TECNOLOGÍAS DE INFORMACIÓN Y CIBERSEGURIDAD

Plan de Recuperación de Desastres (DRP)

Seguridad de la Información

Generalidades

Un plan de recuperación ante desastres permite garantizar la respuesta a un incidente o emergencia que afecte a los sistemas tecnológicos.

Es un documento clave para cualquier empresa que busque un mínimo estándar de ciberseguridad, pero sobre todo para aquellas con base tecnológica, donde la disponibilidad de los sistemas es un asunto crítico que no puede ignorarse.

Crear un plan de recuperación ante desastres se trata principalmente de elaborar estrategias y procedimientos.

DRP

Un Disaster Recovery Plan (DRP) es un documento donde las empresas describen los procedimientos a seguir para reanudar el área de TI en caso de una interrupción (como caída de servidores cloud, base de datos, falla de infraestructura o software, catástrofes).

El plan de recuperación ante desastres forma parte del plan de continuidad del negocio (BCP) que contiene procedimientos para todas las áreas de una empresa.

nacap

¿Para qué sirve el plan de recuperación ante desastres (DRP)?

Las estrategias y acciones definidas en el plan de recuperación ante desastres le permiten a una empresa reanudar sus actividades en el menor tiempo posible y con la menor pérdida de información.

Este es, de hecho, uno de los principales motivos por el que los directivos y auditores lo solicitan a menudo, ya que es una forma de evidenciar cómo se manejan los problemas de continuidad o disponibilidad de los sistemas críticos.

nacap

Beneficios de un DRP

Beneficios
Atención continua al cliente y proveedores: reduce el tiempo de inactividad al máximo para mantener la buena relación comercial con clientes y proveedores.
Minimiza las pérdidas por inactividad: organiza y capacita a los equipos para que actúen rápidamente y restablezcan los sistemas críticos.
Minimiza el estrés de la toma de decisiones: en una situación extrema es primordial que todos sepan cómo actuar, desde el personal de menor rango hasta el de mayor rango.
Asegura el acceso a la información: el respaldo permite proteger los datos ante cualquier evento negativo.

Pasos para crear un plan de recuperación ante desastres

Definición de objetivo y alcance

Objetivo	se debe indicar lo que la organización quiere lograr con este plan. Un ejemplo puede ser: garantizar la respuesta a un desastre que afecte a los sistemas de información y minimizar su efecto en el funcionamiento del negocio.
Alcance	Se debe definir los componentes tecnológicos que estarán involucrados en el plan, es decir todos aquellos que sean críticos para los servicios o productos del negocio.

Crear estrategias de recuperación

Al igual que en el plan de continuidad del negocio (BCP), se debe crear alternativas que aseguren la disponibilidad de los recursos tecnológicos ante cualquier interrupción.

Lo recomendable es elaborar varias estrategias para distintos escenarios de incidentes. Por ejemplo, algunos escenarios de incidentes comunes son:

- Indisponibilidad del sistema operativo
- Indisponibilidad del sistema de procesamiento de datos
- Caída de la base de datos
- Falla en el software
- Indisponibilidad del servicio de proveedor nube

Ejemplo estrategia recuperación

Escenario de incidente	Estrategia de recuperación
Caida de la base de datos	A.- Backup de información
	B.- Infraestructura alternativa o sitio de contingencia
	C.- Cambio de ruteo de servidores desde una región a otra

nacap

Crear los procedimientos para las estrategias

Una vez que se tiene claridad con las estrategias hay que describir el paso a paso a seguir para que el equipo encargado logre restaurar la tecnología según el escenario de incidente.

nacap

Escenario de Incidente	Estrategias de recuperación	Procedimiento
Caída Base de datos		Contactar al equipo de desarrollo y de operaciones.
	A. Backup de información.	Realizar respaldo extraordinario de la base de datos.
	B. Infraestructura alternativa o sitio de contingencia.	Realizar snapshot de los servidores de base de datos.
	C. Cambio de ruteo de servidores desde una región a otra.	Restaurar un ambiente de QA de la base de datos. En dicho ambiente revisar que la base de datos tenga espacio disponible en disco .
		Si la base de datos no puede ser corregida, se debe restaurar la última versión respaldada
		Se notifica al responsable operacional y al usuario final.

Caso 1: DRP Sistema Ecommerce

Escenario: Falla del servidor principal Sergioexpress

Objetivo: Restaurar el servicio de ventas online en menos de 1 hora (RTO) y sin perder más de 15 minutos de transacciones (RPO).
1.- Detectar falla con monitor automático.
2.- Notificar al equipo de TI y responsables de e-commerce.
3.-Activar el servidor en la nube de respaldo (failover automático en AWS).
4.- Restaurar última base de datos desde backup incremental (cada 15 min).
5.- Validar funcionamiento del sistema y confirmar pedidos pendientes.
6.- Informar al cliente si hubo interrupción perceptible.
7.- Registrar incidente y revisar logs.

Caso 2: DRP empresa financiera

Escenario: Ciberataque con ransomware

Objetivo: Recuperar sistemas críticos en 4 horas. Ninguna pérdida de datos permitida (RPO = 0).
1.- Detectar actividad sospechosa
2.- Aislar inmediatamente el servidor afectado.
3.- Notificar a Seguridad Informática y Dirección.
4.- Activar entorno alternativo en sitio de contingencia (cold site).
5.- Restaurar backup inmutable (almacenado offline).
6.- Realizar escaneo de seguridad completo antes de reactivar el sistema.
7.- Cambiar credenciales globales.
8.- Notificar a entes reguladores si aplica (CMF)
9.- Investigar causa raíz y aplicar mejoras.

Caso 3: DRP Site servidores físicos

Escenario: Incendio en la oficina central

Objetivo: Reanudar operaciones administrativas en 24 horas.
1.-Evacuar personal y activar protocolo de emergencia.
2.-Validar daños físicos y acceso al centro de datos.
3.- Activar sitio alterno (oficina secundaria con puestos habilitados).
4.- Restaurar datos desde backups externos (almacenados en la nube).
5.- Redirigir comunicaciones (teléfonos, correos).
6.- Establecer comunicación con empleados y clientes.
7.- Mantener operaciones críticas funcionando hasta normalización.

Definir las métricas RPO y RTO

El Recovery Point Objective (RPO) y Recovery Time Objective (RTO) son dos métricas de tiempo muy importantes para el plan de recuperación ante desastres (DRP) ya que ayudan a crear estrategias viables para el negocio.

Métricas	
Recovery Point Objective (RPO)	es el tiempo máximo aceptable que puede transcurrir entre el momento en que se realizó la última copia de seguridad de los datos y un incidente.
RTO (Recovery Time Objective)	es el tiempo que un negocio necesita para recuperar sus sistemas después de la inactividad producida por un incidente.

Definir las métricas RPO y RTO

Si bien no existe una solución única para definirlos ya que depende de las necesidades de cada empresa, en esta presentación se puede comentar cuáles son los valores más comunes definidos por las startups, pymes y empresas de tecnología.

	Ejemplo
RPO	Para que este valor sea ínfimo se debe realizar gran cantidad de backups, y eso puede implicar mayor costo con el proveedor. Por lo general, las empresas pequeñas suelen establecer que el tiempo máximo de pérdida de datos sea igual a su SLA (Acuerdo de Nivel de servicio), por ejemplo, 24 hs.
RTO	Es necesario conocer el tiempo de restauración que se tenga con el proveedor de nube y cuánto demora en levantar los servicios caídos. Habitualmente, suele darse entre 4 y 8 horas, aunque depende de la complejidad de lo instalado.

¿Cómo se calcula el RPO?

El RPO no se calcula con una fórmula matemática directa , sino que se define en función de:

- Frecuencia de respaldos (backups)
- Tolerancia de la empresa a la pérdida de datos
- Tipo de datos (por ejemplo , datos financieros pueden requerir un RPO de minutos(por ejemplo, los datos financieros pueden requerir un RPO de minutos)
- Capacidades técnicas y presupuesto .

¿Cómo se calcula el RPO?

Supongamos:

- Se hacen respaldos automáticos cada 6 horas.
- Se considera aceptable perder hasta 6 horas de información.
- En ese caso, el RPO sería de 6 horas .

¿Cómo se calcula el RTO?

El RTO se determina con base en análisis del negocio . Estos son los pasos claves para establecer o calcular un RTO razonable :

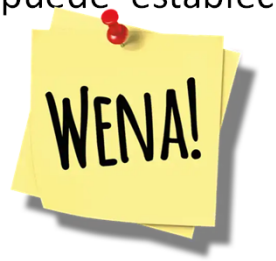
Pasos para definir RTO

Paso	Explicación
Identificar el proceso o sistema crítico	Ej . : sistema de ventas en línea , base de datos deEj.: sistema de ventas en línea, base de datos de clientes, servidor de correo, etc.
Evalúa el impacto del tiempo de inactividad	Preguntas clave:¿Qué pasa si el sistema está inactivo durante 1 hora? ¿Y 4? ¿Y 12?¿Hay pérdidas económicas, legales, de reputación?
Consulta con usuarios y áreas afectadas	Finanzas, operaciones, RRHH, etc.
Determina el tiempo máximo aceptable de inactividad	Por ejemplo: Un sistema de sueldos puede tener un RTO de 24 horas. Un sistema de ventas en comercio electrónico puede tener un RTO de 15 minutos.
Valida con capacidades técnicas y presupuesto	¿Tienes los recursos para cumplir ese RTO? Si no, hay que ajustar o invertir.

Nota

Hay Tener en cuenta que las estrategias y los procedimientos deben estar pensadas para cumplir con estas dos métricas.

Por ejemplo, si se definió que la métrica RPO es de 8 horas, entonces no se puede establecer backups cada 24 hrs.



Probar, Revisar y mantener

El plan de recuperación debe actualizarse anualmente (o cuando ocurran cambios significativos en los recursos tecnológicos).

Por ello, es necesario acordar estas actualizaciones con el equipo de trabajo en materias de actualización del plan DRP.

Por otro lado, también debe ser objeto de prueba cada año para verificar su efectividad. Las Pruebas al DRP son obligatorias ya que son evidencia del mantenimiento y mejora continua.

Sus resultados se detallan en un Informe de Resultado de Pruebas que debe ser revisado y aprobado por el coordinador y el gerente del equipo de recuperación.