Plan de Recuperación ante Desastres (DRP)

TechSys Solutions S.L. reconoce la importancia crítica de restaurar sus operaciones y sistemas de información de manera oportuna y eficaz tras la ocurrencia de un desastre o interrupción significativa. Esta sección define los principios y el marco para el Plan de Recuperación ante Desastres (DRP) de la Empresa.

Objetivos del DRP:

- Minimizar el **impacto** financiero, operativo y reputacional de un desastre.
- **Restaurar** los sistemas y servicios críticos identificados por la empresa dentro de los plazos establecidos (RTO).
- **Asegurar** la recuperación de los datos hasta un punto aceptable de pérdida (RPO).
- **Proteger** la vida y seguridad del personal durante y después de un desastre.

Componentes clave del DRP:

- **Identificación** de sistemas y procesos críticos (basado en el Análisis de Impacto en el Negocio / BIA, se identificarán y priorizarán los sistemas, aplicaciones, datos y procesos de negocio esenciales para la continuidad de las operaciones).

  Los sistemas y procesos críticos identificados:
  - Servidores físicos y virtuales.
  - Sistemas de correo electrónico y VPN.
  - Bases de datos críticas (clientes, facturación, proyectos).
  - Sistemas de desarrollo y almacenamiento en la nube.
  - Equipos de usuarios clave.
  - Comunicaciones y acceso remoto.

- Definición de **objetivos** de recuperación:

  - Recovery Time Objective **(RTO)** - tiempo máximo tolerable para que un sistema o proceso específico vuelva a estar operativo tras una interrupción. Estos RTOs serán definidos para cada servicio crítico.

  - Recovery Point Objective **(RPO)** - la cantidad máxima de pérdida de datos tolerable, medida en tiempo, desde el último respaldo válido hasta el momento del incidente.

    Restauración en orden definido por impacto y dependencia:
    - Comunicaciones (VPN, correo).
    - Sistemas de clientes y soporte.
    - Bases de datos operativas.

        - Plataformas de desarrollo y trabajo interno.

- **Estrategias** de recuperación:
    - **Copias** de seguridad y restauración (implementación de un sistema robusto de copias de seguridad para todos los datos críticos y sistemas, con pruebas periódicas de restauración. Las copias de seguridad se almacenarán en ubicaciones seguras y geográficamente distintas).
        - Backups diarios automatizados (en sede y en la nube).
        - Retención de copias por periodos definidos (por ejemplo, 5 días completos).
        - Pruebas regulares de recuperación para verificar integridad.
    - Infraestructura **redundante** (utilización de sistemas redundantes, como clústeres de servidores, RAID, para componentes críticos y, si es económicamente viable y necesario, un sitio de recuperación alternativo, como hot site, warm site o cold site).
        - Posibilidad de operar desde otras sedes o en modalidad 100 % remota.
        - Accesos habilitados vía VPN con MFA desde ubicaciones seguras.
    - Planes **específicos** por escenario (desarrollo de procedimientos detallados para diferentes tipos de desastres, como fallo de hardware crítico, ciberataque mayor, desastre natural que afecte a una sede).

- **Equipo** de recuperación ante desastres - designación de un equipo con roles y responsabilidades claramente definidos para coordinar y ejecutar el DRP.

  El equipo está integrado por:
    - **CEO**;
    - Responsable de **IT**;
    - Responsable de **operaciones**;
    - Responsable de **comunicaciones**.

  Roles y responsabilidades de cada uno:

    - **CEO** - liderar el equipo de gestión de crisis y tomar decisiones críticas.
    - **IT** - coordinar la solución de problemas técnicos y restaurar el servicio.
    - **Operaciones** - asegurarse de los recursos necesarios y coordinar la respuesta operativa. Soporte escalado con proveedores externos cuando sea necesario.

- **Comunicaciones** - manejar la comunicación con los medios y los grupos de interés clave.

- Procedimientos de **comunicación** - establecimiento de canales y protocolos de comunicación interna y externa para gestionar la información durante un desastre y el proceso de recuperación. Debe establecer los mensajes clave y los responsables de la comunicación con los grupos de interés.

  Mensajes clave: reconocer el problema, explicar la situación y la solución, y ofrecer disculpas y una compensación, si es necesario.

  Canales de comunicación: sitio web, redes sociales, correo electrónico, comunicados de prensa.

  Responsables de la comunicación: comunicaciones y CEO.

- **Documentación** - el plan de recuperación ante desastres detallado, incluyendo todos los procedimientos, contactos, inventarios y estrategias, se documentará formalmente y se mantendrá actualizado. Debe estar disponible fuera del entorno afectado.

Mantenimiento y pruebas del DRP:

- El DRP será revisado y actualizado al menos anualmente, o siempre que ocurran cambios significativos en la infraestructura, procesos de negocio o el entorno de amenazas.

- Se realizarán pruebas periódicas del DRP, incluyendo simulacros de diferentes escenarios (fallo de infraestructura, ciberataque), para verificar su efectividad y la preparación del personal. Los resultados de estas pruebas se utilizarán para identificar áreas de mejora y actualizar el plan.

Herramientas de soporte:

- Se utilizarán herramientas como SIEM (Sistemas de Información y Gestión de Eventos de Seguridad) para la monitorización y detección temprana de incidentes que puedan escalar a un desastre.