¿Cuándo implementar un plan de continuidad de tecnología?

Las fallas y eventos tecnológicos siempre han formado parte de la realidad de las organizaciones, por esto es importante contar con una **estrategia de recuperación** de los servicios buscando hacer frente a la continuidad operativa de forma efectiva y rápida, volviendo a la **normalidad en el menor tiempo** posible.

Para esto es importante como mínimo seguir los siguientes pasos:

1. Definir objetivo y alcance.
2. Identificar los roles y responsabilidades.
3. Tener claros los escenarios y posibles eventos de alto impacto.
4. Definir acciones de respuesta frente a cada posible escenario.
5. Definir acciones para recuperar y regresar a la normalidad.
6. Determinar los recursos necesarios para implementar, mantener, probar y activar el plan.
7. Identificar y documentar las dependencias internas y externas.

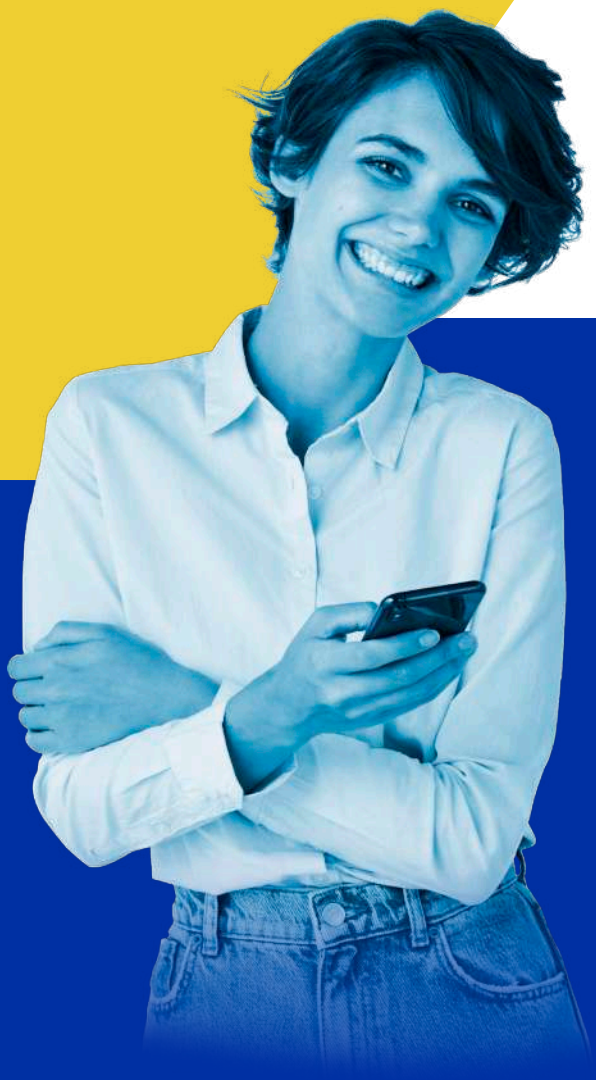
1. Objetivo y alcance

Objetivo

Brindar una respuesta adecuada ante eventos de alto impacto que degraden o interrumpan las operaciones tecnológicas de los servicios ofrecidos por la organización en el menor tiempo posible.

Alcance

Priorizar la atención de los usuarios y el cumplimiento de los compromisos adquiridos garantizando el funcionamiento de la infraestructura tecnológica que soporta los servicios críticos de la organización.



Tener en cuenta que:

La organización es responsable de **identificar** aquellos procesos/servicios **críticos** que deben continuar operando al momento de presentarse una afectación.

Esta identificación se realiza según el pilar fundamental de la organización en cuanto a sus servicios que a su vez son su soporte económico.

2. Roles y responsabilidades

Toda la organización es parte fundamental del plan de continuidad de tecnología, sin embargo, es importante resaltar que hay roles que por sus responsabilidades son relevantes para el buen funcionamiento del plan de continuidad de TI.

Si bien, el equipo de Tecnología es el responsable de garantizar que la infraestructura técnica que soporta los servicios críticos siempre se encuentre disponible, esto no puede hacerlo sin el apoyo y gestión de los equipos de negocio que son quienes conocen desde un rol funcional cada uno de los servicios ofrecidos por la organización.

Por esta razón es de suma importancia identificar personas, cargos y suplentes tanto del equipo de tecnología como del equipo de negocio y proveedores relevantes.

Se debe definir un equipo de crisis que tome las decisiones relevantes al momento de activar el plan de continuidad de tecnología y siga los procedimientos definidos para tal fin.

3. Escenarios y eventos de alto impacto

Es importante que cada organización tenga claro y contemple el **máximo** de escenarios tecnológicos posibles que podrían llegar a presentarse y afectar la operación normal.

Algunos de los escenarios puede ser:

- Falla bases de datos
- Ejecución de cambios sin pruebas previas
- Ataques cibernéticos
- Perdida de la información
- Cambio del proveedor administrador del servicio
- Desastres naturales
- Entre otros...

4. Acciones de respuesta para cada escenario

Es importante que cada organización tenga definido y documentado las acciones que llevará a cabo frente a cada uno de los escenarios y posibles eventos de alto impacto que se puedan presentar.

Al contar con información documentada y detallada, sumado a roles relevantes identificados, será más fácil poder activar las operaciones técnicas y brindar una continuidad en los servicios críticos para la organización.

5. Acciones para regresar a la normalidad

Cuando se tenga identificado y controlado las acciones de respuesta para el escenario presentado, se debe comenzar a detallar aquellas acciones que se deben llevar a cabo para regresar a la operación normal, es decir, para solucionar el evento presentado. Aquí es super importante definir y documentar los roles y responsabilidades que cada persona debe ejecutar, evitando improvisar y conservando siempre llevar a cabo los procedimientos definidos.

6. Determinar los recursos

En este punto, es importante identificar y definir los recursos necesarios para la implementación, mantenimiento actualización pruebas y activación del plan de continuidad de tecnología tanto para el momento en el que deba ser activado como para el regreso a la normalidad de la operación. Se recomienda que dichos recursos hagan parte del presupuesto anual de la organización.

7. Dependencias internas y externas

Identificar aquellos entes o roles relevantes externos e internos de la organización, permitirá no solo conocer los procedimientos acordados y la forma en cómo deben activarse, sino que también se tendrá claro quiénes son los proveedores relevantes (nombres, datos para contacto y responsabilidades) que hacen parte de los equipos de atención y activación del plan de continuidad de tecnología.

¿Contingencia o Continuidad?

Contingencia

Es aquel plan que se ejecuta de manera inmediata al momento de presentarse una falla en uno de los sistemas o plataforma de tecnología que impidan el funcionamiento de la operación normal de los servicios ofrecidos por la organización.

Se caracteriza por:

- Apoyar y soportar durante un tiempo corto.
- Activarse cuando es una falla puntual o focalizada.
- Implicar una operación manual (no en todos los casos).
- Normalmente es responsabilidad del equipo de negocio.

Continuidad

Es aquel plan que se activa en los tiempos definidos y asumidos por la organización.

Busca brindar operatividad tecnológica para aquellos servicios declarados como críticos.

Se caracteriza por:

- Responder a eventos de alto impacto y de duración prolongada o desconocida.
- Activarse de acuerdo a la autorización y procedimientos definidos por los equipos que hacen parte del plan de continuidad de tecnología.
- Es responsabilidad del equipo de tecnología pero debe ser operado y probado por el equipo de negocio.

Al determinarse una activación del plan de continuidad de tecnología...

Evento de falla

Plan activado

Regreso a operación normal

Activación de contingencia

Activación de contingencia

Activación de plan de continuidad de tecnología

Operación en plan de continuidad

Tener en cuenta que:

Al presentarse un evento de alto impacto que amerite la activación del plan de continuidad de tecnología, todos los servicios de la organización deberán activar sus contingencias.

Conceptos claves

***BIA** - Análisis de Impacto del negocio*

Permite identificar los procesos o servicios críticos de una organización en un nivel de negocio.

***AIA** - Análisis de Impacto de las aplicaciones*

Permite identificar las aplicaciones críticos que soportan los servicios o procesos críticos de una organización.

***PRT** - Plan de Recuperación de Tecnología*

Plan para que desde la Tecnología responda, recupere y restaure las operaciones críticas ante un evento que interrumpa los servicios.

***RTO** - Tiempo de Recuperación Objetivo*

Hace referencia al periodo de tiempo dentro del cual las operaciones y servicios deben ser recuperados, antes de ocasionar un impacto mayor

***RPO** - Punto de Recuperación Objetivo*

Información que la organización está dispuesta a “perder” desde la ocurrencia de una falla, hasta la realización del último backup valido.

¿Qué deberías contemplar?

Algunas herramientas o estrategias tecnológicas deberías tener en cuenta e implementar son:

- Respaldo de toda tu información (incluyendo pruebas de restauración).
- Pruebas de restauración.
- Alta disponibilidad de tus aplicaciones.
- Planes de contingencia y continuidad de tus proveedores.
- Identificación, gestión y mitigación de riesgos.
- Ejecución de auditorías internas o externas.

Formatos básicos

A continuación encontrarás algunos formatos básicos que te servirán como punto de partida para la documentación de la información relevante al momento de implementar, mantener, activar y probar tu plan de continuidad de tecnología:

- **BIA_AIA.**
- **Análisis de impacto en las aplicaciones.**
- **Formato Técnico Aplicación Crítica.**
- **Plan de Recuperación de Tecnología (PRT).**
- **Matriz de Riesgos.**
- **Documentación Contingencia.**

Responde las preguntas que encontrarás en este archivo y conoce qué tiene y qué necesita tu organización para implementar un plan de continuidad de tecnología.

- **Checklist Plan de Continuidad de Tecnología.**

sura

Empres SURA, **un aliado para avanzar.**