CONSEJO DE LA JUDICATURA
PODER JUDICIAL DEL ESTADO DE PUEBLA

Plan de Recuperación de Desastres para el Poder Judicial del Estado de Puebla

Dirección de Tecnologías de la Información y Comunicaciones

Diciembre 2024

Contenido

Un plan de recuperación de desastres (DRP, por sus siglas en inglés) para un centro de cómputo y datos es esencial para garantizar la continuidad del negocio y minimizar el tiempo de inactividad en caso de un desastre. A continuación, se presenta un plan detallado que cubre los aspectos clave para proteger y recuperar servidores, aplicaciones y equipos de telecomunicaciones.

Plan de Recuperación de Desastres para un Centro de Cómputo y Datos

1. Objetivos del Plan

- Minimizar el tiempo de inactividad y la pérdida de datos.
- Restaurar operaciones críticas en el menor tiempo posible.
- Proteger la infraestructura física y lógica del centro de cómputo.
- Cumplir con la seguridad y continuidad del servicio.

---

2. Identificación de Riesgos

Realizar un análisis de riesgos para identificar posibles amenazas:

- Desastres naturales (terremotos, inundaciones, incendios, etc.).
- Fallos de hardware (servidores, almacenamiento, equipos de red).
- Ciberataques (ransomware, DDoS, intrusiones).
- Cortes de energía eléctrica.
- Errores humanos (configuraciones incorrectas, eliminación accidental de datos).

---

3. Equipo de Respuesta a Desastres

Designar un equipo multidisciplinario con responsabilidades claras:

- **Coordinador del DRP**: Supervisa la ejecución del plan.
- **Equipo de TI**: Responsable de la recuperación de servidores, aplicaciones y datos.
- **Equipo de Telecomunicaciones**: Restablece la conectividad y servicios de red.
- **Equipo de Seguridad**: Garantiza la integridad física y lógica del centro de cómputo.
- **Comunicaciones**: Informa a los mandos superiores y usuarios sobre el estado del incidente.

4. Inventario de Activos Críticos

Identificar y documentar los activos críticos:

- Servidores físicos y virtuales.
- Aplicaciones institucionales (ERP, CRM, bases de datos, etc.).
- Servicios de red (FTP, mail, DNS, DHCP)
- Equipos de telecomunicaciones (routers, switches, firewalls).
- Almacenamiento de datos (SAN, NAS, backups).
- Infraestructura de soporte (UPS, generadores, sistemas de enfriamiento).

5. Estrategias de Prevención y Mitigación

Implementar medidas para reducir el impacto de desastres:

- **Infraestructura física**:
  - Instalación de sistemas de detección y extinción de incendios.
  - Uso de sistemas de alimentación ininterrumpida (UPS) y generadores de respaldo.
  - Protección contra inundaciones y control de temperatura/humedad.
- **Seguridad lógica**:
  - Firewalls, sistemas de detección de intrusiones (IDS) y prevención (IPS).
  - Actualizaciones periódicas de software y parches de seguridad.
  - Segmentación de redes para limitar el impacto de ataques.
- **Copia de seguridad y redundancia**:
  - Implementar respaldos automáticos y periódicos (diarios/semanales).
  - Almacenar copias de seguridad en ubicaciones externas o en la nube.
  - Configurar replicación de datos en tiempo real a un sitio secundario.
- **Servicios**
  - Identificación y documentación de portales y sistemas.
  - Creación de ambientes de desarrollo, pruebas y productivos para los servicios identificados.

6. Procedimientos de Respuesta ante Desastres

Definir pasos específicos para diferentes escenarios:

1. **Corte de energía**:
   - Activar UPS y generadores de respaldo.
   - Apagar equipos no críticos para conservar energía.

- Monitorear el tiempo restante de la UPS.

2. **Fallo de hardware**:
   - Reemplazar componentes defectuosos con piezas de repuesto.
   - Activar servidores o servicios de telecomunicaciones redundantes.
3. **Ciberataque**:
   - Aislar sistemas afectados para evitar la propagación.
   - Restaurar sistemas desde respaldos limpios.
   - Investigar el origen del ataque y reforzar medidas de seguridad.
4. **Desastre natural**:
   - Evacuar al personal y asegurar la infraestructura.
   - Activar el sitio de recuperación secundario (si está disponible).
   - Evaluar daños y coordinar con proveedores para reparaciones.
5. **Fallo de Servicios**
   - Identificar el servicio o componente que está fallando.
   - Revisar el log del servicio para identificar el problema.
   - Corregir el problema en el ambiente de desarrollo
   - Realizar pruebas unitarias en el ambiente de pruebas
   - Aplicar las correcciones en el ambiente productivo

---

7. Sitio de Recuperación

Establecer un sitio de recuperación para operaciones críticas:

- **Sitio caliente**: Réplica completa del centro de cómputo, listo para operar en minutos.
- **Sitio tibio**: Infraestructura parcialmente configurada, lista en horas.
- **Sitio frío**: Espacio físico con infraestructura básica, requiere configuración.

---

8. Pruebas y Simulacros

Realizar pruebas periódicas para validar la efectividad del plan:

- Simulacros de corte de energía.
- Pruebas de restauración de respaldos.
- Simulaciones de ciberataques.
- Ejercicios de evacuación y respuesta ante desastres naturales.
- Pruebas unitarias y funcionales en el ambiente de pruebas

---

9. Documentación y Actualización

- Mantener documentación actualizada del plan, incluyendo:

  - Contactos de emergencia.
  - Diagramas de red y configuración de equipos.
  - Procedimientos detallados para cada escenario.
- Revisar y actualizar el plan periódicamente o después de cambios significativos en la infraestructura.

---

10. Comunicación y Capacitación

- Capacitar al personal en procedimientos de respuesta ante desastres.
- Establecer canales de comunicación claros para informar sobre incidentes.
- Proporcionar guías y manuales de referencia rápida.

---

11. Recuperación Post-Desastre

- Evaluar el impacto del desastre y documentar lecciones aprendidas.
- Restaurar operaciones completas en el centro de cómputo principal.
- Realizar una auditoría de seguridad para garantizar que no quedan vulnerabilidades.
- Replicar el ambiente productivo en el ambiente de pruebas y realizar pruebas unitarias y funcionales.

Este plan debe adaptarse a las necesidades específicas del centro de cómputo y revisarse periódicamente para asegurar su efectividad. La preparación y la prevención son clave para minimizar el impacto de cualquier desastre.

ELABORÓ	AUTORIZÓ
JAIME SANTIAGO HÉRNANDEZ SUBDIRECTOR DE INFRAESTRUCTURA TECNOLÓGICA	**ARLETTE HERNÁNDEZ PELÁEZ** DIRECTORA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
ALEJANDRO RAMÍREZ CRUZ JEFE DE DEPARTAMENTO DE INGENIERÍA DE SOFTWARE	**MARÍA GUADALUPE FLORES SANTOS** SECRETARIA DE ADMINISTRACIÓN DEL CONSEJO DE LA JUDICATURA