Plan de Recuperación de Desastres (DRP)

Procedimiento

OID 1.3.6.1.4.1.53748.1.1.006

Identificación del Documento

Identificación del documento	Plan de Recuperación de Desastres
Registro(s) relacionado(s)	Escriba texto
Documento(s) relacionado(s)	POL 0000 Política de Continuidad del Negocio_Toc2019
Responsable de aprobación	Ricardo Navarro - CEO
Dueño funcional	OSI – Gustavo Veliz Estrada
Puesto(s) implicado(s)	Responsable del SGI, OSI, CEO, Gerente General, Líder de Proceso, Responsables de proceso.

1. Alcance

El presente documento se inserta dentro del Programa de Continuidad de negocios, provee una base para comprender, desarrollar e implementar planes de continuidad para los servicios de TOC
Define un protocolo de acción y una lista de actividades a desarrollar cuando se declare una situación de “Contingencia Operacional o Informática”, con el objeto de mantener la continuidad operacional del negocio y restituir el funcionamiento de los sistemas: Verificación de identidad con biometría dactilar, Verificación de identidad con biometría facial, Firma Electrónica, Firma Electrónica Avanzada. Además, se debe mantener en condiciones de funcionamiento la Red Telefónica, Red de Datos, Internet y los servicios de correo electrónico.

Los servicios ofrecidos por TOC están disponibles para uso en horario de Lunes a Domingo en forma continuada desde las 07:00 a las 23:00 horas.

Establecido el nivel de servicios esperado, se entenderá por “Contingencia Informática” a aquel estado en la cual no es posible dar cumplimiento al nivel de servicio comprometido y como consecuencia está en riesgo la continuidad del desarrollo del negocio. Una Contingencia Informática puede derivar en una “Contingencia Operacional”, cuando la disponibilidad es nula o insuficiente para responder a los requerimientos de los clientes, lo que obliga a recurrir a procesos operativos alternativos.

El responsable de mantener y actualizar este Plan es el Oficial de Seguridad de información de TOC.

2. Objetivo

Los objetivos del Plan de Recuperación de Desastres de TOC, son los siguientes:

- Minimizar el grado de la interrupción, el daño y el impacto asociado a los procesos críticos del negocio, frente al escenario de contingencia definido en el Sistema de Gestión de Seguridad de la Información.
- Proporcionar los mecanismos para una rápida y adecuada restauración de las operaciones tecnológicas en las instalaciones declaradas por TOC.

El Plan se enfoca en responder en forma adecuada frente a situaciones de contingencia, y que se logre mitigar el impacto que dicha contingencia puede ocasionar en nuestros clientes.

En base a este enfoque, se definen procedimientos que permiten: administrar una posible crisis; recuperar el negocio; recuperar el soporte informático y de telecomunicaciones; operar durante el régimen de contingencia; y volver a la normalidad una vez superada la interrupción. También da relevancia a que el personal tome conciencia sobre la continuidad operacional, lo que permite que las personas responsables de ejecutar las soluciones las lleven a cabo de la mejor manera. Además es fundamental contar con los recursos mínimos y críticos necesarios, tanto tecnológicos, de infraestructura y personal, que permitan implementar y ejecutar las estrategias de recuperación descritas en el Plan.

3. Definición de estructura y responsabilidades

En presencia de un escenario de contingencia, TOC S.A. ha determinado que sólo algunos puestos de trabajos serán restituidos para garantizar la continuidad del negocio, decisión que se basa en las siguientes definiciones de procesos necesarios para la continuidad del negocio

Áreas que deben seguir operando:

- Gerencia de Operaciones
- Desarrollo
- Labs
- Finanzas

En consecuencia se privilegiarán los puestos de trabajo que necesitan estar conectados a la red de servidores y servicios con el objetivo que la operación del día sea soportada.

4. Evaluación de impacto de interrupción de servicios relacionados con las obligaciones

Las obligaciones con nuestros clientes están descritas en el documento contrato acordado y firmado con cada uno de ellos y TOC S.A. cuenta con procedimientos que ayudan en el cumplimiento adecuado de estas (obligaciones y horarios definidos) y cuyo incumplimiento es de alto impacto para la organización, tanto en términos de calidad, imagen y reputación.

Dado lo anterior cualquier escenario de Contingencia podría impactar en el cumplimiento de estas obligaciones y las medidas necesarias para mitigar su efecto.

Tiempos Máximos
De acuerdo a loa anterior se determinan los siguientes RTO (Recovery Time Objective, tiempo durante el cual TOC puede tolerar la falta de funcionamiento de sus aplicaciones, sin afectar a la continuidad del negocio).

Servicios	RTO
Verificación de identidad con biometría dactilar	2 horas
Verificación de identidad con biometría facial	2 horas
Firma electrónica	2 horas
Firma electrónica avanzada	2 horas

5. Declaración de Escenario de Contingencia

La transición desde un escenario de operación normal de servicio a un escenario de contingencia, será impulsada por una decisión y declaración explícita del Gerente de Operaciones, al constatarse que no hay acceso a las instalaciones y/o los servicios de TI.

Contingencia de red de datos

i) Falla de red que impide el acceso a los servidores centrales.

Desastre de instalación

ii) Destrucción total o parcial de las instalaciones por efectos de sismo, incendio, inundación o actos maliciosos.
iii) Destrucción total o parcial del datacenter en el cual se encuentran los servidores de TOC.

Los eventos enumerados, pueden ser el producto de múltiples causas aisladas o concurrentes, cuyo estudio y solución es materia del plan de acción específico que se elabore para cada tipo de contingencia.

6. Declaración de contingencia

- Habiéndose reportado una interrupción de alguno de los servicios de antes enunciados, la Gerencia de Operaciones inspeccionará el problema de forma de determinar, Veracidad del reporte, clientes afectados, Impacto en el negocio y deberá informar al resto de las gerencias el estado de la situación.

- A continuación el Gerente de Operaciones emitirá una comunicación a los clientes notificando de la presencia de una falla e identificando los servicios afectados, este mensaje se emitirá por correo interno.

- La Gerencia de Desarrollo/Labs y la Gerencia de Operaciones efectuarán todas las acciones técnicas que están a su alcance para corregir la falla y restituir el servicio, este esfuerzo se desarrollará mediante recursos propios o de terceros contratados.

- Transcurridos un máximo de 1 hora desde el reconocimiento de la falla y no habiéndose restituido el servicio afectado, el Gerente de Operaciones presentará al CEO un informe que incluye: Estado de la instalación, Acciones de reparación en desarrollo, Cursos de Acción Alternativos y sus costos estimados, además de los plazos de solución estimados.

- El Gerente de Operaciones, CEO y Gerente de Desarrollo/Labs, una vez evaluado los antecedentes disponibles resolverán si se declara escenario de contingencia o se continúa en escenario de falla de servicios.

- Transcurridas una hora más y no habiéndose restituido el servicio afectado automáticamente se declarará escenario de contingencia.

- Una vez declarado el escenario de contingencia el Gerente de Operaciones se comunicará con el CEO para informar respecto al estado de la instalación y de la activación de los planes de contingencia previstos.
  Una comunicación en igual sentido se hará llegar a todos los clientes.

- El Gerente de operaciones coordinará con miembros del personal del área de Tecnología, que estime conveniente y que se requiere su presencia en la oficina o en las instalaciones alternativas definidas.

- De ahí en adelante a intervalos de 2 horas y hasta la restitución del servicio, el Gerente de operaciones informará directamente al CEO, respecto a la evolución del Plan de Contingencia en ejecución.

- La coordinación operativa para la ejecución del Plan de Contingencia y su supervisión en terreno queda asignada al Gerente de Operaciones con el apoyo del OSI, el cual en este escenario asume plenas atribuciones para asignar tareas propias del plan al personal de TOC y para reubicar físicamente los puestos de trabajo del personal.

- La responsabilidad final por la ejecución del Plan de Contingencia y sus resultados, así como la autorización para volver a la operación normal le corresponde al Gerente de Operaciones.

7. Plan de contingencia frente a distintos escenarios

TOC S.A. tiene un plan de contingencia que permite el funcionamiento alternativo, para cada uno de los servicios y cada uno de ellos está calificado con criticidad alta. Dicho plan de contingencia estará activo todo el tiempo que sea necesario, y consistente en procesos alternativos Se consideran planes para los siguientes escenarios:

a) Sin sistemas
b) Sin instalaciones
c) Sin personal
d) Sin proveedores
e) Sin servicios básicos (agua potable, energía eléctrica)

8. Plan de contingencia frente a falla de Datos

Esta falla puede ser declarada por 2 causas, la primera es por una falla en la instalación interna de la red de TOC y la segunda una falla en el enlace de internet en el Datacenter.
En el primer caso, falla es reportada al área de soporte internos.
En el segundo caso, se activa enlace de contingencia y se reporta al proveedor y soporte externo.

9. Plan de contingencia frente a indisponibilidad de energía eléctrica

Esta falla puede ser generada debido a una interrupción programada o una interrupción imprevista.
En el caso de la interrupción del servicio se debe averiguar con la compañía proveedora del servicio de electricidad el tiempo de demora del corte, en el caso que amerite se debe activar el **Procedimiento Sin servicios básicos**. Esta medida será validad por el Gerente de Operaciones y CEO, esta decisión dependerá de la cantidad de tiempo que exista el corte programado o imprevisto y el horario del corte.

10. Plan de contingencia frente a falla de red telefónica

En caso de interrupción del servicio telefónico, se utilizará la telefonía celular y correo electrónico como mecanismo de comunicación tanto interna como con los clientes de TOC.
Los clientes deben utilizar el sitio web de TOC para reportar cualquier requerimiento o incidente (operación normal realizada por los clientes).

11. Plan de contingencia frente a escenarios sin instalaciones y sin sistemas.

TOC ha desarrollado un Plan para enfrentar las contingencias informáticas, el que tiene como objeto asegurar el correcto funcionamiento de sus sistemas.
En el caso de indisponibilidad del datacenter primario los servicios serán provistos por el sitio secundario o de contingencia. **Refiérase al Procedimiento sin Sistemas.**

12. Pruebas de contingencia

Las pruebas de Contingencia cumplen dos objetivos:

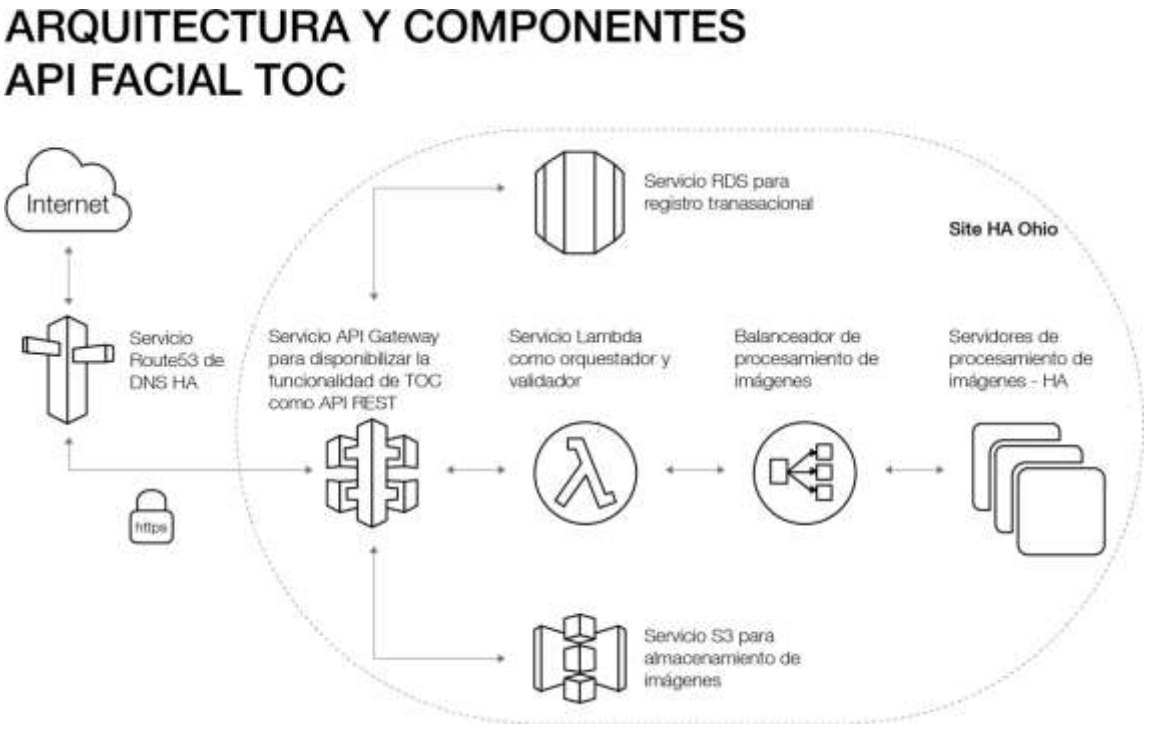
- Verificar la operación y recursos necesarios
- Capacitar y entrenar al personal de manera que esté debidamente preparado ante situaciones de contingencia.

Las pruebas deben quedar debidamente documentadas y deben contener evidencias que acrediten que el plan funciona correctamente.
El plan debe ser probado y actualizado basándose en los resultados de cada ejercicio. Es importante que cada componente sea probado individualmente. Las pruebas pueden ser disruptivas, por tanto se requiere el apoyo por parte de cada área o gerencia para asegurar la disponibilidad del personal.

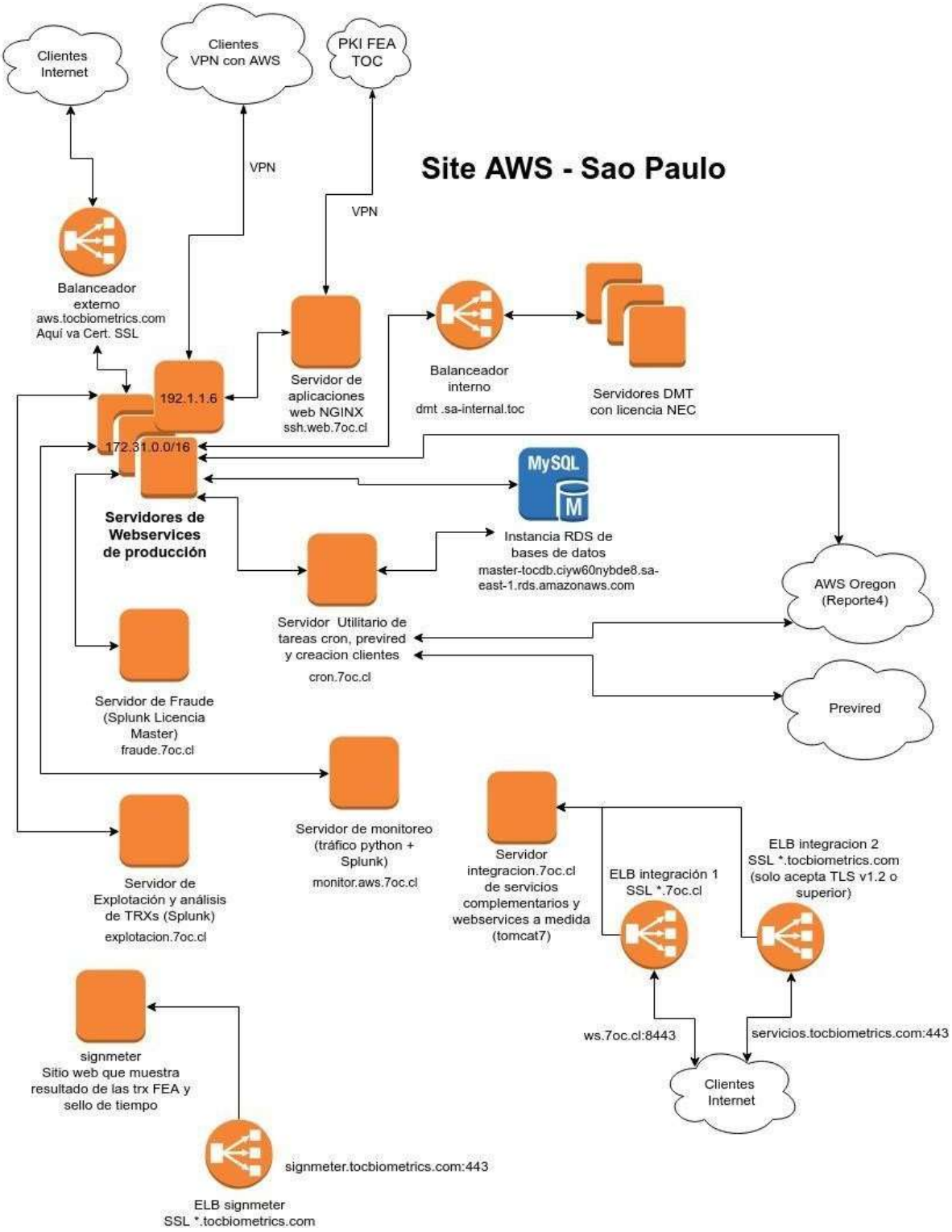
El plan está compuesto de una serie de actividades orientadas a mantenerlo actualizado y vigente. Las pruebas están enmarcadas dentro de un calendario de pruebas y se compone de las siguientes partes:

- Definir el alcance y objetivo de la prueba
- Programar la prueba
- Definir el equipo participante de la prueba
- Ejecutar la prueba
-

13. Servidores/Servicios

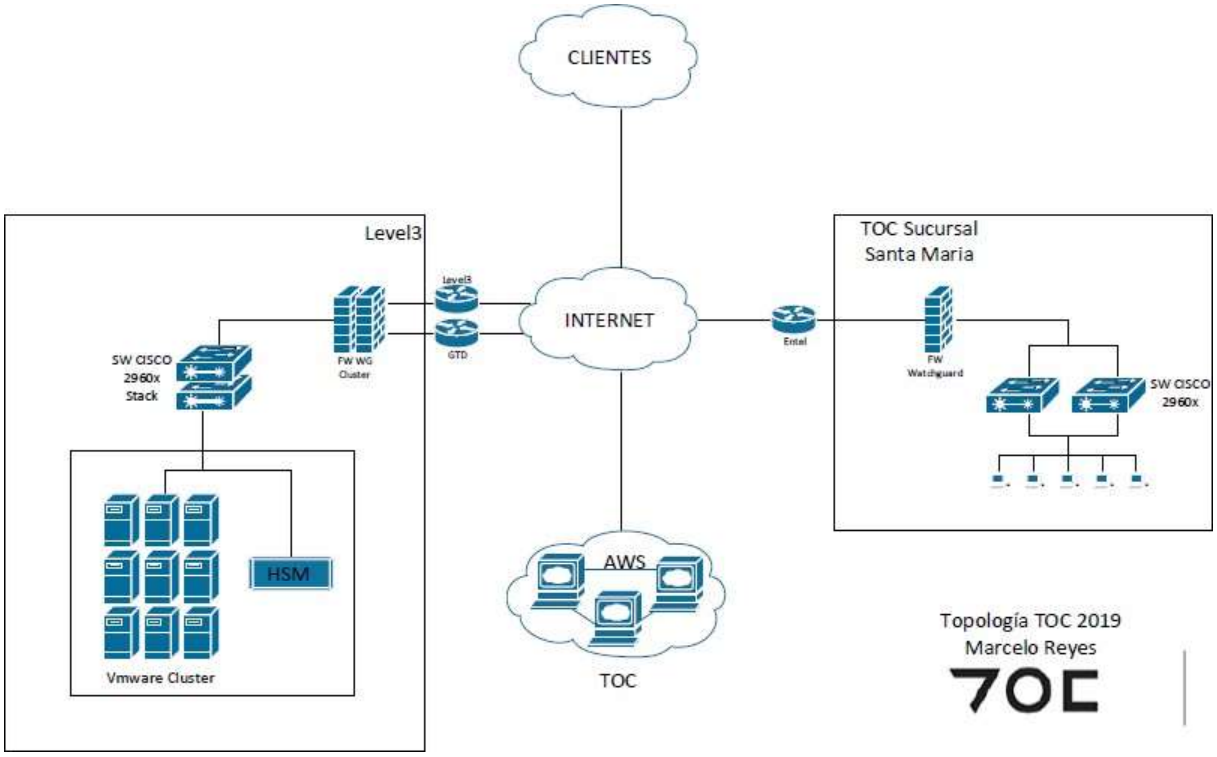


ARQUITECTURA VERIFICACION



Servicio	Ubicación	Descripción Escenario	Estrategia de Recuperación
Verificación de identidad DACTILAR	**CenturyLink**	**Inhabilitación total del sitio producto de un desastre (terremoto, incendio, inundación, falla completa de energía, u otro evento). Implica la interrupción simultánea de todos los servicios.**	**Activación sitio AWS-Sao Paulo**
	AWS-Sao Paulo.		**1) Activación de sitio CenturyLink** **2) Activación sitio AWS Virginia del Norte, USA**
Verificación de identidad FACIAL	**AWS OHIO**		**Activación sitio AWS-Irlanda**
Firma Electrónica Avanzada (FEA)	**CenturyLink**		**Activación sitio AWS-Sao Paulo**

14. Diagrama de enlaces



15. Equipo Recuperación de desastres

Equipo de Recuperación de Desastres		
Nombre	**Cargo**	**Rol**
Nicolás Aguilera	Gerente de Operaciones	Coordinador Recuperación de Tecnología de información (CRTI)
Tomás Castañeda	Gerente de Labs y Desarrollo	Coordinador de infraestructura Tecnológica (CIT)
Diego de la Cruz	Jefe Desarrollo	Coordinador Sistemas de información (CSI)
Gustavo Veliz	OSI	Coordinador Recuperación de Tecnología de información (CRTI)

Servicios	Cargo
Infraestructura	Servidores de aplicación
	Controlador de Dominio
	Backup/Restore
	Correo Electrónico
	Comunicaciones
	Documental
Sistemas	Bases de Datos
	Documentación
	Seguridad perimetral
	Seguridad Física
	Aplicación

Equipo de Recuperación de Desastres

Esta sección identifica a los equipos de personas involucradas en el esfuerzo de recuperación del evento de desastre y sus responsabilidades asociadas. Las pautas consideradas para la conformación de estos equipos han sido las siguientes:

- Todo equipo debe estar conformado por un líder y un reemplazante.
- Ninguna persona debe estar participando en más de un área cuyas tareas sean concurrentes durante la recuperación de un desastre,
- Todas las personas identificadas en el Equipo de Recuperación de Desastres, deben conocer las responsabilidades que tienen que asumir. De esta manera se minimiza las posibilidades de inoperatividad de los equipos debido a la ausencia de sus integrantes y/o al desconocimiento de sus responsabilidades.

a) Coordinador Recuperación de tecnología de información (CRTI)

- Encargado de coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Recuperación de Desastres TI.
- Liderazgo general a los equipos de personas involucradas en el proceso de recuperación.
- Evaluar la extensión del desastre y sus consecuencias potenciales sobre la infraestructura.
- Mantener informada a la alta gerencia acerca de la situación y el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Documentar detalladamente los hitos del evento y las actividades

realizadas para lograr la recuperación de las operaciones.
- Monitorear la ejecución de los procedimientos de recuperación
- Supervisar/vigilar la recuperación de infraestructura de TI ubicada en el datacenter.
- Generación de gestión, informando el estado de los servicios y resultado de la contingencia.

b) Coordinador de infraestructura tecnología (CIT)

- Evaluar el daño en la plataforma tecnológica de TOC, coordinar y dirigir las acciones necesarias para su recuperación en el Data Center secundario y la restauración de los servicios a condiciones normales.
- Recuperar la plataforma base de los sistemas críticos TOC de acuerdo a la prioridad de recuperación definida.
- Asegurar que toda la documentación relacionada a estándares, operaciones, registros vitales, programas de aplicación, etcétera, se encuentren almacenados en un ambiente seguro.
- Mantener procedimiento de respaldo y restauración actualizado
- Mantener actualizado el diagrama actual de conexiones de dispositivos primario y de contingencia
- Mantener actualizado inventario de infraestructura de comunicaciones de datos y coordinar las estrategias de recuperación con los proveedores de servicios.

c) Coordinador de Sistemas de información (CSI)

- Levantar los servicios de Base de Datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios.
- Supervisar el correcto funcionamiento de sistemas y/o aplicaciones
- Disponer de documentación actualizada de aplicaciones y/o sistemas productivos.
- Disponer procedimientos operacionales
- Validar el correcto desempeño de los servicios durante la contingencia

d) Oficial de Seguridad de información (OSI)

- Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de contingencia.
  Disponer informes que describan la situación de contingencia, sus hitos, desarrollo y solución.

16. Revisión y aprobación del documento

El presente documento ha sido revisado y aprobado mediante firma electrónica:

Elaborado	Revisado	Aprobado
Gustavo Veliz Estrada	Ricardo Navarro Luft	Ricardo Navarro Luft

17. Revisión y aprobación del documento

Versión	Descripción del cambio	Solicitado por:	Realizado por:	Aprobado por:	Fecha Aprobación	Vigente a partir de:
0.0	Versión inicial	OSI	OSI	CEO	14/02/2019	14/02/2019

LegalSign

12484529-7
Gustavo Alonso
Veliz Estrada
A030303174
NzhmMjk1MDE0O0Y3MDEz
2019/05/27 22:42:36 UTC
gustavo.veliz@toc.cl

6956763-0
Ricardo Andres
Navarro Luft
100004900
OGE1MWM3YzBjO0Y3MDIz
2019/05/28 14:51:42 UTC
ricardo.navarro@toc.cl