Implementación de un Sistema de Backup y Recuperación ante Desastres en Codearts Solutions

🔹 Fase 1: Evaluación de riesgos y planificación del sistema de backup

```
# Crear inventario de datos críticos (modo manual o script)

find /home /var/www /etc -type f -printf "%T@ %p\n" | sort -n | tail -n 100 > top_critical_files.txt


# Definir y registrar RTO y RPO (documentación técnica interna)

# Ejemplo de RTO: 1h | RPO: 15 min → anotar en "DRP_document.md"
```

🔹 Fase 2: Configuración del sistema de backup y almacenamiento seguro

```
# Instalar rsync

sudo apt update && sudo apt install rsync -y


# Backup local automatizado con rsync (a disco externo/montado)

rsync -avh --delete /home/user/data/ /mnt/backup_disk/data/


# Backup cifrado con GPG

tar -czf backup-$(date +%F).tar.gz /home/user/data

gpg --symmetric --cipher-algo AES256 backup-$(date +%F).tar.gz


# Subida a Google Drive con rclone (previamente configurado)

rclone copy backup-$(date +%F).tar.gz.gpg remote:Backups/Codearts
```

Retención y rotación con cron (ejemplo: eliminar backups de +7 días)

echo "0 3 * * * find /mnt/backup_disk/data -type f -mtime +7 -delete" | sudo tee -a /etc/crontab

(Opcional) Veeam Backup (Linux Agent CLI)

sudo veeamconfig job create --name "LocalBackup" --path /home/user/data --target /mnt/backup_disk --schedule daily

---

🔹 Fase 3: Simulación de fallo del sistema y recuperación de datos

Simular fallo: renombrar y bloquear acceso a directorio crítico (NO EN PRODUCCIÓN)

sudo mv /home/user/data /home/user/data_locked

Restaurar desde copia rsync local

rsync -avh /mnt/backup_disk/data/ /home/user/data/

Verificar integridad con sha256sum

sha256sum /home/user/data/file.txt

sha256sum /mnt/backup_disk/data/file.txt

Restaurar backup cifrado

gpg -d backup-2025-07-24.tar.gz.gpg | tar -xz -C /home/user/restored_data

---

🔹 Fase 4: Desarrollo del Plan de Recuperación ante Desastres (DRP)

```
# Crear plantilla de DRP paso a paso (Markdown)

nano /opt/DRP/recuperacion_codearts.md


# Ejemplo de contenido:

# 1. Notificar al equipo de respuesta

# 2. Montar disco de respaldo

# 3. Ejecutar restauración rsync

# 4. Verificar integridad

# 5. Reportar cierre de incidente


# Asignar responsables en archivo de planificación

nano /opt/DRP/equipo_respuesta.csv


# Programar pruebas de restauración trimestrales con cron

echo "0 2 1 */3 * /usr/local/bin/simular_restauracion.sh" | sudo tee -a /etc/crontab
```