Plan de Continuidad

P-CON-03

SHIFT
Workforce Management

1. Objetivo

El objetivo de este documento es identificar y analizar las potenciales amenazas que podrían impactar las operaciones de SHIFT, para definir las estrategias de recuperación necesarias que puedan dar soporte a los procedimientos críticos de la empresa, incluyendo las Tecnologías de Información y Comunicación (TIC), permitiéndole ser resiliente y con la capacidad para recuperarse ante eventos inesperados.

Además, este documento tiene como finalidad el asegurar el conocimiento para la implementación correcta de los procedimientos de continuidad a través de su mantenimiento, capacitación constante y la aplicación de pruebas.

2. Alcance

Este documento alcanza a todas las áreas de la empresa de manera integral, incluyendo el Plan de Recuperación ante Desastres, el Análisis de Impacto en el Negocio (BIA), y a todos los elementos que sean requeridos para mantener la continuidad de las operaciones del negocio.

3. Plan de Continuidad

3.1 Responsabilidades de la gestión de la continuidad del negocio

SHIFT define a los integrantes del comité de crisis y del equipo de continuidad en la siguiente tabla:

Rol de continuidad	Área y rol	Nombre	Contacto
Comité de Crisis	Comité de Seguridad de la Información	• Francisco López • Andres Lillo • Nelson Vasquez • Pablo Vega • Masato Wada • Javier Olivares	• flopez@shiftlabor.com • alillo@shiftlabor.com • nvasquez@shiftlabor.com • pvega@shiftlabor.com • mwada@shiftlabor.com • jolivares@shiftlabor.com

Líder del equipo de continuidad	TI-CTO	Francisco López	flopez@shiftlabor.com
Miembros del equipo de continuidad	• Infraestructura & Seguridad • Líder de Desarrollo • Jefe de Operaciones • CCO • Gerencia General – CEO • Gerencia de eficiencia operacional	• Fermín Vargas • Andres Lillo • Javier Olivares • Masato Wada • Nelson Vasquez • Pablo Vega	• fvargas@shiftlabor.com • alillo@shiftlabor.com • jolivares@shiftlabor.com • mwada@shiftlabor.com • nvasquez@shiftlabor.com • pvega@shiftlabor.com

A continuación, se describen las responsabilidades específicas del comité de crisis y del equipo de continuidad:

- El Equipo de Continuidad es el responsable de revisar que todos los elementos alcanzados por el SGSI se encuentren considerados dentro de los planes y procedimientos para la gestión de la continuidad del negocio.
- El Equipo de Continuidad es el responsable de garantizar que la gestión de la continuidad del negocio sea implementada siguiendo lo establecido en este documento y de proporcionar los recursos necesarios para ello.
- El Equipo de Continuidad es el responsable de adoptar e implementar el programa de capacitación y concientización aplicable a todas las personas que cumplen una función en la gestión de la continuidad del negocio.
- Infraestructura & Seguridad es el responsable de la implementación operativa, la aplicación de las pruebas pertinentes y del mantenimiento de la continuidad del negocio, así como de implementar, atender y mitigar operativamente cualquier amenaza en los procesos establecidos y en las TIC.
- Infraestructura & Seguridad es el responsable de elaborar los informes de resultados de las pruebas de continuidad aplicadas, de identificar las oportunidades de mejora y proponer las acciones correctivas pertinentes, en caso de ser necesarias.
- Infraestructura & Seguridad es el responsable de evaluar y supervisar periódicamente la eficacia de los procedimientos establecidos en este documento durante su implementación en un evento inesperado.
- El Comité de Seguridad es la responsable de revisar y aprobar el plan al menos **una vez por año** o cada vez que se produzca una modificación significativa.

3.2 Procedimientos de recuperación

SHIFT define estrategias y procedimientos de recuperación para todos los elementos tecnológicos y operacionales que dan soporte a los procesos críticos de la organización.

Y para definir el plan de continuidad más adecuado a las operaciones y necesidades de la empresa, se realiza un Análisis de Impacto del Negocio (BIA) aplicando los siguientes pasos:

1. **Recopilación de información:** Esto consiste en identificar, por lo menos, la siguiente información:
    - Nombre y descripción de todos los procesos que son alcanzados por el SGSI de la organización, y otros procesos de negocio relevantes para el programa de seguridad.
    - Área o puesto responsable de los procesos.
    - Dónde se llevan a cabo.
    - Las entradas y salidas de cada uno de los procesos.
    - Interferencias o dependencias con otros procesos.
    - Los recursos y herramientas utilizadas para ejecutarlos.
    - Los usuarios del proceso.
2. **Análisis de la información:** Se analiza la información recopilada buscando responder las siguientes preguntas:
    - ¿Cuáles son los procesos críticos o más importantes para mantener en funcionamiento las operaciones de tu negocio?
    - ¿Cuáles son los recursos necesarios para que dichos procesos funcionen correctamente?
    - ¿Cuál es el tiempo ideal que debería tomar el recuperar el funcionamiento de esos procesos en caso de presentar fallas o interrupciones, y cuál es el presupuesto disponible para ello?
3. **Criticidad de los procesos:** Una vez realizado el análisis, se identifican los procesos críticos de la organización que son esenciales para las operaciones y su continuidad, y con base en ello, se priorizan para la generación de estrategias de recuperación.
4. **Impacto en las operaciones:** Se debe identificar y clasificar el impacto que la interrupción de un proceso crítico puede ocasionar al negocio. Esta evaluación considerará dimensiones tanto cualitativas como cuantitativas, y su severidad dependerá de los tiempos de recuperación establecidos.

    Para determinar el nivel de impacto, se deben analizar las siguientes categorías:
    - Impacto Financiero: Considera las pérdidas económicas directas o indirectas, como la pérdida de ingresos, costos de recuperación, multas por incumplimiento de contratos (SLA) o sanciones regulatorias.

- Impacto Reputacional y de Marca: Evalúa el daño a la imagen y confianza de SHIFT ante clientes, proveedores y el mercado en general. Una afectación a la reputación puede impactar la lealtad del cliente y la capacidad de atraer nuevos negocios.
- Impacto en la Seguridad de la Información: Analiza la afectación a los pilares de la información, tales como:
    - Confidencialidad: Divulgación no autorizada de información sensible.
    - Integridad: Alteración no autorizada de los datos.
    - Disponibilidad: Imposibilidad de acceder a la información o a los servicios.

- Impacto Legal y de Cumplimiento: Considera el incumplimiento de obligaciones contractuales, leyes o regulaciones aplicables en los países donde operan.

5. **Tiempos de recuperación:** Una vez definidos los procesos críticos, se establece el RTO (objetivo de tiempo de recuperación) y RPO (objetivo del punto de recuperación) que deben cumplir las estrategias de recuperación para cada uno de estos procesos.

Los siguientes documentos complementan la gestión de continuidad dentro de la empresa:

- Procedimiento de Gestión de Incidentes de Seguridad
- Plan de Recuperación ante Desastres
- Matriz de Riesgos

3.2.1 Recuperación ante indisponibilidad total de suministro eléctrico

RPO: 0 hora	RTO: 1 hora

SHIFT plantea las siguientes acciones para mantener la continuidad de sus operaciones en caso de presentar indisponibilidad total del suministro eléctrico:

- Traslado a una ubicación segura, ya sea pública o personal, donde se puedan obtener los servicios de suministro eléctrico pertinentes para continuar con las actividades de trabajo.
- Asegurar que los colaboradores utilicen una conexión a internet segura. En caso de conectarse a redes públicas, deben usar la VPN de la empresa.
- Utilizar los dispositivos portátiles de la compañía, los cuales deben tener activado el antivirus, firewall y cifrado de disco.
- Acceder a la información y sistemas a través de los repositorios oficiales de la empresa, evitando descargar archivos localmente.

- Mantener un entorno de trabajo que garantice la privacidad de la información, evitando que personas no autorizadas puedan ver documentos o pantallas con datos confidenciales.

3.2.2 Recuperación ante indisponibilidad total de los servicios On premise o en la nube

RPO: hasta 24 horas	RTO: hasta 24 horas

SHIFT plantea las siguientes acciones para recuperar sus operaciones en caso de presentar indisponibilidad total del servicio de Azure:

- El colaborador que identifique la caída de los servicios de nube debe reportar de inmediato al líder del equipo de continuidad para que se analicen las acciones a tomar.
- El líder del equipo de continuidad comunica al personal interno sobre la caída de los servicios de la Infraestructura On-Premise o Infraestructura Azure.
- El equipo de continuidad evalúa el impacto de la caída de los servicios en las operaciones de la empresa, y levanta el reporte correspondiente con el proveedor, tanto para establecer la causa raíz del problema como para determinar el tiempo estimado de restablecimiento del servicio.
- Una vez dimensionado el impacto del incidente, se evalúa la necesidad de notificar a los clientes por medio de un correo electrónico para comunicar la interrupción del servicio.
- El comité de crisis en conjunto con el equipo de continuidad debe analizar diferentes estrategias para mitigar el impacto sobre las operaciones y servicios, como por ejemplo el envío y almacenamiento de recursos críticos en ubicaciones alternativas.
- En una última instancia, se debe considerar la contratación de proveedores alternativos que puedan satisfacer las necesidades de la organización.

3.2.3 Recuperación ante indisponibilidad de la conexión de red

RPO: 0	RTO: 6

SHIFT plantea las siguientes acciones para recuperar sus operaciones en caso de presentar indisponibilidad de la conexión de red:

- El equipo de Infraestructura & Seguridad inicia el reporte al proveedor para hacer valer el SLA y dar seguimiento a la resolución.

- Solicitar o realizar conmutación por falla (Failover) en caso de aplicar para los escenarios de datacenter y servicios Azure, en el caso de oficina aplican las mismas acciones que en **Recuperación ante indisponibilidad total de suministro eléctrico**.

- Se registra el evento siguiendo el "Procedimiento de Gestión de Incidentes de Seguridad", documentando la causa, el impacto y las acciones tomadas.

3.2.4 Recuperación ante indisponibilidad parcial o total de personal crítico

RPO: 24 horas (o el cierre del último día hábil)	RTO: hasta 24 horas

SHIFT plantea las siguientes acciones preventivas para mantener la continuidad de sus operaciones en caso de presentar indisponibilidad parcial o total de personal crítico:

- Identificar las principales responsabilidades del personal crítico dentro de la empresa.
- Reducir las actividades no críticas y aquellas que son susceptibles a ser pospuestas.
- Seleccionar a los colaboradores más adecuados y capacitarlos para que obtengan los conocimientos y habilidades necesarios para suplir al personal crítico.
- Brindar una formación multidisciplinaria a los colaboradores a través de webinars, talleres, cursos, capacitaciones, etcétera.

Se definen además, las siguientes acciones correctivas:

- Dividir las actividades de trabajo del personal crítico entre los colaboradores más adecuados dentro del área correspondiente, mientras se planifica un programa de capacitación adecuado y/o se encuentran los reemplazos.
- Levantar los requerimientos de personal necesarios al área de Recursos Humanos y publicar las ofertas de empleo para reclutar nuevos candidatos.
    - Dependiendo de la urgencia del reclutamiento, se podrá realizar una contratación extraordinaria que facilite la velocidad de aprobación o rechazo del candidato por parte de la alta dirección.

3.2.5 Recuperación ante indisponibilidad parcial de sistemas operativos / base de datos

RPO: hasta 24 horas	RTO: hasta 24 horas

SHIFT plantea las siguientes acciones para recuperar sus operaciones en caso de presentar indisponibilidad o fallas en los sistemas operativos y/o bases de datos:

- Se debe realizar el reporte pertinente y la ejecución de los pasos establecidos dentro del Plan de Recuperación ante Desastres de la empresa.

3.2.6 Recuperación ante siniestros y catástrofes

RPO: hasta 24 horas	RTO: hasta 24 horas

SHIFT plantea las siguientes acciones para recuperar sus operaciones en caso de ocurrir algún suceso catastrófico, siniestro o desastre natural:

- Tener una lista de todos los colaboradores y mantener actualizada su información de contacto, incluyendo números telefónicos alternos y de emergencia.
- Contactar a los colaboradores que estuvieron presentes durante el suceso o cerca de la zona.
- Investigar si hubo heridos o víctimas fatales.
- Investigar si hubo pérdidas materiales o daños a los espacios de trabajo y de ser así, identificar todos los elementos o activos afectados.
- Determinar los daños a las oficinas o instalaciones de la empresa.
- Estimar los gastos y planificar las actividades de recuperación.

3.2.7 Recuperación ante indisponibilidad parcial de las Tecnologías de Información y Comunicación (TIC)

RPO: hasta 24 horas	RTO: hasta 12 horas

SHIFT plantea las siguientes acciones para recuperar sus operaciones en caso de presentar indisponibilidad o fallas en las tecnologías de información y comunicación.

- Se debe realizar el reporte pertinente y la ejecución de los pasos establecidos dentro del Plan de Recuperación ante Desastres de la empresa.

4. Mantenimiento del plan

4.1 Difusión y formación

SHIFT ha definido un programa de capacitación para los principales responsables, los cuales son adecuadamente formados y concientizados sobre los temas más relevantes que contempla la continuidad del negocio, incluyendo la identificación de los procesos críticos, la gestión de riesgos, los procedimientos de respuesta a incidentes de seguridad, etcétera.

Además, se difunden todos los documentos relacionados a la gestión de la continuidad del negocio, incluyendo la Política de Seguridad de la Información.

4.2 Mejora y actualización

SHIFT revisa anualmente este documento y lo actualiza siempre que sea necesario, ante cambios significativos y por la aplicación de mejoras; incorporación de nuevos escenarios, procesos, etcétera.

4.3 Pruebas del plan

SHIFT realiza pruebas de los procedimientos y estrategias de recuperación definidos en este documento para asegurar su efectividad, simulando los escenarios descritos y siguiendo las acciones establecidas.

Estas pruebas se realizan anualmente o cuando haya cambios significativos dentro de la gestión de la continuidad.

Los resultados de estas pruebas quedan documentados y generan los informes pertinentes para mantener informada a la alta dirección. Si no se demuestra el funcionamiento y efectividad de los planes diseñados, se deberán planificar e implementar todas las acciones correctivas necesarias.

5. Versionado

Elaborado por:	Francisco López - CTO
Aprobado por:	• Comité de Seguridad
Fecha de aprobación:	03/08/2026
Clasificación de esta información:	• Información Pública