	COMERCIALIZADORA RÁPIDO S.A. DE C.V.	
	Tipo de documento:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSIO2

CONTROL DE CAMBIOS

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

1. INTRODUCCIÓN

Comercializadora Rápido S.A. de C.V. tiene como prioridad: mantener y resguardar la seguridad de sus clientes internos y externos, así como la de sus activos de la información, por ello contempla y sabe de las necesidades de continuar con sus actividades aun presentándose una amenaza que desestabilicen las acciones de respuesta ante situaciones desafortunadas, “7/24” trabaja internamente bajo un esquema de mejora continua en todos sus procesos y eso ha permitido que desarrolle métodos preventivos.

Actualmente el incremento de las amenazas externas e internas ha llevado a considerar la verdadera importancia de implementar planes, procedimientos, estructuras y todo tipo de método que garanticen la continuidad del servicio del negocio ante cualquier tipo de eventualidad, sin importar su categoría y su nivel de impacto. Estos factores, han llevado a que en la actualidad la presencia de estos planes sea un factor común a lo largo de la cadena de suministro de los productos y servicios que ofrece.

Históricamente las amenazas han estado asociadas principalmente a contingencias de carácter natural y tecnológico, las amenazas cada vez se tornan en diferentes escenarios como es el terrorismo, la política, la globalización y las ciber-amenazas, lo cual buscan la necesidad de incorporar nuevas estrategias para garantizar la continuidad de las operaciones ante cualquier evento relacionado con el tipo de riesgos al que se está expuesto.

El Plan de Continuidad de Negocios es una solución para proteger a Comercializadora Rápido S.A. de C.V. durante posibles amenazas.

2. OBJETIVO


Establecer políticas que permitan la protección y seguridad de los activos de la empresa, y la de los recursos humanos; antes, durante y después de un evento que se suscite y atente contra las actividades normales de Comercializadora Rápido S.A. de C.V.

2.1 Objetivos específicos del Equipo del PCN

- Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio.
- Identificar actividades y plataformas consideradas críticas para la operación del negocio.
- Identificar personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- Identificar los riesgos presentes para la continuidad (Evaluación de Riesgos).
- Establecer los elementos esenciales requeridos en el plan de recuperación.
- Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 1 de 11
--	-----------------------	---------------------------

“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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

- Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

3. ALCANCE

Involucra al área de Sistemas IT, iniciando con la detección del evento, el proceso de continuidad del producto/servicio, y finaliza con la estrategia de recuperación (en caso de necesitarse).

Elaboró:	Vo. Bo.	Revisó:	Aprobó:
<u>Gutiérrez Zéspedes Héctor Hugo</u> Jefe 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

4. REFERENCIAS

ISO/IEC 27000:2018 Descripción general y vocabulario

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

ISO/IEC 27005:2022 Seguridad de la información, ciberseguridad y protección de la privacidad: orientación sobre la gestión de riesgos de seguridad de la información

5. DEFINICIONES Y ABREVIATURAS

4.1 Amenaza

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

4.2 Ataque

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

4.3 Control

medida que está modificando el riesgo.

Nota 1 a la entrada: Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo.

Nota 2 a la entrada: Es posible que los controles no siempre ejerzan el efecto modificador previsto o supuesto.

4.4 Eficacia

Grado en que se realizan las actividades planificadas y se logran los resultados planificados.

4.5 Evento

Ocurrencia o cambio de un conjunto particular de circunstancias

Nota 1 a la entrada: Un evento puede ser una o más ocurrencias y puede tener varias causas.

Nota 2 a la entrada: Un evento puede consistir en que algo no suceda.


Nota 3 a la entrada: En ocasiones, un evento puede denominarse “incidente” o “accidente”.

4.6 Seguridad de información

Preservación de la confidencialidad, integridad y disponibilidad de la información.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 2 de 11
--	-----------------------	---------------------------

“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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

4.7 Continuidad de la seguridad de la información

Procesos y procedimientos para garantizar operaciones continuas de seguridad de la información.

4.8 Sistema de información

Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

4.9 IT:

Tecnología de la información.

4.10 PCN:

Plan de Continuidad de Negocio.

4.11 Tiempo de Recuperación Objetivo RTO:

Período de tiempo dentro del cual los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte deben recuperarse después de que se haya producido una interrupción.

4.12 Objetivo del Punto de Recuperación (RPO):

Momento en el que se deben recuperar los datos después de que se haya producido una interrupción

4.13 IRBC:

Disponibilidad de las tecnologías de información y comunicaciones para la Continuidad del Negocio.

4.14 MCBO:

Objetivo Mínimo de Continuidad del Negocio.

4.15 TIC:

Tecnologías de información y comunicación.

4.16 Riesgo

Efecto de la incertidumbre sobre los objetivos

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, positiva o negativa.

Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y pueden aplicarse en diferentes niveles.

Nota 3 a la entrada: La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, comprensión o conocimiento de, un evento, su consecuencia, o probabilidad.


Nota 4 a la entrada: El riesgo generalmente se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y su probabilidad.

Nota 5 a la entrada: En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como efecto de la incertidumbre sobre los objetivos de seguridad de la información.

Nota 6 a la entrada: Los riesgos de seguridad de la información generalmente están asociados con un efecto negativo de la incertidumbre sobre los objetivos de seguridad de la información.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 3 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

Nota 7 a la entrada: Los riesgos de seguridad de la información pueden estar asociados con la posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización.

6. RESPONSABILIDADES

6.1 Liderazgo y equipo del PCN

El Plan de Contingencia del Negocio busca asegurar su cumplimiento a través de un Equipo de trabajo capaz y adecuado, el cual estará conformado de la siguiente forma:

- Líder del Equipo: -Gerente General
- Participantes: -Gerente de Sistemas IT
-Gerente de Recursos Humanos

7. DESARROLLO

7.1 Preparación de las TICs para la continuidad del negocio

El Plan de Continuidad del Negocio para la Seguridad y Privacidad de la Información, contempla su implementación en 4 etapas, para que se pueda gestionar la seguridad y privacidad de la información, con el fin de fortalecer la protección de los datos y dar cumplimiento a lo establecido en las Auditorías de cliente y Auditorías internas.

Este Plan aplica a todos los procesos, de manera que conserven las expectativas de las partes interesadas, tanto internas como externas. Los recursos para la gestión del Plan están definidos por los resultados de las actividades de cada etapa, establecidos en el marco de seguridad y privacidad de la información.


7.2 Descripción de la preparación de las TICs para el Plan de Continuidad del Negocio basados en la seguridad y privacidad de la información

A continuación, se define el funcionamiento del Plan de Continuidad del Negocio y su funcionamiento dentro de los requisitos para la seguridad y privacidad de la información, además de la descripción de cada una de sus etapas.

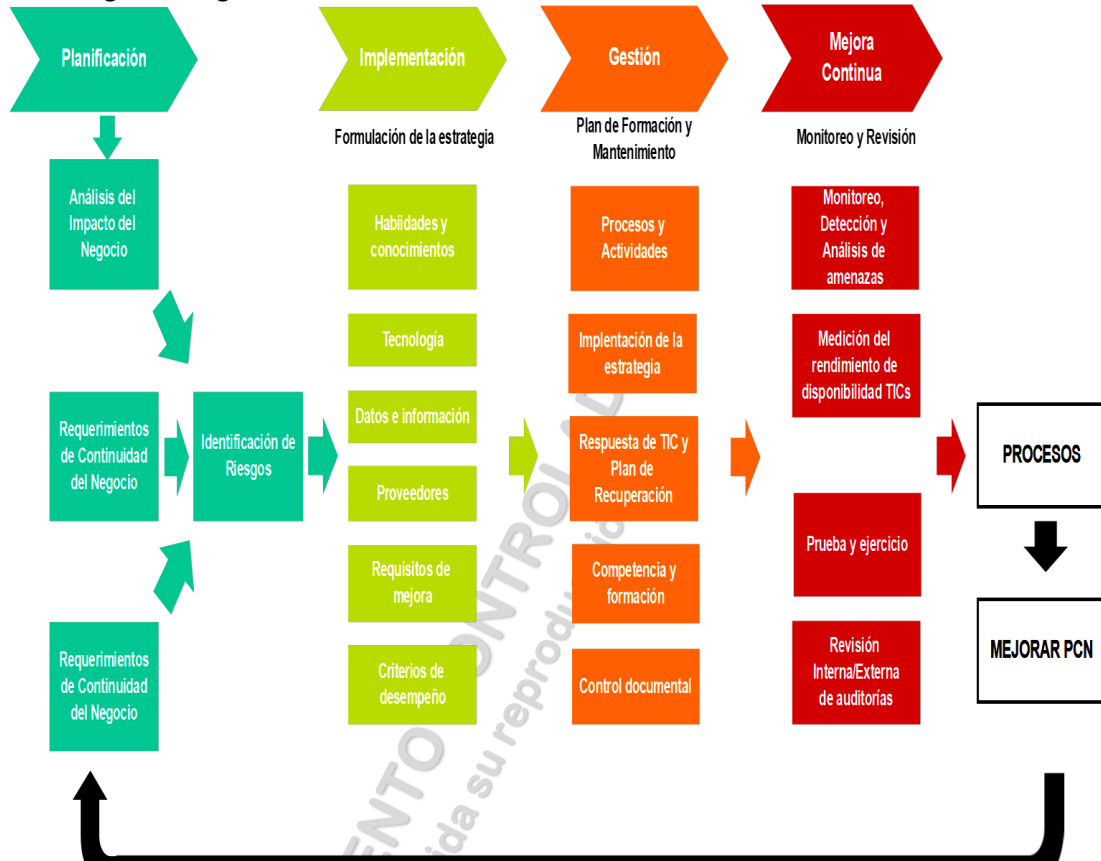


Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 4 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSIO2

Solo tendremos en cuenta las fases de planificación, implementación, gestión y mejora continua, como se muestra en la siguiente figura en donde:



La preparación de las TIC para la Continuidad del Negocio, debe mejorar y permitir:

- Responder al cambiante ambiente de riesgos.
- Asegurar la continuidad de las operaciones críticas del negocio soportadas por servicios de TIC.
- Estar preparado para responder antes de que una disrupción de los servicios de TIC ocurra, identificar los eventos o la serie de eventos relacionados provenientes de incidentes.
- Responder y recuperarse de incidentes y/o desastres y fallas.


7.3 Planificación y preparación de las TIC para la continuidad del negocio

Esta Etapa, define la estrategia metodológica que nos permitirá establecer políticas, objetivos, procesos y procedimientos pertinentes que permitan la preparación de las TIC para la continuidad del negocio. La alta dirección debe aprobar los requerimientos de continuidad del negocio de la organización y estos requerimientos darán lugar a un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad del negocio por producto, servicio o actividad.

Estos RTO's comienzan desde el punto en el cual la interrupción ocurrió hasta que el producto, servicio o actividad está disponible nuevamente.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 5 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSIO2

7.4 Política PCN

La Alta Dirección aprueba esta Política del Plan de Continuidad del Negocio, como muestra de su compromiso y responsabilidad para que se garantice su efectividad ante respuesta de emergencias o situaciones que ponga en riesgo la vulnerabilidad del negocio y sus partes interesadas.

7.5 Objetivo de la política PCN

Definir lineamientos a seguir antes, durante y después de una interrupción en los servicios de tecnologías de la información del negocio, esperando la respuesta oportuna ante estos eventos, ya que pueden afectar el funcionamiento del mismo, así como la gestión de la continuidad y restauración de las actividades, siempre garantizando el mínimo impacto.

7.6 Alcance PCN

Este plan está dirigido a cubrir las fallas en el proceso de TI en la operatividad de Comercializadora Rápido S.A. de C.V.

7.7 Declaración de la política PCN

El área de Sistemas IT se compromete a garantizar que todas las actividades primordiales se lleven a cabo con normalidad, siempre teniendo presente la continuidad, oportunidad, calidad y confiabilidad y así asegurar los servicios ofrecidos, todo esto mediante la correcta implementación y desarrollo del PCN.

Para el buen funcionamiento de esta política, se asignan Recursos: humanos, financieros y materiales, pues estos deben asegurar el cumplimiento a la misma, y además ejecutarse acorde a lo establecido.

Cada una de las personas responsables debe cubrir el 100% de sus funciones dentro de la presente política. A continuación, se establecen las políticas de PCN internas que el Área de Sistemas IT debe gestionar y supervisar:

- Sistemas IT debe supervisar que la aplicación de la presente política sea correcta y en tiempo y forma.
- Validará los procesos y actividades críticas que se establezcan en el PCN, así como el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO).
- Responsabilidades frente al Plan de Continuidad del Negocio se deben definir, compartir, comunicar y aceptar a través de cada uno de los colaboradores, contratistas y terceros.
- Asegurar que las funciones y responsabilidades descritas en el BCP, se asignen al personal idóneo y capacitado.
- Cumplimiento a los planes de capacitación al personal, tanto responsable como general, con el fin de ser útil ante alguna situación que lo amerite.
- Mantener actualizado el presente documento, con el fin de evitar obsolescencia y cruce de información.


7.8 Asignación de responsabilidades en el PCN y en seguridad de la información.

La Alta Dirección determina el siguiente comité para el PCN y poder definir la seguridad de la información, los cuales tiene como integrantes:

- Gerente General
- Gerente de Sistemas IT

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 6 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

- Gerente de Recursos Humanos

PUESTO	ROL	RESPONSABILIDADES
Gerente General	Líder	Responsables de dirigir las acciones requeridas durante la contingencia.
Gerente Sistemas	Sub-líder	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 Recursos Humanos	Sub-líder 2	Responsables de reunir los medios necesarios para llevar a cabo la activación del plan de continuidad (lugar alternativo de reunión, materiales necesarios, herramientas, etc)

7.9 Actividades críticas del negocio

Al poner en marcha el PCN, se determinan las actividades que se consideran como críticas para el negocio, puesto que, en caso de alguna catástrofe o siniestro, estas perjudican altamente a las operaciones, la información y clientes actuales. Ver **Evaluación de incidentes de seguridad de la información PECRSI14**

A continuación, se describen estas actividades:

1. Descarga eléctrica derivada de rayos eléctricos.
2. Corte de luz en tienda.
3. Restablecimiento/configuración de fábrica del equipo.
4. Apagado intencional o accidental del equipo DVR.
5. Reseteo de Modem a configuración de fábrica.
6. Escurrimiento de agua por deshielo de los climas.
7. Infección del servidor.
8. Sobrecalentamiento de servidores por falla de clima en SITE.


Derivados de estas actividades se establece el Tiempo de Recuperación (RTO), así mismo el Punto Objetivo de Recuperación (RPO) y el Objetivo Mínimo de Continuidad del Negocio (MCBO).

ACTIVIDAD CRÍTICA	TIEMPO DE RECUPERACIÓN RTO	PUNTO OBJETIVO DE RECUPERACIÓN RPO
Descarga eléctrica derivada de rayos eléctricos	120 minutos	120 minutos
Corte de luz en tienda	70 minutos	70 minutos
Restablecimiento/configuración de fábrica	40 minutos	40 minutos
Apagado intencional o accidental del equipo DVR	30 minutos	30 minutos
Reseteo de Modem para configuración de fábrica del equipo	10 minutos	10 minutos
Escurrimiento de agua por deshielo de los climas	180 minutos	180 minutos
Conexión del servidor	10 minutos	10 minutos
Sobrecalentamiento de servidores por falla de clima en SITE	30 minutos	30 minutos

EL MCBO define que las actividades: 5 y 7, deben ser las mínimas activas para que el negocio continúe sin problemas y se puedan obtener los resultados esperados.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 7 de 11
--	-----------------------	---------------------------

"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:	Manual	
	Título:	Plan de continuidad del negocio	
	Código:	MNCRSIO2	

Teniendo en cuenta los tiempos RTO, RPO y MCBO, se derivan las estrategias que aseguren la preparación de las TIC para la continuidad del negocio. Estas estrategias se mencionan a continuación:

NO	ACTIVIDAD	ESTRATEGIA		
		PREVENCIÓN	DETECCIÓN	RESPUESTA
1	Descarga eléctrica derivada de rayos eléctricos	Mtto por parte de MCD.	Inmediato	1 hr.
2	Corte de luz en tienda	Mtto de UPS Unidad de Soporte Eléctrico	Inmediato	1 hr.
3	Restablecimiento/configuración de fábrica	Mtto sistemas	Inmediato	30 min
4	Apagado intencional o accidental del equipo DVR	Encapsulamiento	1 semana de supervisión	5min
5	Reseteo de Modem para configuración de fábrica.	Stock de modem	Reporte de usuario	2min
6	Escurrecimiento de agua por deshielo de los climas	Mtto preventivo interno.	Semestral	24 hr.
7	Infección del servidor	Candados de firewall y antivirus actualizado.	Inmediata	30min
8	Sobrecalentamiento de servidores por falla de clima en SITE	Clima alterno.	Alerta Sistema de Alarmas y Seguridad	10 min

7.10 Recursos mínimos asignados para la recuperación de los servicios y sistemas

- **Recursos de hardware:** Computadoras de escritorio y portátiles, impresoras, scanner, necesarios para dar soporte a las actividades críticas.
- **Recursos de software:** Describir todo recurso software utilizado, cumpliendo con la seguridad de la información.
- **Recursos humanos:** Gerente Sistemas IT, Jefe de Sistemas, Administrador de Infraestructura, DBA, Programador, Auxiliares.
- **Recursos financieros:** Toda inversión o gasto utilizado para dar soporte y apoyo a las actividades críticas del negocio.


7.11 Implementación y preparación de las TICs para la continuidad del negocio

Esta etapa permite desarrollar el componente de planificación, teniendo en cuenta los aspectos más relevantes en la implementación de la estrategia de preparación de las TIC en la continuidad del negocio, las cuales deberán ser implementadas después de la aprobación de la alta dirección.

La alta dirección debe gestionar y proporcionar los recursos necesarios, procedimientos y operación para preparación de las TIC en la continuidad del negocio, así como los programas de entrenamiento y concientización.

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 8 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

Se deben de tener en cuenta estándares internacionales pertinentes durante la implementación de la detección y respuesta de incidentes y de los componentes de recuperación de desastres, incluyendo los siguientes:

ISO 27000
ISO 22300.

7.12 Recursos para las TIC

En este punto, debemos definir específicamente las características o condiciones que deben tener los recursos que nos serán de utilidad antes, durante y después de cualquier incidente que ponga en riesgo la continuidad del negocio.

No	RECURSO	CATEGORÍA	CARACTERÍSTICAS / CONDICIONES
1	Computadoras	Hardware	B
2	Internet	Hardware	B
3	Servidores	Hardware	B
4	Sistema operativo	Software	B
5	Capacidad ROM y RAM	Software	B
6	Antivirus	Software	B
7	Operador de los servicios	Humano	B
8	Operador del servidor	Humano	B
9	Mantenimiento	Humano	B
11	Área climatizada	Infraestructura	B
12	Candados de seguridad	Infraestructura	B
13	CCTV	Infraestructura	B

Nota: Pendiente De Cambio (PC), Bueno (B), Cambio (C), No comprobado (NC), Falta (F)


7.13 Infraestructura de los sistemas de recuperación de las TIC e información crítica

En esta parte se define características y condiciones que deben tener Sistemas de Recuperación de las TIC y de la información crítica. Dentro de esto se considera hardware, software, capacidades, mantenimientos, etc.

SISTEMA DE RECUPERACIÓN	CARACTERÍSTICAS	MANTENIMIENTO
Recuperación de la información de las operaciones.	El primer sistema se ocupa para mantener la seguridad de los equipos en red	El respaldo de la información se genera de forma diaria, para asegurar la integridad de la información.
Recuperación de la información de los clientes.	El segundo sistema se ocupa cuando se han averiado las UPS.	Por automático se genera un respaldo en base de datos con proveedor externo

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 9 de 11
--	-----------------------	---------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

Recuperación de los servidores.	Sistema de recuperación utilizado en caso de una pérdida del servidor por falla técnica o incidente.	Mantenimiento preventivo a todos los activos de la información.
Recuperación de los equipos operativos	Se hacen los cambios de piezas, en caso de funcionalidad nula; se destruyen.	

7.14 Estructuras tecnológicas de tic implementadas

Determinamos que tecnologías actuales y nuevas tenemos implementadas para la preparación de las TIC ante la continuidad del negocio. En este caso, pueden ser ya implementadas o por implementar, siempre siendo validadas por la Alta Dirección.

TECNOLOGÍA	ESTADO	FUNCIÓN
CPU	B	OPERATIVA/ADVA
Monitor	B	OPERATIVA/ADVA
Teclado	B	OPERATIVA/ADVA
Mouse	B	OPERATIVA/ADVA
Escáner	B	OPERATIVA/ADVA
Impresora	B	OPERATIVA/ADVA
Cajón efectivo	B	OPERACIONAL
PIN PAD Bancomer	B	OPERACIONAL
PIN PAD Santander	B	OPERACIONAL
Mikrotik	B	OPERACIONAL
UPS	B	OPERACIONAL
Teléfono	B	COMUNICACIÓN
DVR	B	VIGILANCIA
Cámaras	B	VIGILANCIA
Cables red	B	OPERACIONAL

Nota: Pendiente De Cambio (PC), Bueno (B), Cambio (C), No comprobado (NC), Falta (F)


7.15 Disponibilidad de datos

La disponibilidad de datos se deriva de los tiempos de recuperación y el objetivo mínimo de continuidad, puesto que estos determinan que tanta disponibilidad se puede tener durante un incidente. Estos nos muestran un panorama más real del impacto que se tiene en el negocio.

No	Actividad/Proceso	Disponibilidad de datos (%)	Ante un incidente	
			RPO	Disponibilidad de datos (%)
1	Respaldo de información	100%	90%	100%
2	Validación de los antivirus	100%	90%	100%
3	Actualizar desarrollos de software	100%	90%	100%
4	Mantener actualizado mikro Tik	100%	90%	100%
5	Monitoreo de temperatura de servidores	100%	90%	100%

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 10 de 11
--	-----------------------	----------------------------

"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:	Manual
	Título:	Plan de continuidad del negocio
	Código:	MNCRSI02

7.16 Proveedores críticos y su capacidad para soportar los servicios

PROVEEDOR CRÍTICO	SERVICIO
TELMEX	Internet
CFE	Electricidad
AREA DE MTTO	Mantenimiento Preventivo a Activos
TELCEL	Telefonía
EMUNAH	Telefonía y servicios otros
SANTANDER	Servicios Financieros
BANCOMER	Servicios Financieros
FACTURACIÓN SIFEI	Facturación Electrónica

7.17 Plan de respuesta: control, contención y comunicación de incidentes, involucrando a partes interesadas

Teniendo en cuenta las actividades críticas, los tiempos, recursos y partes interesadas, se determina un Plan de Respuesta para los incidentes actuales y por haber, incluyendo medidas preventivas y de acción para dichos incidentes.

7.18 Evaluación del desempeño de las TIC para la continuidad del negocio

Esta etapa nos permite evaluar el desempeño y la eficacia de la implementación, para la medición de la efectividad de los procesos y controles, se deben tomar los indicadores definidos en el componente de implementación para llevar a cabo el plan de seguimiento, evaluación y análisis.

7.19 Mejora continua para la preparación de las TIC para continuidad del negocio.

Esta etapa permite realizar acciones correctivas apropiadas a los potenciales impactos determinados por el análisis de impacto del negocio **Análisis de Impacto al Negocio (BIA) PECRSI21_F01(2)** de acuerdo lo descrito en el **Gestión de disponibilidad y capacidad PECRSI21**.

8. DIAGRAMA DE FLUJO

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

9. ANEXOS

TIPO	CODIGO	TITULO
Formato	NA	NA
Ayuda visual	NA	NA
Políticas	NA	NA
Otros (documento externo)	PECRSI21	Gestión de disponibilidad y capacidad
	PECRSI21_F01(2)	Análisis de Impacto al Negocio (BIA)

Vigente a partir de: 29-ABR-2024	Revisión: 4	Página: 11 de 11
--	-----------------------	----------------------------

"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"