

## Identificación

Implica identificar el riesgo potencial que puede afectar las operaciones u objetivos del negocio.

## Evaluación

Incluye evaluar la probabilidad y el impacto de cada peligro en las empresas.

# 6.4 Seguridad y Prevención en el Proceso de Replicación



Plan de Contingencia



## Respuesta

Esta fase cubre la definición de las



## Supervisión

Se trata de



# Definición y propósito del plan de contingencia

El plan de contingencia en el proceso de replicación es **un conjunto de procedimientos y estrategias diseñados para garantizar la disponibilidad y recuperación de los datos en caso de fallos o desastres.**

*"Para garantizar la plena seguridad de los datos y de los ficheros de una organización es imprescindible salvaguardar la integridad y disponibilidad de dichos datos."*

- ✓ Protección contra pérdidas de datos
- ✓ Garantía de continuidad operativa
- ✓ Recuperación rápida ante incidentes



# Elementos esenciales del plan de contingencia

## Componentes clave para un plan efectivo

- 1 Política de replicación claramente definida
- 2 Gestión de soportes y registros
- 3 Registro de incidencias
- 4 Verificación y pruebas periódicas
- 5 Separación de sistemas
- 6 Responsabilidades y autorizaciones

## 4 ELEMENTOS DE UN PLAN DE CONTINGENCIA

- ☒ DEFINIR LAS SITUACIONES DELICADAS
- ☒ DIVIDE LAS RESPONSABILIDADES
- ☒ ACCIONES DE RESPUESTA
- ☒ MANTENIMIENTO DEL PLAN

*Todos los elementos son fundamentales para garantizar la seguridad y disponibilidad de los datos*

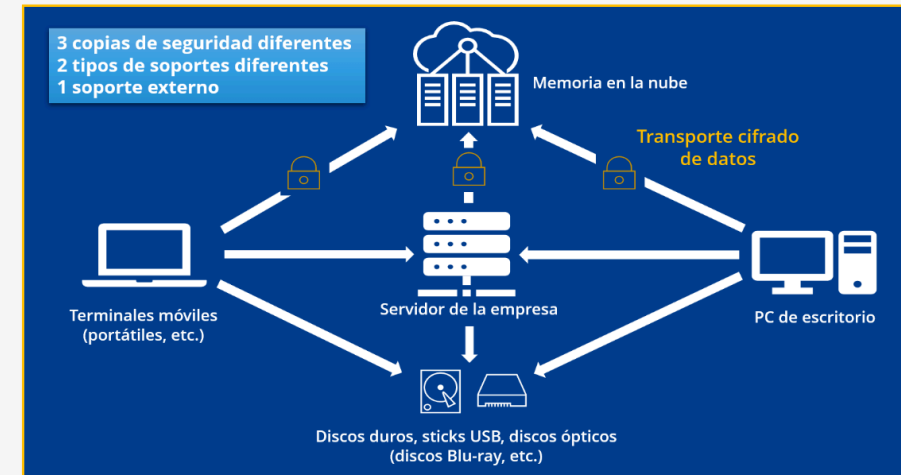
# Elemento 1: Política de replicación claramente definida

*"La política de replicación de los datos de la organización debería establecer la planificación de las copias que se deberían realizar en función del volumen y tipo de información generada por el sistema informático, especificando el tipo de copias (completa, incremental o diferencial) y el ciclo de esta operación (diario, semanal)."*

## Recomendaciones

- ⌚ Establecer **frecuencias adecuadas** según la criticidad de los datos
- 📌 Definir **claramente los tipos** de copias a realizar
- 📄 Documentar los procedimientos de manera detallada
- 👤 Designar responsables de la ejecución y supervisión

### Optimizar la estrategia de backup con la regla 3-2-1



IONOS

*Estrategia de backup 3-2-1: 3 copias, 2 tipos de soportes, 1 copia externa*

# Elemento 2: Gestión de soportes y registros

*"Así mismo, será preciso establecer cómo se van a inventariar y etiquetar las cintas y otros soportes utilizados para la replicación, registrando las copias realizadas, así como las posibles restauraciones de datos que se tengan que llevar a cabo en caso de pérdida de datos."*

## Recomendaciones

- Implementar un **sistema de inventario** y etiquetado claro
- Mantener **registros actualizados** de todas las operaciones
- Establecer procedimientos para verificación periódica
- Definir vida útil de soportes y programa de reemplazo



*Diversos soportes de almacenamiento para una gestión eficiente de datos*

# Elemento 3: Registro de incidencias

*"La pérdida o destrucción, parcial o total, de los datos de un fichero debería anotarse en un registro de incidencias. Las restauraciones de datos deberían llevarse a cabo con la correspondiente autorización de un responsable del sistema informático, siendo anotadas en el propio registro de incidencias o en un registro específico habilitado a tal fin por la organización."*

## Recomendaciones

- ⚠ **Documentar** todas las incidencias relacionadas con la pérdida de datos
- ✓ Establecer **autorizaciones claras** para operaciones de restauración
- 🕒 Mantener registro detallado de todas las restauraciones
- 📊 Analizar periódicamente las incidencias para mejorar el plan



*Gestión de eventos de seguridad con control de acceso y registro*



# Elemento 4: Verificación y pruebas periódicas

*"Así mismo, la organización debería establecer cómo y cuándo se realizarán comprobaciones de forma periódica para verificar el estado de los soportes y el correcto funcionamiento del proceso de generación de las copias de seguridad."*

## Recomendaciones

- 🕒 Programar **verificaciones regulares** de la integridad de las copias
- 🔄 Realizar **pruebas de restauración** periódicas para verificar funcionalidad
- 📄 Documentar los resultados de las pruebas y acciones correctivas
- 🔄 Actualizar el plan según los resultados de las pruebas



*Verificación física de los soportes de almacenamiento*

# Elemento 5: Separación de sistemas

*"Es recomendable que los datos y el sistema operativo se encuentren en discos o particiones separadas, para facilitar la aplicación del plan de contingencia."*

## Recomendaciones

- Implementar una **estructura de almacenamiento** que facilite la recuperación
- Separar **datos críticos** del sistema operativo y aplicaciones
- Considerar almacenamiento geográficamente distribuido para protección ante desastres







*Separación de sistemas: almacenamiento distribuido y procesamiento de datos*

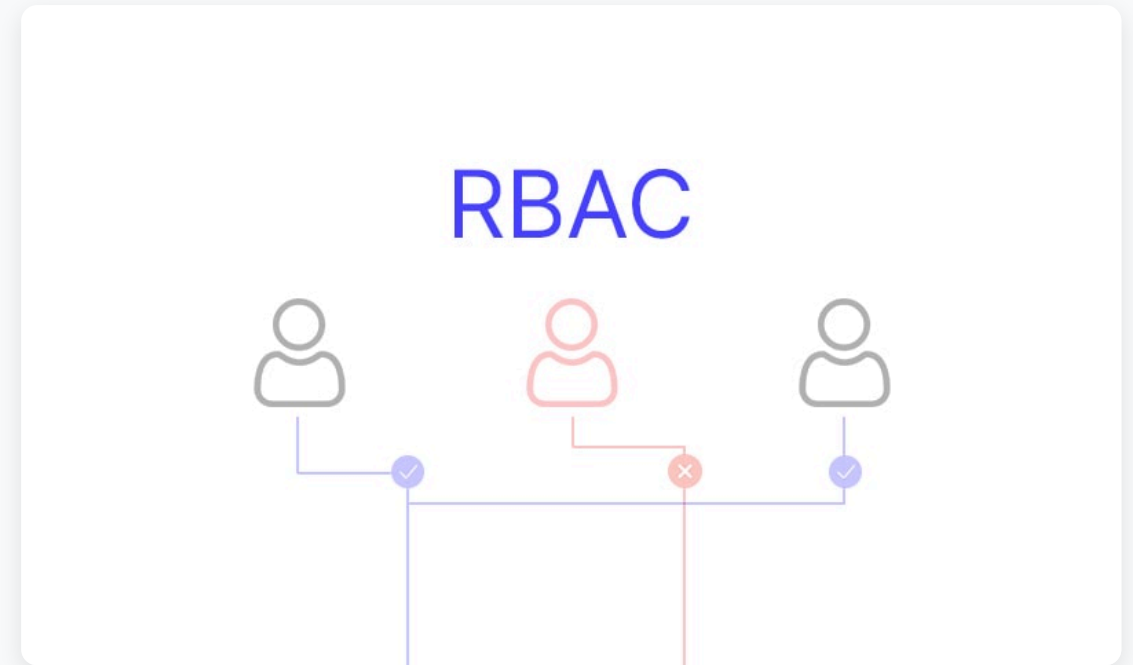


# Elemento 6: Responsabilidades y autorizaciones

*"Las replicasiones de los datos y ficheros de los servidores deberían ser realizadas y supervisadas por personal debidamente autorizado."*

## Recomendaciones

-  **Definir claramente** quién es responsable de cada aspecto del plan
-  Establecer **niveles de autorización** para diferentes operaciones
-  Implementar controles de acceso adecuados a las copias de seguridad
-  Proporcionar formación específica al personal responsable



*Modelo RBAC: relación entre usuarios, roles y permisos*

# Estrategias de seguridad adicionales

## Medidas complementarias para protección de datos



### Cifrado de copias

Proteger las copias que contengan información sensible



### Control de acceso

Limitar el acceso a las copias solo al personal autorizado



### Prevención de ejecución de datos (DEP)

Supervisión de programas para garantizar uso seguro de memoria

*"DEP ayuda a protegerse contra los virus y otras amenazas a la seguridad, mediante la supervisión de los programas para garantizar que utilizan la memoria de forma segura."*



### Planificación de recuperación





Establecer tiempos máximos de recuperación (RTO) y puntos de recuperación aceptables (RPO)

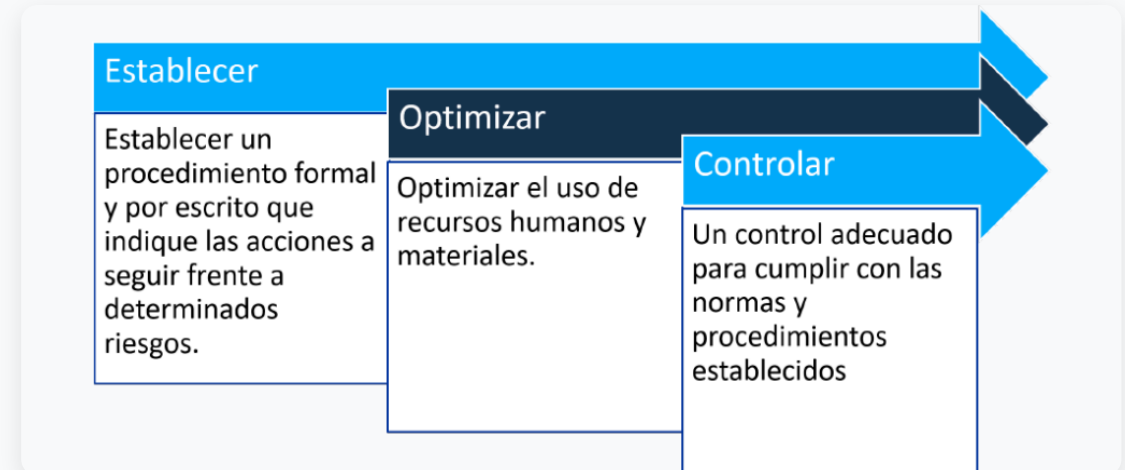


*Pasos para una estrategia efectiva de replicación de datos*

# Conclusión: Características de un plan de contingencia efectivo

## Elementos clave para garantizar la seguridad de los datos

-  **Completo:** Cubriendo todos los aspectos críticos de la organización
-  **Documentado:** Con procedimientos claros y accesibles
-  **Probado:** Con verificaciones periódicas de funcionalidad
-  **Actualizado:** Adaptado a los cambios en la infraestructura y necesidades



*Ciclo de mejora continua: establecer, optimizar y controlar*

*"¿Qué ocurriría si por error, distracción, fallo mecánico, etc., se produce una pérdida de datos importante? Pues no pasaría nada si se cuenta con un buen sistema de copias de seguridad de dichos datos que permita restaurar la información prácticamente al mismo nivel que se encontraba antes de su pérdida."*