Disaster Recovery Plan,

todo lo que necesitas
para implementarlo

NOVIS

En cualquier momento, las empresas pueden enfrentarse a eventos disruptivos que ponen en riesgo la continuidad operativa de sus sistemas SAP. Estos sucesos afectan también a sus operaciones y pueden tener diversos orígenes.

Los imprevistos vienen de dentro o fuera de la organización y comprenden una gran variedad como ataques cibernéticos, errores humanos, fallas eléctricas o desastres naturales.

Esto implica que la operación de las empresas se ve afectada ya sean minutos, horas, incluso días o semanas. Entre más tiempo pase, mayor será la afectación, lo que se traduce en pérdidas financieras y pérdida de información valiosa, que no logra recuperarse.

Es por eso que un Disaster Recovery Plan (DRP) o plan de recuperación ante desastres es tan importante para la continuidad de las organizaciones.

¿Cuánto pierden las empresas?

El costo para las compañías es variable y depende de diferentes factores a considerar:

El tamaño de la empresa.

Las áreas que la inactividad ha afectado.

El número de empleados inactivos.

Si se han perdido transacciones y cuántas.

Si ha tenido que parar la producción.

El tiempo de inactividad.

El tiempo que toma volver a la normalidad.

Si se incumplió con alguna entrega o plazo.

Si hay alguna demanda por incumplimiento.

A nivel mundial, el costo promedio por hora de tener los servidores inactivos le cuesta a la mayoría de las empresas arriba de 300,000 dólares, con base en una encuesta a compañías de todos los tamaños:

7% entre 201,000 y 300,000 dólares.

25% entre 301,000 y 400,000 dólares.

12% entre 401,000 y 500,000 dólares.

11% entre 501,000 y 1 millón de dólares.

13% entre 1 millón y 2 millones de dólares.

10% entre 2 millones y 5 millones de dólares.

17% más de 5 millones de dólares.

Fuente: *Statista, Average cost per hour of enterprise server downtime worldwide 2020.*

¿Qué es un DRP?

El Disaster Recovery Plan forma parte del Plan de Continuidad del Negocio (BCP, por sus siglas en inglés) y son los protocolos a seguir en caso de que se presente un evento disruptivo.

Estos planes abarcan desde identificar los riesgos, la estrategia para hacerles frente, el propio sistema SAP, las personas que estarán a cargo de la contingencia, hasta la capacitación y entrenamiento que recibirán los colaboradores para hacerle frente.

Todo el proceso debe estar documentado, probado y ajustado para evitar fallas en el momento crítico.

7 fases que deben seguirse

Para crear un plan se consideran algunos elementos clave que es necesario incluir:

1. IDENTIFICA LOS RIESGOS

¿Cuáles son los incidentes a los que se puede ver expuesta tu compañía? Considera elementos internos, externos, desastres naturales, interrupciones del sistema o fallas de la infraestructura de TI. Algunos de los incidentes más comunes son:

22%
fallas en el software, por ejemplo, aplicaciones, drivers o firmware.

20%
fallas en el hardware.

17%
brechas de seguridad, como virus o ransomware.

15%
errores humanos, como accidentes.

15%
cortes de luz.

6%
fallas en la red.

2%
fallas en la nube o SaaS.

Fuente: *451 Research, Voice of The Enterprise (VotE): Storage, Data Management & Disaster Recovery 2020.*

2. HAZ UN INVENTARIO

Identifica cuáles son las herramientas, sistemas y procesos claves de tu organización. Haz una lista detallada y ordénala de mayor a menor, para establecer cuáles son imprescindibles en el funcionamiento de la empresa.

Los que se encuentren entre los primeros lugares son en los que deberás enfocarte y destinar mayores recursos.

Considera que los datos son un activo importante para cualquier compañía. Éstos tienen que formar parte del inventario y también estar jerarquizados. También debes incluir a tu sistema SAP, que es el que se encarga de la gestión de los recursos empresariales.

3. ESTIMA EL IMPACTO EN LOS NEGOCIOS

Una vez que conozcas cuáles son los elementos más importantes para la operación de la organización, también podrás saber cuánto te costará no contar con ellos.

Por ejemplo, un corte de luz por minutos o incluso horas puede hacer fallar algunos de los sistemas, incluido el ERP SAP, detener la producción o interrumpir las transacciones.

La pérdida de información en el caso de un ciberataque o ransomware, tiene algunos otros impactos negativos:

Pérdida de la productividad de los empleados, 49%.

Daño en la reputación de la marca, 35%.

Pérdida de ingresos, por oportunidades comerciales no concretadas, 28%.

Pérdida de la lealtad del cliente, 19%.

Sanciones por falta de cumplimientos, 23%.

Fuente: *451 Research, Voice of The Enterprise (VotE): Storage, Data Management & Disaster Recovery 2020.*

4. PERSONAL DE RESPUESTA

Tu equipo de trabajo será la clave para responder a una contingencia de forma efectiva y ágil. Así que también debes saber con quién cuentas o quién responderá ante la emergencia y capacitar a ese personal.

Por ejemplo, si hay una interrupción en la red, establece qué persona deberá estar a cargo de su restablecimiento.

El personal de respuesta a cargo deberá realizar simulacros de forma periódica, para comprobar que el DRP funciona de forma efectiva, que cuentan con los accesos pertinentes y que se da una resolución al problema en tiempo y forma.

5. ESTABLECE LOS OBJETIVOS Y TIEMPOS DE RESPUESTA

Existen diferentes momentos clave que debes tener siempre en mente y que son importantes ante un evento de este tipo:

Recovery Point Objective (RPO). El objetivo de punto de recuperación es la cantidad máxima de datos que se puede perder durante la interrupción, sin afectar la operación de la empresa.

En muchos de estos eventos, perder información es imposible de evitar. Generalmente las organizaciones establecen tiempos de respaldo de la información considerando el RPO.

Ésta es una medida de tiempo, por ejemplo, puede ser en horas o incluso en minutos. Hay empresas a las que perder horas de información puede resultarles desastroso.

Es por ello que se realizan respaldos periódicos de las bases de datos y de la información más importante. Algo que tu sistema SAP realiza de forma automatizada.

Recovery Time Objective (RTO). Es el tiempo máximo que los sistemas de la organización pueden estar fuera de línea. Aunque exista alguna aplicación o software que pueda permanecer más tiempo, muchos de los sistemas son indispensables para la operación, por ejemplo, SAP.

En ese caso, se mide el tiempo que tomará que éstos vuelvan a estar operativos.

El tiempo real de recuperación. Identificar cuál es el tiempo real, desde que ocurre la interrupción, hasta que se restablecen todos los sistemas, los datos y vuelven a funcionar con normalidad.

Esta métrica puede ser mayor al RTO, puesto que el sistema ya puede estar activo, sin embargo deben comprobarse las bases de datos o la integridad de la información.

6. PLANTEA LA ESTRATEGIA

Una vez que ya tienes todos los riesgos identificados, las métricas, las personas involucradas y las prioridades de la empresa, es momento de hacer tu estrategia.

El DRP debe incluir todos los planes preventivos para minimizar las pérdidas y los gastos, como las réplicas o copias de seguridad y encriptación de las bases de datos, por si se presenta un ciberataque.

Tiempo y personas de primera respuesta del equipo de TI para resolver caídas del sistema o contingencias. Tu sistema SAP también forma parte de la ecuación.

Una de las principales estrategias es la migración de ciertas aplicaciones e información a la nube. Así, si hay alguna interrupción local, como un desastre natural, la información puede recuperarse desde la nube.

7. DOCUMENTA TODO, HAZ PRUEBAS Y AJUSTA EL PLAN

El DRP tiene que estar por escrito y contener todas las estrategias planteadas. Además, incluirá los teléfonos y contactos de las personas involucradas y las que deberán tomar decisiones.

Es importante realizar pruebas de cómo funcionaría el DRP ante una eventualidad y qué tan efectivo es. Esto tendría que ser antes de que se presente una emergencia real.

Después de las pruebas se harán todos los ajustes necesarios y se documentará cualquier cambio que se haga.

Checklist al hacer tu DRP

A continuación te dejamos un lista de todos los elementos que debe incluir tu DRP:

- [ ] Riesgos internos. Errores humanos o posibles accidentes
- [ ] Riesgos externos. Desastres naturales, ciberataques, etc
- [ ] Identifica las operaciones prioritarias.
- [ ] Haz una lista de los sistemas, equipo, software y herramientas indispensables.
- [ ] Registra el personal a cargo de las diferentes contingencias
- [ ] Identifica los datos imprescindibles para la operación.
- [ ] Establece tus métricas: RPO, RTO y tiempo real de recuperación.
- [ ] Evalúa las prioridades identificando las pérdidas financieras que podrían llegar a ocurrir.
- [ ] Plantea las estrategias a seguir para los diferentes escenarios.
- [ ] Haz pruebas.
- [ ] Ajusta el plan.
- [ ] Realiza la documentación adecuada.
- [ ] Mantente preparado.

Como podrás ver el DRP es indispensable para mantener en funcionamiento las principales operaciones de tu empresa y evitar pérdidas que puedan amenazar la continuidad del negocio.

Considera a Novis como tu socio estratégico para la implementación de planes que permitan el óptimo funcionamiento de tu sistema SAP.

Déjanos ayudarte, nuestro equipo puede brindarte las alternativas que requieres generar en tu empresa, para contar con un plan para la recuperación de datos que te permita restablecer tus servicios lo antes posible.

Fuentes:

- *Statista, Average cost per hour of enterprise server downtime worldwide.*
- *451 Research, Voice of The Enterprise (VotE): Storage, Data Management & Disaster Recovery 2020.*
- *OpenText, DRaaS ushers in changes to data protection strategy.*
- *IBM, What is a disaster recovery (DR) plan?*
- *Federal Emergency Management Agency (FEMA), IT Disaster Recovery Plan.*
- *Federal Emergency Management Agency (FEMA), Business Impact Analysis.*

NOVIS