Plan de recuperación ante desastres

Esta parte del documento es la descripción del plan de recuperación ante desastres para poder garantizar la operatividad del CPD ante un incidente que se pueda producir que ponga en peligro la actividad del CPD.

1. Copias de seguridad

1.1. Tipos de copias

- **Copias de seguridad incrementales**: se realizarán diariamente.
- **Copias de seguridad diferenciales:** se realizarán de manera semanal.
- **Copias de seguridad completas:** se hacen de manera mensual.

1.2. Almacenamiento seguro

- Almacenamiento local: Se hará uso de los sistemas RAID y NAS.
- Almacenamiento externo: Se hace uso de un servidor en una ubicación alternativa.
- Almacenamiento en la nube: Se utilizan soluciones cifradas de almacenamiento remoto.
- Cifrado de datos: Se implementa el sistema AES-256 para todos los datos.

2. Restauración de datos

2.1. Pasos para la restauración

1) Identificación: Determinar la causa del fallo del sistema
2) Evaluación: Medir el alcance del grado de afectación en los sistemas y datos.
3) Restauración inicial: Recuperar los servidores principales.
4) Restauración de bases de datos: Implementar las copias de seguridad recientes para recuperar los datos.
5) Verificación y pruebas: Evaluar la integridad y la funcionalidad de los sistemas reparados y no afectados.

2.2. Procedimientos de recuperación

- **Recuperación con snapshots:** Utilizar las imágenes almacenadas en los entornos de almacenamiento redundantes implementados anteriormente.
- **Restauración desde servidores alternativos:** Activar los entornos de respaldo que se han puesto en servidores remotos.

3. Mecanismos redundantes

3.1. Redundancia en el almacenamiento

- **RAID:** Garantizar la recuperación y la disponibilidad de los datos.
  En nuestro caso hemos decidido decantarnos por el RAID 5, ya que su combinación de rendimiento, redundancia y capacidad de almacenamiento es la que más se adecua al caso de este CPD.
- **Almacenamiento SATA:** Usar discos de alta velocidad para poder garantizar la eficiencia operativa del sistema.

3.2. Infraestructura alternativa

- **Servidores de respaldo:** Implementar un servidor en un sitio alternativo al del CPD.
- **Balanceo de carga:** Distribuir el tráfico de manera equitativa para evitar cualquier tipo de saturación.
- **Energía redundante:** Utilizar UPS y añadir generadores de emergencia.

4. Protocolos ante desastres

4.1. Plan de acción

- **Roles:** Definir unos roles y unas responsabilidades claras para todo el personal de informática y de administración.
- **Protocolos de comunicación:** Coordinar los equipos internos y externos.
- **Escalamiento:** Definir los niveles de respuesta y los tiempos de respuesta.

4.2. Pruebas regulares del plan

- **Pruebas trimestrales:** Simular una recuperación de sistemas críticos.
- **Evaluación de fallos:** Analizar las posibles vulnerabilidades y mejorar las mismas.
- **Actualizar el plan:** Revisar y ajustar el plan según aparezcan nuevas amenazas y necesidades operativas.