocio, es decir que se puede operar normalmente.


Nivel C: Operación no es una parte íntegra del negocio.

A continuación, se presente la información referida al nivel de criticidad actual en Comercializadora Rápido S.A. De C.V.:

Datos y tiempos estimados, se verifican los tiempos de respuesta en los simulacros que se realicen de forma programada por el líder del proyecto.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 5 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRS114

CATEGORÍA	PROCESO	NIVEL	TOLERANCIA A FALLAS	DESCRIPCIÓN
Proveedores de comunicaciones	Descarga eléctrica derivada de rayos eléctricos	B	2 horas	Mantenimiento de sistemas de suministro de energía
Seguridad de la información	Restablecimiento/configuración de fábrica	B	40 minutos	Respaldo o resguardo de datos
Seguridad de la información	Apagado intencional o accidental del equipo DVR	B	30 minutos	Respaldo o resguardo de datos
Seguridad de la información	Reseteo de Modem para configuración de fabrica	A	10 minutos	Respaldo o resguardo de datos
Seguridad de la información	Recargas fantasmas	C	1 hora	Mantenimiento de servicios internos
Infraestructura	Escurrimiento de agua por deshielo de los climas	C	3 horas	Mantenimiento de infraestructura
Seguridad de la información	Infección del servidor	A	10 minutos	Servicio de Firewall/Antivirus
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	A	30 minutos	Servicio de centro de datos

6.2.3 Identificación De Procesos Críticos

La identificación de los procesos críticos de Comercializadora Rápido S.A. De C.V., se da con base en la clasificación de los impactos operacionales, por lo que tenemos lo siguiente:

CATEGORÍA	PROCESO	NIVEL
Seguridad de la información	Reseteo de Modem para configuración de fabrica	A
Seguridad de la información	Infección del servidor	A
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	A

6.2.4 Establecimiento De Tiempos De Recuperación


Una vez identificados los procesos críticos de Comercializadora Rápido S.A. De C.V., se deben establecer los tiempos de recuperación que son una serie de componentes correspondientes al tiempo disponible para recuperarse de una alteración o falla de los servicios; el entendimiento de estos componentes es fundamental para comprender el BIA. Los tiempos de recuperación de describen a continuación:

TIEMPO DE RECUPERACIÓN	DESCRIPCIÓN
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Una vez identificados los procesos críticos de Comercializadora Rápido S.A. De C.V., función que hace parte del análisis de los impactos operacionales, se procede a identificar el MTD, que corresponde al tiempo

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 6 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

máximo de inactividad que puede tolerar la organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio).

CATEGORÍA	PROCESO	MTD	PRIORIDAD DE RECUPERACIÓN
Seguridad de la información	Reseteo de Modem para configuración de fabrica	30 min	BAJA
Seguridad de la información	Infección del servidor	10 min	ALTA
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	30 min	ALTA

6.2.5 Identificación de recursos

Las diferentes actividades contempladas en la función crítica de Comercializadora Rápido S.A. De C.V. deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto al negocio.

CATEGORÍA	PROCESO	RECURSOS CRÍTICOS
Seguridad de la información	Reseteo de Modem para configuración de fabrica	Contar con los enlaces de comunicación con proveedor.
Seguridad de la información	Infección del servidor	Actualización constante del software de protección contra virus
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	Monitoreo de la temperatura del sitio en frio.

6.2.6 Disposición de los RTO/RPO

La siguiente tabla muestra un ejemplo de valores RTO/WRT para los procesos críticos en Comercializadora Rápido S.A. De C.V.


CATEGORÍA	PROCESO	RECURSOS CRÍTICOS	RTO	WRT	RPO
Seguridad de la información	Reseteo de Modem para configuración de fabrica	Contar con los enlaces de comunicación con proveedor.	40 minutos	40 minutos	60 minutos
Seguridad de la información	Infección del servidor	Actualización constante del software de protección contra virus	10 minutos	10 minutos	60 minutos
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	Monitoreo de la temperatura del sitio en frio.	30 minutos	30 minutos	60 minutos

6.2.7 Identificación de procesos alternos

La identificación de procesos alternos hace posible que los procesos en Comercializadora Rápido S.A. De C.V. puedan continuar operando en caso de presentarse una interrupción; para ello es oportuno aplicar los métodos alternativos (descritos en procedimientos) de manera temporal que ayuden a superar la crisis que ha generado una interrupción; por lo tanto, para cada proceso crítico se establece:

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 7 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

CATEGORÍA	PROCESO	RECURSOS CRÍTICOS	RTO	WRT	RPO	PROCESO ALTERNO
Seguridad de la información	Reseteo de Modem para configuración de fabrica	Contar con los enlaces de comunicación con proveedor	40 minutos	40 minutos	60 minutos	Ingresar a servidor de sucursal, abrir page internet e ingresar a IP del MODEM; ingresar usuario y contraseña, generar cambio de contraseña WIFI, deshabilitar WIFI, y habilitar función DMZ.
Seguridad de la información	Infección del servidor	Actualización constante del software de protección contra virus	10 minutos	10 minutos	60 minutos	Restringir el acceso a páginas de internet, cambio de los privilegios a: solo lectura/ CAMBIO de antivirus contratación anual, desconexión de la computadora a red y formateo del equipo.
Base de datos	Sobrecalentamiento de servidores por falla de clima en SITE	Monitoreo de la temperatura del sitio en frio	30 minutos	30 minutos	60 minutos	Se apagan servidores y se activan los climas de respaldo mientras se restablece temperatura los servidores

6.2.8 Generación de informe de impacto del negocio

Se presentar un informe de impacto a Comercializadora Rápido S.A. De C.V. que corresponde a la guía para el BIA con los siguientes resúmenes:

- Listado de procesos críticos
- Listado de prioridades de sistemas y aplicaciones
- Listado de tiempos MTD, RTO y RPO
- Listado de procedimientos alternos.

6.3 Plan de recuperación de Desastres (DRP)

Este enfoque organizado para tratar (responder a) los incidentes de ciberseguridad y la recuperación de Desastres (DRP) debe ejecutarse de manera que se mitiguen los daños, se reduzca el tiempo de recuperación y se minimicen los costos. El conjunto de instrucciones que Comercializadora Rápido S.A. De C.V. utiliza para guiar a su equipo de respuesta a incidentes cuando se produce un evento de seguridad (es decir, una violación de la seguridad) es el Plan de Respuesta a Incidentes.


El plan de Recuperación documentado ayuda a responder rápidamente agilizando las decisiones, revisando los procesos y definiendo el uso apropiado de las tecnologías disponibles.

Para desarrollar el RI, se consideraron 6 etapas de respuesta a incidentes que se deben planear:

- **Preparación:** preparar al personal de seguridad para manejar posibles incidentes. Esto incluye entrenamiento, equipamiento y práctica.
- **Identificación:** detectar y decidir si un incidente cumple las condiciones para ser considerado un incidente de seguridad por la organización, y su gravedad.
- **Contención:** contención del incidente mediante el aislamiento de sistemas comprometidos para evitar daños futuros.
- **Mitigación:** detectar la causa del incidente y eliminar las amenazas de los sistemas afectados.
- **Recuperar:** restaurar los sistemas afectados y asegurarse de que no quede ninguna amenaza.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 8 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

- **Aprender:** analizar los registros de incidentes, actualizar el plan de respuesta y completar la documentación del incidente.

6.3.1 Preparación

Es necesario estar preparado para cualquier suceso o actividad que pueda ocurrir, una buena anticipación y entrenamiento previo nos puede dar la gran diferencia entre una respuesta de un incidente o desastre absoluto, en donde debemos tener en cuenta 3 aspectos fundamentales: Recurso humano, Recurso Documental y Tecnologías.

Para el caso del Recurso humano, debemos tener claro el contexto del alcance con el cual contamos, es decir, que personal tanto interno como externo tenemos, sus capacidades para reaccionar ante algún incidente y en su caso, tener a la mano un número de contacto en caso de requerir su apoyo y asistencia.

Una mejor gestión es tener un listado actualizado de contactos internos y externos que nos puedan auxiliar durante situaciones fuera de alcance o de apoyo, este apoyo se puede solicitar a partir de **SICA PECSI30** y en la **Matriz de Escalamiento PECSI30_AV01(3)**.

En el caso de los procedimientos, se cuenta con listado de documentos para atender cualquier incidente, esto va desde procedimientos, anexos, formatos u otro tipo de medio donde se puede determinar el qué hacer y cómo hacerlo.

TIPO	CÓDIGO	NOMBRE
POLITICA	PECRSI14_PO01(3)	Política Respuesta a Incidentes
PROCEDIMIENTO	PECRSI01	Respaldo de la información
MANUAL	MNCRSI02	Plan de continuidad del negocio
ANEXOS	PECRSI20_F01(2)	Matriz de vulnerabilidades

Y, por último, las Tecnologías con las que se cuentan, al igual que el Recurso Humano, se describe si es interno o externo y su capacidad ante cualquier incidente.

TIPO	NOMBRE	CAPACIDAD
Interno	Soporte Técnico 7/24	Atención y servicio ante alguna falla tecnológica
Interno	Mantenimiento De Instalaciones	Reparación y mantenimiento de los recursos de infraestructura.
Externo	SOS. S.A. De C.V.	Abastecimiento de los recursos tecnológicos.
Externo	TELMEX S.A. De C.V.	Abastecimiento de los servicios de telecomunicaciones


6.3.2 Identificación

En esta etapa definimos nuestra capacidad y estado actual de operación y los sucesos que son parte de operación diaria, para identificar aquellos casos que no entren dentro de lo "normal" y que requieran un análisis más a detalle.

Dentro de lo general, podemos definir algunos aspectos habituales que requieren especial atención en Comercializadora Rápido S.A. De C.V., los cuales son:

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 9 de 14
--	-----------------------	---------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

- Correo electrónico
- Vulnerabilidades conocidas (contenidos, componentes, módulos, dispositivos, aplicaciones web y software)
- Dispositivos de almacenamiento externo
- Uso de activos

Las fuentes de información que apoyan y ayudan a identificar el origen de un posible incidente de ciberseguridad y el alcance del mismo, se describen a continuación:


NIVEL	ORIGEN
Red	Registros de conexiones realizadas a través de sistemas proxy.
Red	Registros de conexiones autorizadas por los firewall.
Red	Registros de intentos de conexión bloqueados por el firewall.
Red	Trazas de red que muestren conexiones a destinos, puertos o a través de protocolos no esperados, así como picos de tráfico anómalos o en horarios no habituales.
Red	Sistemas de correlación de eventos de seguridad (SIEM)
Red	Sistemas en red de detección/prevención de intrusos (NIDS/NIPS).
Red	Sistemas en red de prevención de fugas de información (NDLP).
Equipo	Registros de sistemas locales de detección/prevención de intrusos (HIDS/HIPS).
Equipo	Cuentas de usuario inusuales en el sistema, especialmente aquellas con privilegios administrativo.
Equipo	Ficheros ocultos o con tamaños, nombres o ubicaciones sospechosas, pudiendo indicar los mismos algún tipo de fuga de información o almacenamiento por parte de algún malware.
Equipo	Entradas sospechosas en el registro, principalmente en el caso de infecciones por malware en sistemas Windows, donde ésta es una de las técnicas habituales utilizadas por el malware para asegurar la persistencia en el sistema comprometido.
Equipo	Registros de auditoría y accesos no autorizados.
Equipo	Sistemas locales de prevención de fugas de información (DLP).
Equipo	Una carga excesiva de disco o memoria puede estar producida por un incidente de seguridad como malware, denegaciones de servicio o intrusiones.
Equipo	En el caso de equipos de usuario o terminales móviles, pueden indicar algún tipo de infección en el sistema, entre otros: comportamiento anómalo de alguna aplicación, ventanas emergentes del navegador, conexiones muy lentas, reinicios o aplicaciones que se cierran sin motivo.
Equipo	Tareas programadas o actividad sospechosa en los registros de auditoría y logs que indique un funcionamiento anormal del sistema o intentos de intrusión en algún servicio, por ejemplo, mediante fuerza bruta.
Equipo	Registros de consolas antivirus o de alguna herramienta habitualmente instalada en el sistema para la identificación de rootkits, de control de integridad de ficheros, firma de los binarios, etc
Equipo	Anomalías o condiciones reportadas por otros usuarios.
Aplicación	Registros de auditoría y accesos no autorizados.
Aplicación	Registros o logs de aplicaciones que puedan recoger información de interés, como fechas, transacciones o actividad de los usuarios.

6.3.3 Contención

Si un atacante ha logrado comprometer un dispositivo, se debe evitar que pueda comprometer un segundo; si ha logrado extraer un documento del servidor de archivos, la labor del equipo de respuesta, en este

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 10 de 14
--	-----------------------	----------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

momento, es evitar que salga más información al exterior. La formación y experiencia del personal implicado en la gestión de incidentes será un factor determinante durante esta etapa.

Cuando ocurre un ciberincidente, esta suele ser la fase en la que se toman las decisiones de forma más rápida ya que el tiempo es un factor determinante y la reputación o la continuidad del negocio están en riesgo y hay que recordar que las decisiones precipitadas son buenas, aunque no siempre son acertadas.

Algunas de las acciones que Comercializadora Rápido S.A. De C.V. toma en primer lugar consisten en:

- Desconectar el equipo o segmento de red del resto de redes de la organización. Esto puede hacerse, si se trata de un equipo aislado, desconectando el cable de red o tirando el enlace inalámbrico si la conexión se realiza a través de Wi-Fi.
- En caso de tratarse de algún equipo que desempeña una función crítica para el negocio, es posible proceder a la colocación de un firewall intermedio entre el segmento afectado y el resto de la red que permita filtrar el tráfico y permitir únicamente aquello que sea estrictamente necesario para la prestación del servicio.
- Reubicación del recurso comprometido en una VLAN aislada.
- Considerar la aplicación de técnicas de DNS sinkholing para controlar tráfico malicioso.
- Si se conocen los detalles técnicos del tipo de ciberincidente se pueden aplicar medidas de contención más ajustadas a cada situación (bloqueo de determinados correos electrónicos, aplicación de reglas en los cortafuegos, bloqueo de acceso a unidades compartidas, etc.).
- Contactar con terceras entidades que pueden ofrecer ayuda en la contención. Los proveedores de servicio de Internet pueden aplicar filtros o activar medidas de protección.


Una vez que se han tomado las medidas iniciales para contener el problema, cuidando de no destruir información valiosa, es momento de comenzar con los procedimientos de toma y preservación de evidencias. Este paso resulta importante, tanto por sí finalmente es necesario judicializar el incidente, como para poder analizar correctamente el origen y determinar el impacto real del problema.

NOMBRE DE EVIDENCIA	DESCRIPCIÓN
Falla eléctrica.	Mantener un procedimiento de contingencia en casos de que la energía eléctrica presente un fallo y se detengan las operaciones de correspondencias y/o venta con tarjeta de crédito o débito.
Respaldo de la información.	Ejecutar el procedimiento de respaldo de información de las correspondencias con la finalidad de tener los procesos de correspondencias y ventas en resguardo y disponibilidad en caso de que se requiera.
Detección y prevención de fraudes.	Fortalecer las normativas internas para reducir el riesgo de que ocurra un fraude y si llegara a ocurrir, poder detectarlo oportunamente.

En este caso, existen dos situaciones: datos volátiles almacenados y datos no volátiles; para el primer caso debemos hacer la adquisición de memoria volátil se pueden utilizar herramientas forenses (tanto hardware como software), procurando en todo momento no alterar el sistema ni los datos del mismo ya que podrían

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 11 de 14
--	-----------------------	----------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

modificarse o perderse evidencias importantes. Ahora para el caso contrario, se deben realizar copias exactas (bit a bit) de los datos originales. Esto se puede realizar a través de diferentes utilidades o herramientas, o mediante dispositivos físicos conocidos comúnmente con el nombre de clonadoras.

A partir de este momento se pueden comenzar las acciones de análisis de los datos copiados para tratar de obtener la máxima información sobre lo ocurrido y continuar con la fase de mitigación del incidente.

Medidas a considerar por Comercializadora Rápido S.A. De C.V.:

- Eliminar procesos sospechosos.
- Eliminar cuentas de usuario que se hayan creado por parte de los posibles atacantes.
- Aplicar reglas de filtrado y medidas adicionales de seguridad en los sistemas de protección perimetrales.

6.3.4 Mitigación

La medida de mitigación más adecuada suele empezar por realizar un borrado seguro de los medios de almacenamiento comprometidos y una reinstalación del sistema, pero desgraciadamente no siempre posible; en algunos casos porque no existe una copia de seguridad reciente de la información (si existe) y en otros casos porque volver a poner un sistema en producción sin conocer las causas del ciberincidente puede acarrear un nuevo e idéntico problema.

Las medidas de mitigación dependerán del tipo de ciberincidente, así, en casos de denegaciones de servicio distribuidas (DDoS) puede ser necesario solicitar asistencia de entidades externas, como proveedores de servicios de mitigación de este tipo de ataques o que puedan apoyar en el análisis y definición de la estrategia de mitigación.

MEDIDA DE MITIGACIÓN	TIPO DE INCIDENTE	DESCRIPCIÓN
Uso de firewalls	Protección de Software mal intencionado	La aplicación de firewalls provee seguridad virtual en los equipos, condiciona los accesos a sitios de internet.
Seguridad de ingreso a SITE	Sabotaje/vandalismo/Robos	El SITE que alberga los racks, servidores y equipos de comunicaciones se encuentran cerrados y el ingreso es exclusivo de personal de Sistemas IT.
Antivirus	Virus	El antivirus se encuentra alojado en el server que provee seguridad a toda la red contra amenazas internas o externas.


Cuando no existan copias de seguridad disponibles y se haya realizado una reinstalación completa del sistema, la información debe ser extraída manualmente del equipo previamente comprometido y transferida al nuevo sistema, con la correspondiente cautela de no transmitir junto con ella la infección.

6.3.5 Recuperación

Consiste en devolver el nivel de operación a su estado normal y que las áreas de Comercializadora Rápido S.A. De C.V. afectadas puedan retomar su actividad. Es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en algún incidente.

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 12 de 14
--	-----------------------	----------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

En los casos de sistemas críticos, conviene prestar especial atención a las instrucciones del fabricante del producto para su restauración o reinstalación, programando mantenimientos correctivos y paradas de sistemas necesarias para llevar a cabo la recuperación del incidente.

A continuación, se enlistan los pasos a realizar cuando se pone a operación nuevamente un servicio o sistema (puede apoyarse de formatos o procedimientos de trabajo ya establecidos en el sistema).

- Instalación de software
- Ejecución de pruebas
- Preparar los dispositivos de las copias de seguridad
- Hardening
- Reglas Firewall
- Asignación de usuario
- Antivirus
- Restauración/recuperación de la información
- Respaldo de la información corresponsales

6.3.6 Aprender

Una vez que el incidente está controlado y la actividad ha vuelto a la normalidad, es momento de llevar a cabo un proceso al que NO SE DEBE RESTAR la importancia que merece: las lecciones aprendidas.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir. Esto ayudará también a evaluar los procedimientos de actuación, la cadena de mando, las políticas de seguridad y entrenará a los implicados para futuras situaciones de crisis. La importancia de crear comunicación a las partes interesadas deberá ser en cada incidente ocurrido.

6.4 Mejora Continua

Una vez realizado el seguimiento, evaluación, análisis y monitoreo de los indicadores de Seguridad de la información, es necesario, continuar con la Mejora.

La aplicación de esta fase, le permite a Comercializadora Rápido S.A. De C.V, a partir de los resultados de la Fase de Gestión, corregir de ser necesario, los errores cometidos, así como mejorar las acciones llevadas a cabo en las fases anteriores, llevando a cabo el plan de mejoramiento continuo de seguridad y privacidad de la información.


Para la definición el plan de mejora continua, se debe tener en cuenta:

6.4.1 No conformidades y acciones correctivas

- En caso de presentarse no conformidades en las auditorías realizadas, se deberá llevar a cabo las acciones necesarias para controlarlas y corregirlas (Ver formato para acción correctiva).
- Evaluar y revisar la raíz de la no conformidad con el fin de eliminar las causas de la misma y evitar que vuelva a presentar (Ver formato para acción correctiva).

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 13 de 14
--	-----------------------	----------------------------

"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:	Evaluación de incidentes de seguridad de la información
	Código:	PECRSI14

- Comparar las no conformidades presentadas con las acciones correctivas tomadas; esto, con el fin de asegurar que no se vuelvan a presentar y evaluar
- la efectividad de las acciones correctivas aplicadas.
- Implementar las acciones que sean necesarias
- Evaluar la efectividad de las acciones correctivas tomadas.
- Realizar los cambios en el sistema que sean necesarios.

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	PECRSI14_PO01(3)	Política Respuesta a Incidentes
	PECRSI20_F01(2)	Matriz de vulnerabilidades
Otros (documento externo)	PECRSI01	Respaldo de la información
	MNCRSI02	Plan de continuidad del negocio

Vigente a partir de: 29-ABR-2024	Revisión: 3	Página: 14 de 14
--	-----------------------	----------------------------

"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"