Facultad de Ingeniería

# Unidad 5. Disponibilidad y continuidad del negocio

Apunte de cátedra

# Contenido

# 5. Disponibilidad y Continuidad del Negocio

**Introducción**

La seguridad de la información no solo busca proteger la información contra accesos no autorizados o modificaciones indebidas, sino también garantizar que los datos y los servicios estén disponibles cuando sean necesarios. Por este motivo, la **disponibilidad** constituye uno de los tres pilares fundamentales de la seguridad de la información, junto con la confidencialidad y la integridad.

Para lograr un nivel adecuado de disponibilidad, las organizaciones implementan diferentes mecanismos técnicos y organizativos destinados a reducir el impacto de las fallas y asegurar la continuidad de sus operaciones. Entre ellos se encuentran la redundancia de componentes, los sistemas de alta disponibilidad, el almacenamiento mediante RAID, las copias de seguridad, los planes de recuperación y los planes de contingencia.

## 5.1. Disponibilidad de la Información

### 5.1.1. Concepto de Disponibilidad

La **disponibilidad** es la propiedad que garantiza que la información, los sistemas y los servicios informáticos puedan ser utilizados por los usuarios autorizados cuando los necesiten.

En otras palabras, la disponibilidad asegura que los recursos informáticos permanezcan operativos y accesibles durante el tiempo requerido para el desarrollo normal de las actividades de una organización.

Desde el punto de vista de la seguridad informática, la disponibilidad constituye uno de los tres pilares fundamentales del modelo **CIA (Confidencialidad, Integridad y Disponibilidad)**.

Mientras que:

- la **confidencialidad** protege la información frente a accesos no autorizados;
- la **integridad** garantiza que la información no sea modificada de forma indebida;

la **disponibilidad** procura que la información y los servicios puedan utilizarse en el momento en que sean requeridos.

**Ejemplo**

Un hospital dispone de un sistema informático para acceder a las historias clínicas de sus pacientes.

Aunque la información sea confidencial y los datos almacenados sean íntegros, si el sistema deja de funcionar durante una emergencia médica, los profesionales no podrán acceder a la información necesaria para atender al paciente.

En este caso, el problema no afecta la confidencialidad ni la integridad de la información, sino su **disponibilidad**.

Este ejemplo demuestra que proteger la información implica no solo evitar su pérdida o alteración, sino también garantizar que permanezca accesible cuando resulte necesaria.

## 5.1.2. Importancia de la Disponibilidad

La disponibilidad es un requisito esencial para el funcionamiento de cualquier organización que dependa de sistemas informáticos.

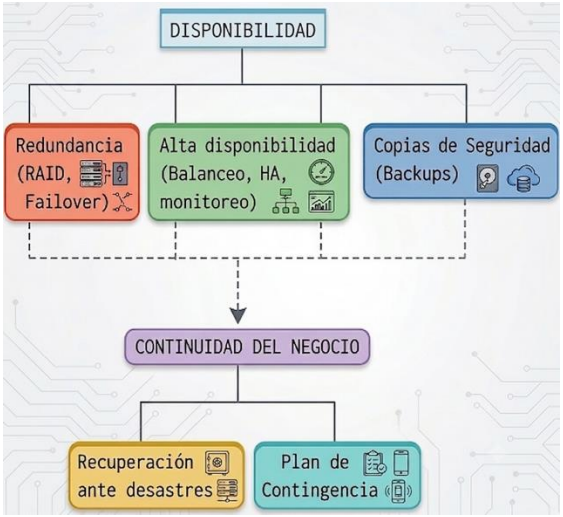
La interrupción de un servicio puede producir consecuencias como:

- suspensión de las actividades operativas;
- pérdidas económicas;
- disminución de la productividad;
- incumplimiento de contratos o requisitos legales;
- pérdida de confianza de clientes y usuarios;
- daños a la imagen institucional.

En algunos sectores, como la salud, la banca, el transporte o las telecomunicaciones, incluso una interrupción de pocos minutos puede generar consecuencias significativas.

Por este motivo, las organizaciones implementan diferentes mecanismos para reducir la probabilidad de fallas y minimizar el tiempo necesario para recuperar los servicios cuando ocurre un incidente.

La siguiente figura muestra la relación entre la disponibilidad y la continuidad de los servicios.




## 5.1.3. Factores que afectan la disponibilidad

La disponibilidad de la información puede verse comprometida por diversos factores que provocan la interrupción parcial o total de los sistemas informáticos. Estas interrupciones pueden afectar desde un único equipo hasta toda la infraestructura tecnológica de una organización. Conocer las causas que pueden provocar la indisponibilidad de los servicios

constituye el primer paso para implementar mecanismos que permitan prevenirlas o minimizar sus consecuencias.

Los principales factores que afectan la disponibilidad pueden agruparse en las siguientes categorías.

# 5.1.3.1. Fallas de hardware

Las fallas de hardware constituyen una de las causas más frecuentes de indisponibilidad de los sistemas informáticos. Los componentes físicos poseen una vida útil limitada y pueden dejar de funcionar debido al desgaste, defectos de fabricación o condiciones ambientales inadecuadas.

Algunos ejemplos son:

- fallas en discos rígidos o unidades SSD;
- averías en servidores;
- fallas de memoria RAM;
- fuentes de alimentación defectuosas;
- interrupciones en equipos de red, como switches y routers.

Cuando alguno de estos componentes falla, el servicio puede quedar total o parcialmente fuera de funcionamiento hasta que el problema sea solucionado.

# 5.1.3.2. Fallas de software

Los errores presentes en el software también pueden afectar la disponibilidad de los servicios.

Estos problemas pueden originarse por:

- errores de programación;
- fallas del sistema operativo;
- incompatibilidades entre aplicaciones;
- actualizaciones defectuosas;
- configuraciones incorrectas.

En algunos casos, una falla de software puede provocar que un servidor deje de responder o que una aplicación crítica resulte inaccesible para los usuarios.

# 5.1.3.3. Errores humanos

Las acciones involuntarias realizadas por los usuarios o administradores representan otra causa importante de indisponibilidad.

Entre los errores más comunes se encuentran:

- eliminación accidental de archivos;
- configuraciones incorrectas;

- desconexión de equipos críticos;
- instalación de software incompatible;
- administración inadecuada de los sistemas.

La capacitación del personal y la existencia de procedimientos adecuados permiten reducir considerablemente este tipo de incidentes.

## 5.1.3.4. Ataques informáticos

Los incidentes de seguridad también pueden afectar directamente la disponibilidad de los sistemas. Algunos ataques buscan impedir que los usuarios legítimos puedan acceder a la información o a los servicios.

Entre ellos se destacan:

- ataques de denegación de servicio (DoS y DDoS);
- ransomware que cifra la información;
- malware que inutiliza equipos o servidores;
- sabotaje interno.

En estos casos, aunque la información no sea destruida, puede permanecer inaccesible durante un período de tiempo considerable.

## 5.1.3.5. Desastres naturales y eventos ambientales

La infraestructura informática también puede verse afectada por fenómenos naturales o problemas ambientales.

Entre ellos pueden mencionarse:

- incendios;
- inundaciones;
- terremotos;
- tormentas eléctricas;
- cortes prolongados del suministro eléctrico;
- temperaturas o humedad excesivas.

Estos eventos pueden ocasionar daños severos en los equipos y provocar interrupciones prolongadas de los servicios.

## 5.1.3.6. Problemas en las comunicaciones

Muchas organizaciones dependen de redes locales, enlaces de Internet y servicios en la nube para desarrollar sus actividades. La interrupción de alguno de estos servicios puede impedir el acceso a aplicaciones o bases de datos, aun cuando los servidores continúen funcionando correctamente.

Entre las causas más frecuentes se encuentran:

- fallas del proveedor de Internet;
- cortes en enlaces de comunicaciones;
- averías en equipos de red;
- saturación del ancho de banda.

Los mecanismos estudiados en los próximos apartados —**redundancia, alta disponibilidad, RAID, copias de seguridad y planes de contingencia**— tienen como objetivo reducir el impacto de estos factores y garantizar que la organización pueda continuar prestando sus servicios aun cuando ocurra una falla o un incidente.

## 5.2. Redundancia, Alta Disponibilidad y Tolerancia a Fallos

En el apartado anterior se analizaron los principales factores que pueden afectar la disponibilidad de los sistemas informáticos. Una vez conocidas las posibles causas de interrupción, el siguiente paso consiste en estudiar los mecanismos que permiten minimizar sus consecuencias.

Entre las estrategias más utilizadas para mantener la disponibilidad de los servicios se encuentran la **redundancia**, la **alta disponibilidad** y la **tolerancia a fallos**. Aunque estos conceptos se encuentran estrechamente relacionados, representan enfoques diferentes para garantizar la continuidad del funcionamiento de los sistemas.

### 5.2.1. Redundancia

La **redundancia** consiste en incorporar componentes adicionales que permitan mantener el funcionamiento de un sistema cuando uno de sus elementos deja de operar correctamente.

En otras palabras, un sistema redundante incorpora elementos de respaldo para evitar que una falla individual provoque la interrupción del servicio.

Estos componentes pueden permanecer inactivos hasta que sean necesarios o funcionar simultáneamente con el componente principal, dependiendo del diseño de la infraestructura.

La redundancia puede aplicarse a distintos recursos informáticos, entre ellos:

- servidores;
- discos de almacenamiento;
- fuentes de alimentación;
- enlaces de comunicaciones;
- dispositivos de red;
- centros de datos.

Su objetivo principal es eliminar los **puntos únicos de falla** (*Single Point of Failure* o **SPOF**), es decir, aquellos componentes cuya avería provocaría la interrupción completa de un servicio. Dependiendo de la arquitectura implementada, los componentes

redundantes pueden permanecer inactivos hasta que ocurra una falla o funcionar simultáneamente con el componente principal.

# 5.2.1.1. Duplicación de componentes

La forma más común de implementar redundancia consiste en la **duplicación de componentes críticos**.

Duplicar un componente significa disponer de otro elemento equivalente que pueda asumir su función cuando el principal deja de funcionar. La duplicación puede aplicarse a diferentes elementos de una infraestructura informática.

Por ejemplo:

- un segundo servidor que reemplaza automáticamente al principal;
- dos fuentes de alimentación en un mismo servidor;
- dos enlaces de Internet contratados con distintos proveedores;
- dos switches conectando la red principal;
- múltiples discos de almacenamiento configurados mediante tecnologías RAID.

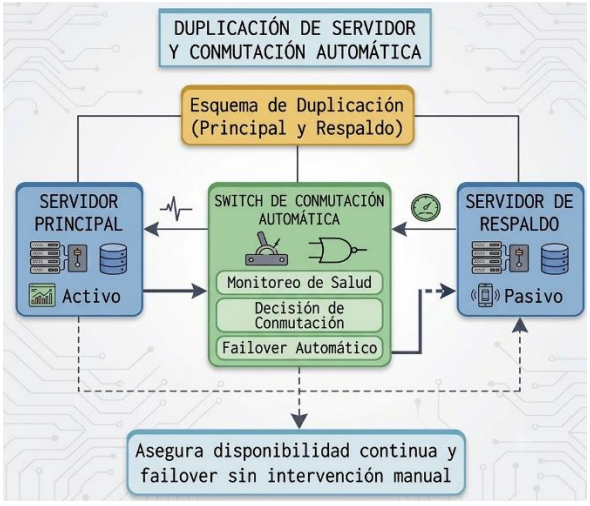
En todos estos casos, el objetivo es evitar que la falla de un único componente provoque la interrupción completa del servicio.

# 5.2.1.2. Ejemplo

Supóngase un servidor que almacena la base de datos de una empresa. Si dicho servidor es el único disponible, una falla de hardware dejará a toda la organización sin acceso a la información.

En cambio, si existe un segundo servidor preparado para reemplazar automáticamente al primero, el servicio podrá continuar funcionando mientras se realiza la reparación del equipo averiado.

La siguiente figura muestra el principio general de la redundancia.



## 5.2.1.3. Ventajas de la redundancia

La utilización de componentes redundantes proporciona diversos beneficios, entre ellos:

- disminuye la probabilidad de interrupción del servicio;
- incrementa la disponibilidad de los sistemas;
- facilita las tareas de mantenimiento;
- mejora la continuidad de las operaciones;
- reduce el impacto producido por fallas de hardware.

## 5.2.1.4. Limitaciones

Aunque la redundancia incrementa la disponibilidad, también presenta algunas desventajas.

Entre las principales pueden mencionarse:

- incremento del costo de adquisición del equipamiento;
- mayor complejidad de administración;
- necesidad de sincronizar la información entre los componentes redundantes;
- incremento de los costos de mantenimiento.

Por este motivo, la incorporación de redundancia suele reservarse para aquellos sistemas cuya disponibilidad resulta crítica para la organización.

## 5.2.2. Alta Disponibilidad (High Availability)

La **alta disponibilidad** (*High Availability* o **HA**) es una estrategia cuyo objetivo consiste en mantener un servicio operativo durante la mayor parte del tiempo posible, minimizando las interrupciones ocasionadas por fallas o tareas de mantenimiento.

Mientras que la redundancia incorpora componentes adicionales, la alta disponibilidad integra diversos mecanismos tecnológicos y organizativos para garantizar la continuidad del servicio.

En consecuencia, **la redundancia constituye uno de los mecanismos utilizados para alcanzar la alta disponibilidad**, **pero no es el único**.

Una infraestructura de alta disponibilidad puede incorporar:

- servidores redundantes;
- almacenamiento redundante;
- balanceadores de carga;
- múltiples enlaces de comunicaciones;
- monitoreo continuo;
- mecanismos de conmutación automática (*failover*);
- detección automática de fallas.

El funcionamiento conjunto de estos elementos permite reducir considerablemente el tiempo de indisponibilidad de los servicios.

# 5.2.2.1. Disponibilidad expresada como porcentaje

La disponibilidad suele medirse como el porcentaje de tiempo durante el cual un servicio permanece operativo.

| Disponibilidad | Tiempo máximo de indisponibilidad aproximado por año |
|---|---|
| 99 % | 3,65 días |
| 99,9 % | 8,76 horas |
| 99,99 % | 52 minutos |
| 99,999 % | 5 minutos |

Estos niveles son conocidos como **"nueves de disponibilidad"** (*Availability Nines*).

Cuanto mayor sea el porcentaje de disponibilidad, menor será el tiempo permitido de interrupción del servicio.

# 5.2.2.2. Ejemplo

Los sistemas de banca electrónica requieren niveles muy elevados de disponibilidad debido a que los clientes necesitan acceder a sus cuentas en cualquier momento.

Para lograrlo, las entidades financieras implementan servidores redundantes, enlaces alternativos de comunicaciones, balanceadores de carga y sistemas de monitoreo permanente que permiten mantener los servicios operativos incluso cuando alguno de sus componentes presenta una falla.

# 5.2.2.3. Beneficios de la Alta Disponibilidad

La alta disponibilidad permite:

- reducir el tiempo de inactividad;
- mejorar la continuidad de los servicios;
- incrementar la confiabilidad de la infraestructura;
- disminuir las pérdidas económicas producidas por interrupciones;
- aumentar la satisfacción de los usuarios.

# 5.2.3. Tolerancia a Fallos

La **tolerancia a fallos** (*Fault Tolerance*) es la capacidad de un sistema para continuar funcionando correctamente aun cuando uno o más de sus componentes presenten una falla.

A diferencia de otros mecanismos que requieren detener el servicio para reemplazar un componente averiado, un sistema tolerante a fallos continúa operando sin interrupciones perceptibles para los usuarios. En otras palabras, el sistema está diseñado para soportar determinadas fallas sin afectar la disponibilidad del servicio.

Para lograr este objetivo, normalmente se utilizan componentes redundantes que funcionan de manera simultánea y mecanismos capaces de detectar automáticamente la falla y continuar la operación utilizando los recursos disponibles.

## 5.2.3.1. ¿Cómo funciona un sistema tolerante a fallos?

En un sistema convencional, la avería de un componente crítico puede provocar la interrupción inmediata del servicio. En cambio, un sistema tolerante a fallos incorpora componentes duplicados o múltiples caminos alternativos que permiten mantener el funcionamiento aun cuando uno de ellos falle.

Cuando se produce la falla:

- el componente defectuoso es aislado;
- otro componente continúa realizando la misma función;
- el servicio permanece disponible para los usuarios.

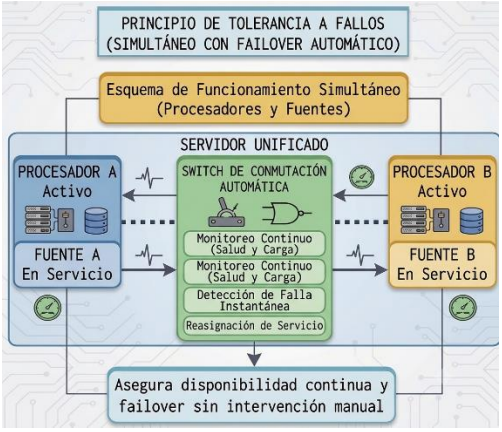
En muchos casos, los usuarios ni siquiera perciben que ocurrió una falla.

## 5.2.3.2. Ejemplo

Supóngase un servidor equipado con dos fuentes de alimentación conectadas simultáneamente. Mientras ambas funcionan, cada una puede alimentar al servidor. Si una de las fuentes deja de operar, la otra continúa suministrando energía de manera inmediata, sin necesidad de apagar el equipo ni interrumpir el servicio.

Desde el punto de vista del usuario, el sistema continúa funcionando normalmente. Este es un ejemplo típico de **tolerancia a fallos**.

La siguiente figura muestra el principio general de funcionamiento de un sistema tolerante a fallos.



## 5.2.3.3. Características de un sistema tolerante a fallos

Los sistemas tolerantes a fallos presentan, generalmente, las siguientes características:

- utilizan componentes redundantes que operan simultáneamente;
- detectan automáticamente la falla de un componente;
- mantienen el servicio sin interrupciones;
- reducen al mínimo la pérdida de información;
- incrementan la confiabilidad del sistema.

Estas características hacen que la tolerancia a fallos sea utilizada principalmente en aplicaciones donde una interrupción del servicio resulta inaceptable.

## 5.2.3.4. Aplicaciones

La tolerancia a fallos suele implementarse en sistemas críticos, entre ellos:

- sistemas bancarios;
- centros de procesamiento de datos;
- hospitales;
- sistemas aeronáuticos;
- telecomunicaciones;
- centrales de energía;
- infraestructuras militares.

En este tipo de organizaciones, incluso una interrupción de pocos segundos puede producir pérdidas económicas importantes o poner en riesgo la seguridad de las personas.

## 5.2.3.5. Ventajas

La utilización de sistemas tolerantes a fallos ofrece diversas ventajas:

- continuidad del servicio aun cuando ocurren fallas;
- mayor disponibilidad de la infraestructura;
- reducción del tiempo de inactividad;
- incremento de la confiabilidad del sistema;
- disminución del impacto producido por fallas de hardware.

## 5.2.3.6. Limitaciones

A pesar de sus ventajas, la tolerancia a fallos también presenta algunas limitaciones.

Entre las principales pueden mencionarse:

- elevado costo de implementación;
- mayor complejidad de diseño;
- incremento de los costos de mantenimiento;
- necesidad de equipamiento especializado;

- mayor consumo de recursos.

Por este motivo, normalmente solo se implementa en infraestructuras cuya disponibilidad resulta esencial para la organización.

## 5.2.4. Diferencias entre Redundancia, Alta Disponibilidad y Tolerancia a Fallos

Los conceptos de **redundancia**, **alta disponibilidad** y **tolerancia a fallos** suelen utilizarse conjuntamente porque todos buscan mejorar la disponibilidad de los sistemas informáticos. Sin embargo, no representan el mismo nivel de protección ni persiguen exactamente el mismo objetivo.

La **redundancia** constituye el mecanismo básico sobre el cual se apoyan las demás estrategias. Consiste en incorporar componentes adicionales que puedan reemplazar a aquellos que presenten una falla.

La **alta disponibilidad** utiliza la redundancia junto con otros mecanismos de administración y monitoreo para reducir al mínimo el tiempo durante el cual un servicio permanece fuera de funcionamiento.

Por su parte, la **tolerancia a fallos** representa el nivel más elevado de disponibilidad, ya que el sistema continúa operando sin interrupciones incluso cuando uno de sus componentes deja de funcionar.

En consecuencia, puede afirmarse que la redundancia constituye la base para implementar soluciones de alta disponibilidad y que, en determinadas arquitecturas, estas permiten alcanzar sistemas tolerantes a fallos.

La siguiente tabla resume las principales diferencias entre estos conceptos.

| Característica | Redundancia | Alta Disponibilidad | Tolerancia a Fallos |
|---|---|---|---|
| **Objetivo principal** | Incorporar componentes de respaldo. | Reducir al mínimo el tiempo de indisponibilidad. | Mantener el servicio funcionando aun cuando ocurran fallas. |
| **¿Utiliza componentes duplicados?** | Sí. | Sí, generalmente. | Sí, siempre. |
| **¿Puede existir interrupción del servicio?** | Sí. | Sí, pero muy breve. | No, o resulta imperceptible para los usuarios. |
| **Tiempo de recuperación** | Depende del reemplazo del componente o del | Muy reducido. | Inmediato. |

| Característica | Redundancia | Alta Disponibilidad | Tolerancia a Fallos |
|---|---|---|---|
| | mecanismo de conmutación. | | |
| **Complejidad de implementación** | Baja o media. | Media o alta. | Muy alta. |
| **Costo de implementación** | Medio. | Alto. | Muy alto. |
| **Ejemplo** | Dos discos configurados en RAID 1. | Clúster de servidores con *failover*. | Servidor con componentes completamente redundantes funcionando simultáneamente. |

## 5.2.5. Relación entre los tres conceptos

Aunque presentan diferencias, estos mecanismos suelen implementarse de manera complementaria.

Por ejemplo, una organización puede comenzar incorporando redundancia en los componentes más importantes de su infraestructura. Posteriormente, puede agregar mecanismos de monitoreo y conmutación automática para lograr una solución de alta disponibilidad. Finalmente, en aquellos sistemas donde una interrupción resulta inaceptable, puede implementarse una arquitectura tolerante a fallos.

## 5.2.6. ¿Qué estrategia conviene implementar?

No todas las organizaciones requieren el mismo nivel de disponibilidad. La elección de una estrategia dependerá de factores como:

- la criticidad del servicio;
- el impacto económico de una interrupción;
- los requisitos legales o contractuales;
- el presupuesto disponible;
- el nivel de riesgo aceptable para la organización.

Por ejemplo, una pequeña empresa puede considerar suficiente implementar copias de seguridad y algunos componentes redundantes. En cambio, un banco, un hospital o una empresa de telecomunicaciones probablemente necesiten infraestructuras de alta disponibilidad o incluso sistemas tolerantes a fallos para garantizar la continuidad de sus operaciones.

En general, cuanto mayor sea la disponibilidad requerida, mayor será la inversión necesaria en infraestructura, administración y mantenimiento.

## 5.2.7. Ejemplos de Aplicación

Las organizaciones no requieren el mismo nivel de disponibilidad para todos sus sistemas. La elección entre implementar únicamente redundancia, una solución de alta disponibilidad o una arquitectura tolerante a fallos dependerá de la importancia del servicio, del impacto que tendría una interrupción y del presupuesto disponible.

A continuación, se presentan algunos ejemplos que ilustran la aplicación de estos mecanismos en distintos escenarios.

### 5.2.7.1. Ejemplo 1. Redundancia en una pequeña empresa

Una pequeña empresa de diseño gráfico posee un único servidor donde almacena los archivos de sus clientes.

Con el propósito de reducir la probabilidad de interrupción del servicio, decide incorporar componentes redundantes, tales como:

- un segundo disco de almacenamiento;
- una segunda fuente de alimentación;
- un enlace alternativo de Internet.

De esta manera, si alguno de estos componentes presenta una falla, existe otro que puede asumir su función o permitir que el servicio continúe funcionando mientras se reemplaza el componente averiado. En este caso, la organización ha implementado **redundancia**, aunque todavía pueden producirse interrupciones mientras se realiza la reparación o el reemplazo del componente defectuoso.

### 5.2.7.2. Ejemplo 2. Alta disponibilidad en un comercio electrónico

Una empresa dedicada a la venta de productos por Internet recibe pedidos las 24 horas del día. Una interrupción prolongada del sitio web impediría realizar ventas y provocaría pérdidas económicas.

Para minimizar este riesgo, la empresa implementa:

- dos servidores de aplicaciones;
- un balanceador de carga;
- almacenamiento redundante;
- monitoreo permanente;
- conmutación automática (*failover*).

Cuando uno de los servidores presenta una falla, el balanceador deriva automáticamente las solicitudes al servidor restante. Los usuarios pueden experimentar una interrupción muy breve o incluso no percibirla. En este caso, la organización dispone de una infraestructura de **alta disponibilidad**.

## 5.2.7.3. Ejemplo 3. Tolerancia a fallos en un hospital

Un hospital utiliza un sistema informático para acceder a las historias clínicas electrónicas de sus pacientes. La indisponibilidad del sistema durante una cirugía o una emergencia médica podría poner en riesgo la vida de las personas.

Por este motivo, la infraestructura incorpora:

- servidores funcionando simultáneamente;
- almacenamiento redundante;
- múltiples fuentes de alimentación;
- enlaces de comunicación duplicados;
- sistemas de alimentación ininterrumpida (UPS);
- mecanismos automáticos de detección y aislamiento de fallas.

Si uno de los componentes deja de funcionar, los restantes continúan prestando el servicio sin interrupciones. Este es un ejemplo de **tolerancia a fallos**, donde el objetivo principal consiste en garantizar la continuidad absoluta del servicio.

## 5.2.7.4. Ejemplo 4. Centro de datos bancario

Una entidad bancaria presta servicios de banca electrónica, cajeros automáticos y transferencias durante las 24 horas del día.

Para garantizar la continuidad de las operaciones implementa una combinación de mecanismos:

- servidores redundantes;
- almacenamiento redundante;
- enlaces de comunicaciones redundantes;
- balanceadores de carga;
- sistemas de alta disponibilidad;
- centros de datos alternativos;
- planes de recuperación ante desastres.

En este caso no se utiliza un único mecanismo, sino una estrategia integral que combina **redundancia**, **alta disponibilidad** y **tolerancia a fallos**, dependiendo de la criticidad de cada servicio.

## 5.2.7.5. ¿Cuál es la solución más adecuada?

No existe una única solución válida para todas las organizaciones. La elección dependerá principalmente de los siguientes factores:

- criticidad del servicio;
- impacto económico de una interrupción;
- requisitos legales o normativos;
- cantidad de usuarios afectados;
- presupuesto disponible;

- nivel de riesgo aceptable para la organización.

Por ejemplo:

- Una pequeña oficina puede considerar suficiente implementar redundancia mediante discos redundantes y copias de seguridad periódicas.
- Una universidad probablemente requiera servidores de alta disponibilidad para garantizar el acceso continuo a sus plataformas educativas.
- Un hospital, una entidad financiera o una empresa de telecomunicaciones necesitarán infraestructuras tolerantes a fallos para asegurar que los servicios permanezcan operativos aun cuando se produzcan fallas.

En consecuencia, la disponibilidad no depende únicamente de la incorporación de equipamiento redundante, sino de un adecuado equilibrio entre los riesgos identificados, la criticidad de los servicios y los recursos que la organización esté dispuesta a invertir.

# 5.3. Sistemas RAID

La falla de un disco rígido o de una unidad de estado sólido (SSD) puede provocar la pérdida de información o la interrupción de los servicios, afectando directamente la disponibilidad de los sistemas.

Para disminuir este riesgo surgieron las tecnologías **RAID (Redundant Array of Independent Disks)**, que permiten combinar varios discos físicos para mejorar la disponibilidad de la información y, en algunos casos, incrementar el rendimiento del sistema de almacenamiento.

# 5.3.1. Concepto de RAID

**RAID** es el acrónimo de **Redundant Array of Independent Disks** (Conjunto Redundante de Discos Independientes). Consiste en una tecnología que permite combinar dos o más discos físicos para que funcionen como una única unidad lógica de almacenamiento.

Dependiendo del nivel RAID utilizado, esta tecnología puede perseguir uno o más de los siguientes objetivos:

- incrementar la disponibilidad de la información;
- mejorar el rendimiento de lectura y escritura;
- proteger los datos frente a la falla de uno o varios discos;
- combinar rendimiento y redundancia.

La forma en que los datos se distribuyen entre los discos determina las características de cada nivel RAID. Algunos niveles priorizan el rendimiento, otros la redundancia y otros buscan un equilibrio entre ambos aspectos.

Es importante destacar que **RAID no reemplaza las copias de seguridad (backups)**.

Aunque algunos niveles permiten continuar trabajando cuando un disco falla, no protegen frente a situaciones como:

- eliminación accidental de archivos;
- ataques de ransomware;
- corrupción de datos;
- incendios;
- inundaciones;
- errores de configuración.

Por este motivo, RAID debe considerarse una tecnología destinada principalmente a mejorar la disponibilidad de la información y no como un mecanismo de respaldo.

# 5.3.1.1. ¿Cómo funciona RAID?

En un sistema convencional, toda la información se almacena en un único disco. Si ese disco deja de funcionar, el sistema puede perder el acceso a los datos hasta que el disco sea reemplazado y la información recuperada.

En cambio, en un sistema RAID la información se distribuye entre varios discos de acuerdo con un esquema determinado.

Dependiendo del nivel RAID implementado, el sistema puede:

- repartir la información entre varios discos para aumentar la velocidad de acceso;
- almacenar copias idénticas de los datos en diferentes discos;
- generar información de paridad que permita reconstruir los datos cuando un disco falla.

Gracias a estos mecanismos, muchos sistemas pueden continuar funcionando incluso después de la avería de uno de los discos que forman parte del arreglo.

# 5.3.1.2. Componentes de un sistema RAID

Un sistema RAID está compuesto, generalmente, por los siguientes elementos:

- **Discos físicos**, donde se almacena la información.
- **Controlador RAID**, encargado de administrar la distribución de los datos entre los discos.
- **Sistema operativo**, que visualiza el conjunto de discos como una única unidad lógica de almacenamiento.

Desde el punto de vista del usuario, el sistema operativo trabaja con un único volumen de almacenamiento, aunque internamente la información se encuentre distribuida entre varios discos.

Dependiendo de dónde se implemente el controlador RAID, es posible distinguir dos formas principales de administración: **RAID por hardware** y **RAID por software**.

## 5.3.1.3. RAID por Hardware y RAID por Software

Existen dos formas principales de implementar un sistema RAID: mediante una **controladora de hardware** o utilizando funciones proporcionadas por el **sistema operativo**. Ambas alternativas permiten construir arreglos RAID, aunque presentan diferencias en cuanto a rendimiento, costo y administración.

# RAID por Hardware

En el **RAID por hardware**, la administración del arreglo es realizada por una **controladora RAID dedicada**, que puede estar integrada en la placa madre del servidor o instalarse como una tarjeta de expansión. Esta controladora se encarga de distribuir los datos entre los discos, reconstruir la información cuando ocurre una falla y presentar el conjunto de discos como una única unidad lógica al sistema operativo.

Como la mayor parte del procesamiento es realizado por la controladora, el procesador principal del equipo prácticamente no interviene en estas tareas.

Entre sus principales ventajas se encuentran:

- mayor rendimiento;
- menor utilización del procesador;
- mayor confiabilidad;
- administración independiente del sistema operativo.

Su principal desventaja es el mayor costo, ya que requiere una controladora especializada.

# RAID por Software

En el **RAID por software**, la administración del arreglo es realizada por el propio sistema operativo, sin necesidad de una controladora específica. El sistema operativo organiza la distribución de los datos entre los discos utilizando los recursos del procesador principal.

Actualmente, la mayoría de los sistemas operativos modernos ofrecen soporte para distintos niveles RAID mediante software.

Entre sus principales ventajas pueden mencionarse:

- menor costo;
- mayor flexibilidad;
- no requiere hardware especializado.

Sin embargo, presenta algunas limitaciones:

- utiliza recursos del procesador principal;
- el rendimiento depende del sistema operativo;
- puede ofrecer un desempeño inferior al RAID por hardware en aplicaciones de alta demanda.

## Comparación entre RAID por Hardware y RAID por Software

La siguiente tabla resume las principales diferencias entre ambas alternativas.

| Característica | RAID por Hardware | RAID por Software |
|---|---|---|
| Administración | Controladora RAID dedicada | Sistema operativo |
| Uso del procesador | Muy bajo | Mayor utilización del CPU |
| Rendimiento | Generalmente superior | Depende del hardware del equipo |
| Costo | Más elevado | Más económico |
| Dependencia del sistema operativo | Baja | Alta |
| Aplicaciones habituales | Servidores empresariales y centros de datos | Equipos personales y pequeños servidores |

En la actualidad, ambas soluciones continúan utilizándose. La elección dependerá del presupuesto disponible, del rendimiento requerido y de la criticidad de los servicios que la organización necesite proteger.

# 5.3.1.4. Objetivos de RAID

La utilización de tecnologías RAID persigue principalmente los siguientes objetivos:

- aumentar la disponibilidad de la información;
- reducir el impacto producido por la falla de un disco;
- mejorar el rendimiento de acceso a los datos;
- facilitar la continuidad del servicio.

Sin embargo, no todos los niveles RAID cumplen simultáneamente estos objetivos. Algunos privilegian el rendimiento, mientras que otros priorizan la redundancia. Por esta razón, resulta fundamental seleccionar el nivel RAID más adecuado según las necesidades de la organización.

# 5.3.1.5. Ventajas de RAID

Entre las principales ventajas de RAID pueden mencionarse:

- mayor disponibilidad de la información;
- continuidad del servicio frente a determinadas fallas de discos;
- incremento del rendimiento en algunos niveles;

- posibilidad de reconstruir la información cuando falla un disco (según el nivel RAID).

Estas características convierten a RAID en una de las tecnologías de almacenamiento más utilizadas en servidores y centros de datos.

#### 5.3.1.6. Limitaciones de RAID

A pesar de sus ventajas, RAID presenta algunas limitaciones importantes:

- requiere dos o más discos físicos;
- incrementa el costo del sistema de almacenamiento;
- algunos niveles reducen la capacidad útil disponible;
- la reconstrucción de un disco averiado puede demandar un tiempo considerable;
- **no sustituye las copias de seguridad (backups)**.

En consecuencia, aunque RAID mejora la disponibilidad y la continuidad del servicio, siempre debe complementarse con una adecuada estrategia de copias de seguridad.

### 5.3.2. Clasificación de los niveles RAID

A lo largo del tiempo se han desarrollado diferentes niveles RAID, cada uno diseñado para satisfacer necesidades específicas de rendimiento, disponibilidad y capacidad de almacenamiento. La principal diferencia entre ellos radica en la forma en que distribuyen la información entre los discos y en los mecanismos utilizados para proteger los datos frente a fallas.

No existe un nivel RAID que resulte adecuado para todas las situaciones. La elección dependerá de factores como la importancia de la información, el rendimiento requerido, el presupuesto disponible y el nivel de disponibilidad que la organización necesite alcanzar.

### 5.3.3. RAID 0

#### 5.3.3.1. Concepto

**RAID 0** es el nivel RAID más simple y tiene como objetivo principal **incrementar el rendimiento del sistema de almacenamiento**. Para lograrlo, divide la información en bloques y los distribuye entre dos o más discos físicos. Esta técnica se conoce como **striping** o **segmentación de datos**.

Al trabajar varios discos simultáneamente, las operaciones de lectura y escritura pueden realizarse con mayor rapidez que utilizando un único disco. Sin embargo, RAID 0 **no incorpora ningún mecanismo de redundancia**, por lo que no ofrece protección frente a la falla de un disco.

## 5.3.3.2. Funcionamiento

En un arreglo RAID 0, los datos se dividen en bloques de tamaño fijo. Cada bloque se almacena de manera alternada en los diferentes discos del arreglo.

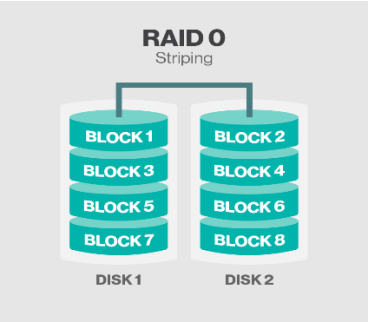
Por ejemplo, si el arreglo está compuesto por dos discos:

- el bloque 1 se almacena en el Disco A;
- el bloque 2 en el Disco B;
- el bloque 3 nuevamente en el Disco A;
- el bloque 4 en el Disco B;

y así sucesivamente.

Como ambos discos trabajan simultáneamente, es posible aumentar considerablemente la velocidad de acceso a la información.

La siguiente figura muestra el funcionamiento básico de RAID 0.




## 5.3.3.3. Ventajas

Las principales ventajas de RAID 0 son:

- incrementa la velocidad de lectura;
- incrementa la velocidad de escritura;
- aprovecha el 100 % de la capacidad de almacenamiento disponible;
- posee una implementación sencilla.

Por estas razones, RAID 0 suele utilizarse cuando el rendimiento resulta más importante que la protección de la información.

## 5.3.3.4. Desventajas

La principal desventaja de RAID 0 es que **no proporciona redundancia**.

Si cualquiera de los discos que forman parte del arreglo falla, se pierde toda la información almacenada. Esto ocurre porque cada archivo se encuentra distribuido entre todos los discos del arreglo y resulta imposible reconstruirlo cuando uno de ellos deja de funcionar.

Por este motivo, RAID 0 no debe utilizarse para almacenar información crítica sin contar con copias de seguridad.

# 5.3.3.5. Aplicaciones

RAID 0 suele utilizarse en situaciones donde el rendimiento constituye el principal objetivo y la pérdida de información no representa un problema crítico.

Algunos ejemplos son:

- edición de video;
- edición de imágenes de alta resolución;
- procesamiento multimedia;
- estaciones de trabajo para diseño gráfico;
- aplicaciones científicas que requieren gran velocidad de acceso a los datos.

En cambio, **no se recomienda** para servidores que almacenan información crítica o sistemas donde la disponibilidad de los datos sea un requisito esencial.

# 5.3.4. RAID 1
# 5.3.4.1. Concepto

**RAID 1** es un nivel RAID cuyo objetivo principal consiste en **proteger la información frente a la falla de un disco**.

Para lograrlo, almacena una copia idéntica de los datos en dos o más discos. Esta técnica recibe el nombre de **mirroring** o **espejado**. Cada vez que se escribe información en el arreglo, los mismos datos se almacenan simultáneamente en todos los discos que forman parte del sistema.

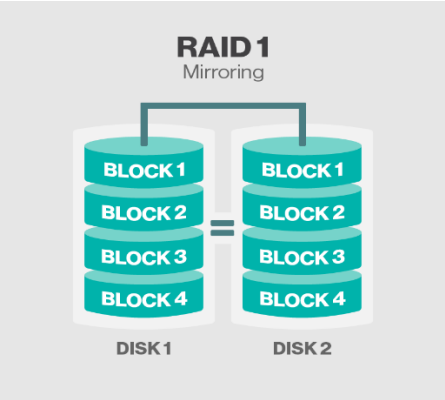
De esta manera, si uno de los discos presenta una falla, la información continua disponible en el otro disco, permitiendo que el sistema siga funcionando.

# 5.3.4.2. Funcionamiento

En un arreglo RAID 1, todos los discos contienen exactamente la misma información. Cuando el sistema escribe un archivo, este se almacena simultáneamente en ambos discos. Si uno de ellos deja de funcionar, el sistema continúa utilizando el disco restante sin pérdida de datos.

Una vez reemplazado el disco averiado, la información vuelve a copiarse automáticamente para restablecer el estado redundante del arreglo.

La siguiente figura muestra el funcionamiento general de RAID 1.




## 5.3.4.3. Ventajas

Las principales ventajas de RAID 1 son:

- proporciona redundancia completa de la información;
- permite continuar trabajando cuando falla uno de los discos;
- ofrece una elevada disponibilidad de los datos;
- facilita la recuperación después del reemplazo de un disco averiado;
- puede mejorar el rendimiento de lectura, ya que algunos controladores leen datos desde ambos discos.

Por estas características, RAID 1 es ampliamente utilizado en servidores que almacenan información crítica.

## 5.3.4.4. Desventajas

Las principales desventajas de RAID 1 son:

- requiere al menos dos discos;
- la capacidad útil de almacenamiento se reduce aproximadamente al **50 %**, ya que toda la información se encuentra duplicada;
- incrementa el costo del sistema de almacenamiento.

Por ejemplo, si el arreglo está formado por dos discos de **1 TB**, la capacidad útil disponible será aproximadamente **1 TB**, ya que el segundo disco almacena una copia exacta del primero.

## 5.3.4.5. Aplicaciones

RAID 1 resulta adecuado para sistemas donde la disponibilidad de la información es más importante que la capacidad de almacenamiento.

Algunos ejemplos son:

- servidores de bases de datos;
- servidores de archivos;
- servidores web;

- equipos que almacenan información empresarial crítica;
- pequeñas y medianas empresas que requieren continuidad del servicio.

En estos casos, la posibilidad de continuar operando después de la falla de un disco justifica el costo adicional de mantener la información duplicada.

## 5.3.5. RAID 5

### 5.3.5.1. Concepto

**RAID 5** es uno de los niveles RAID más utilizados en servidores y centros de datos porque ofrece un equilibrio entre **rendimiento**, **capacidad de almacenamiento** y **disponibilidad**.

A diferencia de RAID 1, que almacena una copia completa de la información, RAID 5 utiliza un mecanismo denominado **paridad**, que permite reconstruir los datos cuando uno de los discos presenta una falla.

Para implementar RAID 5 se requieren como mínimo **tres discos**.

### 5.3.5.2. ¿Qué es la paridad?

La **paridad** es información adicional que el sistema genera automáticamente a partir de los datos almacenados. Su función consiste en permitir la reconstrucción de la información cuando uno de los discos del arreglo deja de funcionar.

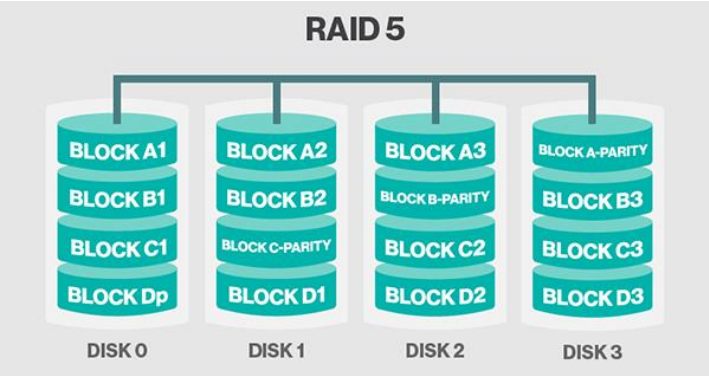
La información de paridad **no corresponde a una copia completa de los datos**, sino a un conjunto de valores matemáticos calculados a partir de los bloques almacenados en los distintos discos. Gracias a esta información, cuando un disco falla, el controlador RAID puede reconstruir temporalmente los datos faltantes utilizando la información almacenada en los demás discos y la información de paridad. En consecuencia, RAID 5 logra proteger la información utilizando menos espacio que RAID 1.

### 5.3.5.3. Funcionamiento

En RAID 5 los datos se distribuyen entre todos los discos del arreglo, de manera similar a RAID 0. Sin embargo, además de almacenar los datos, el sistema distribuye también los bloques de paridad entre los distintos discos.

Una característica importante es que la paridad **no siempre se almacena en el mismo disco**, sino que se distribuye entre todos los discos del arreglo. Esto evita que un único disco se convierta en un cuello de botella durante las operaciones de escritura.

La siguiente figura muestra un ejemplo simplificado de la distribución de datos y paridad en un arreglo RAID 5.




## 5.3.5.4. Ventajas

Las principales ventajas de RAID 5 son:

- proporciona redundancia de la información;
- permite continuar funcionando cuando falla un disco;
- aprovecha mejor la capacidad de almacenamiento que RAID 1;
- ofrece un buen rendimiento en operaciones de lectura;
- constituye un equilibrio entre rendimiento y disponibilidad.

Por estas razones, RAID 5 es uno de los niveles más utilizados en servidores empresariales.

## 5.3.5.5. Desventajas

Entre sus principales desventajas pueden mencionarse:

- requiere al menos tres discos;
- las operaciones de escritura son más lentas que en RAID 0 debido al cálculo de la paridad;
- solo puede tolerar la falla de un disco;
- durante la reconstrucción del arreglo el rendimiento disminuye considerablemente.

Si un segundo disco falla antes de finalizar la reconstrucción, la información del arreglo puede perderse.

## 5.3.5.6. Aplicaciones

RAID 5 suele utilizarse en:

- servidores de archivos;
- servidores de aplicaciones;
- pequeñas y medianas empresas;
- sistemas de almacenamiento empresarial;
- servidores donde se requiere un equilibrio entre capacidad, rendimiento y disponibilidad.

No suele recomendarse para aplicaciones con una gran cantidad de operaciones de escritura intensiva, ya que el cálculo de la paridad puede afectar el rendimiento.

## 5.3.6. RAID 6

### 5.3.6.1. Concepto

**RAID 6** es una evolución de RAID 5 que incorpora un mayor nivel de protección frente a fallas de discos. Al igual que RAID 5, distribuye la información entre varios discos y utiliza información de paridad para reconstruir los datos cuando ocurre una falla. Sin embargo, RAID 6 almacena **dos bloques de paridad**, lo que le permite continuar funcionando incluso cuando fallan **dos discos simultáneamente**.

Para implementar un arreglo RAID 6 se requieren como mínimo **cuatro discos**.

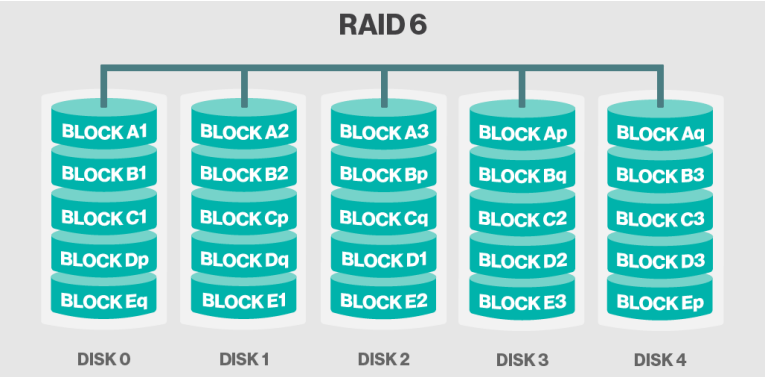
Gracias a esta característica, RAID 6 ofrece un mayor nivel de disponibilidad y confiabilidad que RAID 5, siendo especialmente adecuado para sistemas donde la pérdida de información resulta inaceptable.

### 5.3.6.2. Funcionamiento

En RAID 6, los datos y la información de paridad se distribuyen entre todos los discos del arreglo. La principal diferencia respecto de RAID 5 es que el sistema genera **dos bloques de paridad independientes**, permitiendo reconstruir la información aun cuando dos discos presenten fallas al mismo tiempo.

Cuando un disco deja de funcionar, el controlador RAID utiliza los bloques de datos restantes junto con la información de paridad para reconstruir temporalmente la información faltante. Si durante ese proceso falla un segundo disco, RAID 6 todavía dispone de suficiente información para continuar operando.

La siguiente figura muestra de manera simplificada la distribución de datos y doble paridad en un arreglo RAID 6.




### 5.3.6.3. Ventajas

Las principales ventajas de RAID 6 son:

- tolera la falla simultánea de **dos discos**;
- ofrece un elevado nivel de disponibilidad;
- proporciona mayor seguridad para la información que RAID 5;
- resulta especialmente adecuado para arreglos con gran cantidad de discos;
- reduce el riesgo de pérdida de información durante la reconstrucción del arreglo.

Estas características convierten a RAID 6 en una alternativa ampliamente utilizada en servidores de almacenamiento de gran capacidad.

# 5.3.6.4. Desventajas

Entre sus principales desventajas pueden mencionarse:

- requiere al menos cuatro discos;
- disminuye la capacidad útil debido al espacio ocupado por la doble paridad;
- las operaciones de escritura son más lentas que en RAID 5, ya que deben calcularse dos bloques de paridad;
- presenta un mayor costo de implementación.

En consecuencia, RAID 6 suele utilizarse cuando la disponibilidad resulta más importante que el rendimiento de escritura.

# 5.3.6.5. Aplicaciones

RAID 6 se utiliza principalmente en sistemas donde la disponibilidad de la información constituye un requisito crítico.

Algunos ejemplos son:

- centros de cómputos;
- servidores de almacenamiento masivo;
- sistemas de respaldo empresarial;
- infraestructuras de virtualización;
- organizaciones que administran grandes volúmenes de información.

En estos entornos, la posibilidad de soportar la falla simultánea de dos discos representa una ventaja significativa frente a RAID 5.

# 5.3.7. RAID 10 (1+0)
# 5.3.7.1. Concepto

**RAID 10**, también denominado **RAID 1+0**, es un nivel RAID que combina las características de **RAID 1 (mirroring)** y **RAID 0 (striping)**.

Su objetivo consiste en ofrecer simultáneamente:

- un elevado rendimiento;
- alta disponibilidad de la información;

- tolerancia a fallos.

Para ello, primero duplica la información mediante RAID 1 y posteriormente distribuye los datos entre los distintos pares de discos utilizando RAID 0. De esta forma, RAID 10 aprovecha las ventajas de ambos niveles: la velocidad proporcionada por RAID 0 y la redundancia ofrecida por RAID 1.

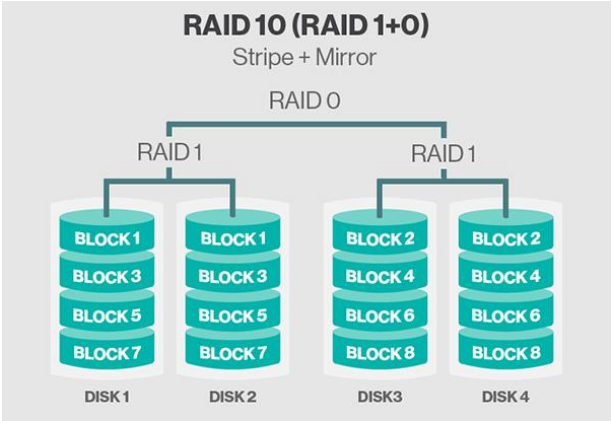
Para implementar un arreglo RAID 10 se requieren como mínimo **cuatro discos**.

## 5.3.7.2. Funcionamiento

En un arreglo RAID 10, los discos se agrupan inicialmente en pares configurados mediante **RAID 1**, donde cada disco posee una copia idéntica de la información almacenada en su par. Posteriormente, estos pares se combinan utilizando **RAID 0**, distribuyendo la información entre ellos para incrementar el rendimiento.

El resultado es un sistema que permite realizar operaciones de lectura y escritura a gran velocidad sin renunciar a la protección de los datos.

La siguiente figura muestra un esquema simplificado de un arreglo RAID 10.




## 5.3.7.3. Ventajas

Las principales ventajas de RAID 10 son:

- excelente rendimiento en lectura y escritura;
- elevada disponibilidad de la información;
- rápida recuperación ante la falla de un disco;
- buena tolerancia a fallos;
- reconstrucción más sencilla que en RAID 5 o RAID 6.

Estas características convierten a RAID 10 en una de las configuraciones más utilizadas en aplicaciones críticas.

## 5.3.7.4. Desventajas

Entre sus principales desventajas pueden mencionarse:

- requiere al menos cuatro discos;
- el costo de implementación es elevado;
- solo se aprovecha aproximadamente el **50 %** de la capacidad total de almacenamiento debido a la duplicación de la información.

Por ejemplo, un arreglo formado por cuatro discos de **2 TB** proporciona una capacidad útil aproximada de **4 TB**.

## 5.3.7.5. Aplicaciones

RAID 10 suele utilizarse en sistemas donde resulta necesario combinar un alto rendimiento con una elevada disponibilidad de la información.

Entre sus aplicaciones más habituales se encuentran:

- servidores de bases de datos;
- servidores de virtualización;
- sistemas transaccionales;
- plataformas de comercio electrónico;
- aplicaciones financieras;
- centros de datos con alta demanda de operaciones de lectura y escritura.

En este tipo de aplicaciones, una interrupción del servicio o una pérdida de rendimiento puede generar importantes consecuencias económicas.

## 5.3.8. Comparación entre los principales niveles RAID

Una vez estudiados los principales niveles RAID, resulta útil compararlos para identificar rápidamente sus diferencias en cuanto a rendimiento, disponibilidad, capacidad útil y tolerancia a fallos.

La siguiente tabla resume las características más importantes de cada nivel RAID y constituye una guía para seleccionar la alternativa más adecuada según las necesidades de una organización.

| **Característica** | **RAID 0** | **RAID 1** | **RAID 5** | **RAID 6** | **RAID 10** |
|---|---|---|---|---|---|
| Objetivo principal | Rendimiento | Disponibilidad | Equilibrio entre rendimiento y disponibilidad | Alta disponibilidad | Alto rendimiento y alta disponibilidad |
| Cantidad mínima de discos | 2 | 2 | 3 | 4 | 4 |
| Redundancia | No | Sí | Sí | Sí | Sí |

| Característica | RAID 0 | RAID 1 | RAID 5 | RAID 6 | RAID 10 |
|---|---|---|---|---|---|
| Mecanismo de protección | Ninguno | Espejado (Mirroring) | Paridad distribuida | Doble paridad distribuida | Espejado + Striping |
| Capacidad útil aproximada | 100 % | 50 % | (n−1)/n | (n−2)/n | 50 % |
| Tolera la falla de | Ningún disco | 1 disco | 1 disco | 2 discos | Depende del arreglo* |
| Rendimiento de lectura | Muy alto | Alto | Alto | Alto | Muy alto |
| Rendimiento de escritura | Muy alto | Medio | Medio | Medio-Bajo | Muy alto |
| Costo | Bajo | Medio | Medio | Alto | Alto |

* En RAID 10 la cantidad de discos que pueden fallar depende de qué discos presenten la avería. En determinadas configuraciones pueden fallar varios discos sin perder la información, siempre que no pertenezcan al mismo par de espejado.

### 5.3.9. Recomendaciones según el tipo de aplicación

La siguiente tabla presenta algunos ejemplos de utilización de los distintos niveles RAID.

| Tipo de aplicación | Nivel RAID recomendado | Justificación |
|---|---|---|
| Edición de video e imágenes | RAID 0 | Máximo rendimiento. |
| Computadora personal con información importante | RAID 1 | Protección sencilla mediante duplicación de datos. |
| Servidor de archivos | RAID 5 | Buen equilibrio entre capacidad y disponibilidad. |
| Centro de datos empresarial | RAID 6 | Mayor tolerancia a fallas. |
| Servidor de bases de datos | RAID 10 | Alto rendimiento y elevada disponibilidad. |
| Plataforma de virtualización | RAID 10 | Excelente desempeño en lectura y escritura. |

Como puede observarse, ningún nivel RAID resulta adecuado para todas las situaciones. La elección dependerá del equilibrio que la organización desee alcanzar entre rendimiento, disponibilidad, capacidad de almacenamiento y costo de implementación. Asimismo, debe recordarse que ningún nivel RAID reemplaza la realización de copias de seguridad, ya que protege frente a fallas de hardware, pero no frente a errores humanos, ataques informáticos o desastres.

## 5.4. Copias de Seguridad (Backups)

La disponibilidad de la información no depende únicamente de que los sistemas continúen funcionando cuando ocurre una falla de hardware. También es necesario garantizar que los datos puedan recuperarse cuando son eliminados accidentalmente, modificados de forma incorrecta o afectados por incidentes de seguridad.

En los apartados anteriores se estudió cómo las tecnologías RAID permiten aumentar la disponibilidad y la tolerancia a fallos de los dispositivos de almacenamiento. Sin embargo, **RAID no protege frente a todos los tipos de incidentes**.

Por ejemplo, RAID no evita la pérdida de información cuando:

- un usuario elimina accidentalmente un archivo;
- un ransomware cifra toda la información;
- una aplicación corrompe una base de datos;
- ocurre un incendio o una inundación;
- un error humano modifica información importante.

Para afrontar este tipo de situaciones resulta indispensable realizar **copias de seguridad**, conocidas también como **backups**. Las copias de seguridad constituyen uno de los controles de seguridad más importantes para garantizar la continuidad de las operaciones y la recuperación de la información.

## 5.4.1. Concepto de Backup

Un **backup** o **copia de seguridad** es una copia de la información que se almacena en un medio diferente al original con el objetivo de poder recuperarla cuando los datos originales se pierden, resultan dañados o dejan de estar disponibles.

El objetivo principal de un backup es permitir que la organización pueda restaurar la información después de un incidente, reduciendo las pérdidas económicas y minimizando el tiempo de interrupción de las actividades. En términos simples, un backup constituye una "segunda copia" de los datos importantes.

Esta copia debe mantenerse protegida y separada de la información original para que pueda utilizarse cuando sea necesario.

## 5.4.2. Objetivos de las Copias de Seguridad

Las copias de seguridad persiguen diversos objetivos relacionados con la protección de la información.

Entre los principales pueden mencionarse:

- recuperar información eliminada accidentalmente;
- restaurar archivos dañados o corrompidos;
- recuperar información después de un ataque informático;
- minimizar la pérdida de datos ante fallas de hardware;
- garantizar la continuidad de las operaciones;
- cumplir requisitos legales o normativos relacionados con la conservación de información.

En consecuencia, una estrategia de copias de seguridad constituye un componente esencial dentro de cualquier sistema de gestión de la seguridad de la información.

## 5.4.3. ¿Qué información debe respaldarse?

No toda la información posee el mismo valor para la organización. Por este motivo, antes de definir una estrategia de respaldo resulta necesario identificar cuáles son los datos cuya pérdida tendría un impacto significativo sobre las actividades de la organización.

Generalmente deben incluirse en las copias de seguridad:

- bases de datos;
- documentos institucionales;
- archivos de configuración de servidores;
- aplicaciones críticas;
- información de clientes y proveedores;
- registros contables;
- correos electrónicos institucionales;
- máquinas virtuales;
- sistemas de gestión.

En cambio, archivos temporales o información fácilmente recuperable normalmente no requieren ser incluidos en todas las copias de seguridad. La selección de la información a respaldar debe realizarse considerando el valor de los activos de información estudiado en la Unidad 4.

## 5.4.4. Importancia de los Backups en la Seguridad Informática

Las copias de seguridad representan uno de los mecanismos más efectivos para reducir el impacto de numerosos incidentes de seguridad. Su importancia quedó demostrada en los últimos años con el incremento de los ataques de ransomware, donde los delincuentes cifran la información de la organización y exigen el pago de un rescate para recuperarla.

Cuando la organización dispone de copias de seguridad actualizadas y correctamente protegidas, puede restaurar la información sin depender del atacante.

Asimismo, los backups permiten recuperarse de:

- errores humanos;
- fallas de hardware;
- errores de software;
- desastres naturales;
- sabotajes;
- incidentes de ciberseguridad.

Por este motivo, prácticamente todas las normas y metodologías de seguridad de la información consideran a las copias de seguridad como un control fundamental para garantizar la disponibilidad de la información.

## 5.4.5. RAID y Backups: diferencias

Es frecuente pensar que la utilización de RAID elimina la necesidad de realizar copias de seguridad. Esta idea es incorrecta. Aunque ambas tecnologías contribuyen a la disponibilidad de la información, cumplen funciones diferentes.

La siguiente tabla resume sus principales diferencias.

| RAID | Backup |
|---|---|
| Protege frente a fallas de discos. | Protege frente a pérdida o corrupción de la información. |
| Permite continuar funcionando cuando falla un disco. | Permite restaurar información perdida. |
| Mejora la disponibilidad del servicio. | Garantiza la recuperación de los datos. |
| No protege frente a ransomware ni eliminación accidental. | Permite recuperar información afectada por estos incidentes. |
| No reemplaza las copias de seguridad. | Complementa el uso de RAID. |

En una infraestructura informática moderna, ambas tecnologías deben utilizarse de manera complementaria para garantizar la disponibilidad y la recuperación de la información.

## 5.4.6. Tipos de Copias de Seguridad

Las organizaciones generan grandes volúmenes de información que cambian constantemente. Realizar una copia completa de todos los datos cada vez que se ejecuta un respaldo puede consumir mucho tiempo y espacio de almacenamiento.

Por este motivo existen distintos tipos de copias de seguridad, cada uno diseñado para equilibrar aspectos como:

- el tiempo necesario para realizar el respaldo;
- el espacio de almacenamiento utilizado;
- la velocidad de recuperación de la información;
- la complejidad del proceso de restauración.

Los tipos de copias de seguridad más utilizados son:

- **Backup completo (Full Backup).**
- **Backup incremental (Incremental Backup).**
- **Backup diferencial (Differential Backup).**

Cada uno presenta ventajas y desventajas, por lo que la elección dependerá de las necesidades de cada organización.

## 5.4.6.1. Backup Completo (Full Backup)

El **backup completo** consiste en copiar todos los archivos seleccionados, independientemente de si fueron modificados desde la última copia de seguridad.

Cada vez que se ejecuta un backup completo se genera una copia íntegra de toda la información.

# Ejemplo

Supóngase una carpeta que contiene los siguientes archivos:

```
Clientes.xlsx
Ventas.xlsx
Facturación.pdf
Empleados.docx
```

Si el lunes se realiza un backup completo, los cuatro archivos serán copiados. Si el martes únicamente cambia **Ventas.xlsx**, al realizar nuevamente un backup completo volverán a copiarse los cuatro archivos.

# Ventajas

- recuperación muy sencilla;
- restauración rápida;
- cada copia es independiente;
- no depende de backups anteriores.

# Desventajas

- requiere mayor espacio de almacenamiento;
- demanda mayor tiempo para realizar cada copia;
- consume mayor ancho de banda cuando el respaldo se realiza por red.

# Aplicaciones

Generalmente se utiliza:

- como primer backup;
- periódicamente (por ejemplo, una vez por semana);
- cuando el volumen de información es reducido.

## 5.4.6.2. Backup Incremental (Incremental Backup)

El **backup incremental** únicamente copia los archivos que fueron modificados desde el último backup realizado, independientemente de si éste fue completo o incremental.

De esta forma, cada respaldo incremental contiene solamente los cambios realizados desde la copia anterior.

# Ejemplo

Supóngase el siguiente escenario.

| Día | Información modificada | Backup generado |
|---|---|---|
| Lunes | Todos los archivos | Completo |
| Martes | Ventas | Incremental |
| Miércoles | Clientes y Facturación | Incremental |
| Jueves | Empleados | Incremental |

Al finalizar el jueves existirán las siguientes copias:

```
Completo (Lunes)

Incremental (Martes)

Incremental (Miércoles)

Incremental (Jueves)
```

# Restauración

Si se desea restaurar la información al estado correspondiente al miércoles será necesario disponer de:

- Backup completo del lunes.
- Backup incremental del martes.
- Backup incremental del miércoles.

Obsérvese que cada backup incremental depende de todos los anteriores. Si alguno de ellos se pierde o resulta dañado, la restauración no podrá completarse correctamente.

# Ventajas

- ocupa poco espacio de almacenamiento;
- las copias son muy rápidas;
- reduce el tráfico de red;
- permite mantener un historial detallado de los cambios realizados entre respaldos.

# Desventajas

- la restauración resulta más lenta;
- requiere conservar toda la cadena de backups;
- si falta uno de los backups incrementales, la recuperación puede quedar incompleta.

# Aplicaciones

Se utiliza cuando:

- la información cambia constantemente;
- el espacio disponible es limitado;
- se realizan respaldos diarios.

# 5.4.6.3. Backup Diferencial (Differential Backup)

El **backup diferencial** copia todos los archivos modificados desde el último backup completo.

A diferencia del backup incremental, no toma como referencia el último respaldo realizado, sino siempre el último backup completo. Por este motivo, el tamaño de los backups diferenciales aumenta con el paso de los días.

# Ejemplo

Supóngase el siguiente escenario.

| Día | Información modificada | Backup generado |
|---|---|---|
| Lunes | Todos los archivos | Completo |
| Martes | Ventas | Diferencial |
| Miércoles | Clientes | Diferencial |
| Jueves | Empleados | Diferencial |

Al finalizar el jueves existirán las siguientes copias:

```
Completo (Lunes)

Diferencial (Martes)

Diferencial (Miércoles)

Diferencial (Jueves)
```

El backup diferencial del miércoles contiene:

- los cambios realizados el martes;
- más los cambios realizados el miércoles.

El backup diferencial del jueves contiene:

- los cambios del martes;
- los cambios del miércoles;
- los cambios del jueves.

Cada nuevo backup diferencial incorpora todos los cambios producidos desde el último backup completo.

# Restauración

Si se desea restaurar la información al estado correspondiente al miércoles únicamente será necesario disponer de:

- Backup completo del lunes.
- Backup diferencial del miércoles.

A diferencia del backup incremental, no es necesario utilizar las copias diferenciales de los días anteriores.

# Importante

En muchas organizaciones únicamente se conserva el **backup diferencial más reciente**, ya que contiene todos los cambios realizados desde el último backup completo.

Sin embargo, cuando se desea conservar distintas versiones históricas de la información, pueden almacenarse varios backups diferenciales correspondientes a diferentes fechas. **En este caso, es posible restaurar la información al estado correspondiente a cualquiera de esas fechas**, de manera similar a lo que ocurre con los backups incrementales, siempre que se conserven los backups diferenciales de los días que se desean recuperar.

La diferencia principal es que, para restaurar una fecha determinada, el backup diferencial solo requiere el **backup completo** y el **backup diferencial correspondiente a esa fecha**, mientras que el backup incremental necesita el backup completo y toda la cadena de backups incrementales realizada hasta ese momento.

# Ventajas

- recuperación más sencilla que el backup incremental;
- menor cantidad de copias necesarias para restaurar la información;
- permite recuperar fácilmente la información correspondiente a cualquiera de las fechas para las cuales se conserve un backup diferencial.

## Desventajas

- cada día ocupa más espacio;
- las copias son más lentas que las incrementales;
- consume más almacenamiento a medida que transcurren los días.

## Aplicaciones

Se utiliza cuando se busca un equilibrio entre:

- velocidad del respaldo;
- rapidez de restauración;
- utilización del espacio de almacenamiento.

# 5.4.6.4. Comparación entre los tipos de Backup

La siguiente tabla resume las principales diferencias entre los tres tipos de copias de seguridad.

| Característica | Completo | Incremental | Diferencial |
|---|---|---|---|
| Información copiada | Todos los archivos | Archivos modificados desde el último backup | Archivos modificados desde el último backup completo |
| Tiempo de realización | Alto | Bajo | Medio |
| Espacio requerido | Alto | Bajo | Medio |
| Velocidad de recuperación | Alta | Baja | Media-Alta |
| Cantidad de backups necesarios para restaurar | Uno | Completo + todos los incrementales | Completo + diferencial deseado |
| Complejidad de restauración | Baja | Alta | Media |

# 5.4.6.5. ¿Qué tipo de Backup conviene utilizar?

No existe un único tipo de backup adecuado para todas las organizaciones.

La elección dependerá de:

- el volumen de información;
- la frecuencia con que cambian los datos;

- el espacio disponible;
- el tiempo máximo aceptable para recuperar la información.

En la práctica es habitual combinar distintos tipos de copias de seguridad.

Por ejemplo:

- realizar un **backup completo** cada domingo;
- realizar **backups incrementales** o **diferenciales** durante el resto de la semana.

De esta manera se logra un equilibrio entre el tiempo de realización de las copias, el espacio utilizado y la rapidez de recuperación.

## 5.4.7. Estrategia de Respaldo 3-2-1

Realizar copias de seguridad constituye una medida fundamental para proteger la información de una organización. Sin embargo, no basta con efectuar respaldos de manera periódica; también es necesario definir **cómo** y **dónde** serán almacenadas dichas copias.

Una estrategia inadecuada puede provocar que todas las copias de seguridad se pierdan simultáneamente ante un mismo incidente, como un incendio, un robo, un ataque de ransomware o una falla del dispositivo de almacenamiento.

Con el objetivo de reducir este riesgo, una de las recomendaciones más difundidas en el ámbito de la seguridad informática es la denominada **regla 3-2-1**, considerada una buena práctica para la gestión de copias de seguridad.

## 5.4.7.1. ¿Qué es la regla 3-2-1?

La **regla 3-2-1** establece que una organización debería mantener:

- **3 copias de la información**;
- almacenadas en **2 medios diferentes**;
- manteniendo **1 copia fuera del sitio principal**.

Esta estrategia incrementa considerablemente la probabilidad de recuperar la información después de un incidente.

## 5.4.7.2. Los tres principios de la regla 3-2-1

## Tres copias de la información

La organización debe disponer de:

- la información original;
- una primera copia de seguridad;
- una segunda copia de seguridad.

De esta manera, si una de las copias resulta dañada o se pierde, todavía existirán otras disponibles para recuperar la información.

## Dos medios de almacenamiento diferentes

Las copias no deberían almacenarse todas en el mismo tipo de dispositivo.

Por ejemplo:

- disco rígido interno;
- disco rígido externo;
- servidor NAS;
- cintas magnéticas;
- almacenamiento en la nube.

La utilización de distintos medios reduce la probabilidad de que una falla tecnológica afecte simultáneamente todas las copias.

## Una copia fuera del sitio

Al menos una de las copias debe almacenarse en una ubicación física distinta de donde se encuentran los datos originales.

Esta copia puede mantenerse:

- en otra sucursal;
- en un centro de cómputos;
- en un servicio de almacenamiento en la nube;
- en una caja de seguridad.

El objetivo consiste en proteger la información frente a incidentes que afecten completamente las instalaciones de la organización, tales como:

- incendios;
- inundaciones;
- robos;
- desastres naturales.

## 5.4.7.3. Ejemplo de aplicación

Supóngase una empresa que almacena toda su información en un servidor ubicado en sus oficinas.

Una posible implementación de la regla 3-2-1 podría ser la siguiente:

| Copia | Medio de almacenamiento | Ubicación |
|---|---|---|
| Original | Servidor principal | Oficina |
| Primera copia | NAS o disco externo | Oficina |
| Segunda copia | Servicio de almacenamiento en la nube | Centro de datos externo |

En este ejemplo, aunque el edificio sufriera un incendio o un robo, la organización conservaría una copia segura de su información en la nube.

# 5.4.7.4. Ventajas de la regla 3-2-1

Entre sus principales beneficios pueden mencionarse:

- reduce significativamente el riesgo de pérdida total de información;
- protege frente a fallas de hardware;
- protege frente a errores humanos;
- facilita la recuperación después de ataques de ransomware;
- incrementa la continuidad operativa de la organización;
- constituye una buena práctica recomendada por numerosos organismos internacionales.

Por estas razones, muchas organizaciones adoptan la regla 3-2-1 como política básica para la gestión de sus copias de seguridad.

# 5.4.7.5. Limitaciones

Aunque la regla 3-2-1 proporciona un elevado nivel de protección, no garantiza por sí sola la recuperación de la información.

También resulta necesario:

- verificar periódicamente la integridad de las copias de seguridad;
- realizar pruebas de restauración;
- proteger las copias mediante mecanismos de cifrado cuando contienen información sensible;
- definir políticas de actualización y conservación de los respaldos.

Una copia de seguridad que nunca fue probada podría resultar inutilizable cuando realmente sea necesaria.

# 5.4.8. Medios de Almacenamiento para Copias de Seguridad

Una vez definida la estrategia de respaldo, la organización debe decidir dónde almacenará las copias de seguridad. El medio de almacenamiento influye directamente en aspectos

como el costo, la velocidad de recuperación, la capacidad disponible y el nivel de protección frente a distintos incidentes.

Los medios más utilizados actualmente son:

- discos rígidos externos;
- servidores NAS (Network Attached Storage), dispositivo de almacenamiento conectado a la red que permite almacenar y compartir información entre múltiples usuarios y equipos;
- cintas magnéticas;
- almacenamiento en la nube.

Cada uno presenta ventajas y limitaciones, por lo que muchas organizaciones utilizan una combinación de ellos para mejorar la disponibilidad y la seguridad de la información.

## 5.4.8.1. Comparación de los principales medios de almacenamiento

La siguiente tabla muestra una comparación de medios para copias de seguridad

| Medio | Ventajas | Desventajas | Uso recomendado |
|---|---|---|---|
| **Disco externo** | Bajo costo, portátil, rápido | Puede dañarse o perderse fácilmente | Usuarios y pequeñas empresas |
| **Servidor NAS** | Compartido, gran capacidad, automatización | Mayor costo y requiere administración | Empresas y oficinas |
| **Cintas magnéticas** | Muy alta capacidad y larga vida útil | Acceso lento y equipamiento específico | Grandes organizaciones |
| **Almacenamiento en la nube** | Copia fuera del sitio, alta disponibilidad | Depende de Internet y tiene costo periódico | Todo tipo de organizaciones |

---

## 5.4.8.2. Recomendaciones

La elección del medio dependerá del volumen de información, del presupuesto disponible y del tiempo máximo aceptable para recuperar los datos.

En la práctica es habitual combinar varios medios de almacenamiento. Por ejemplo:

- una copia local en un servidor NAS para restauraciones rápidas;
- una copia externa en la nube para proteger la información frente a incendios, robos o desastres naturales.

Esta estrategia resulta compatible con la **regla 3-2-1**, estudiada en el apartado anterior.

## 5.5. Recuperación de la Información

Realizar copias de seguridad constituye una medida fundamental para proteger la información. Sin embargo, un backup solo resulta útil si puede restaurarse correctamente cuando ocurre un incidente.

La **recuperación de la información** consiste en restaurar los datos almacenados en una copia de seguridad para devolver un sistema a un estado operativo después de una pérdida, corrupción o indisponibilidad de la información. El objetivo principal es reducir el impacto del incidente y permitir que la organización reanude sus actividades lo antes posible.

### 5.5.1. ¿Cuándo es necesario recuperar información?

La restauración de una copia de seguridad puede ser necesaria en situaciones como:

- eliminación accidental de archivos;
- fallas de hardware;
- corrupción de bases de datos;
- errores de software;
- ataques de ransomware;
- desastres naturales;
- errores humanos.

En todos estos casos, disponer de copias de seguridad actualizadas permite recuperar la información y reducir las pérdidas ocasionadas por el incidente.

### 5.5.2. Importancia de verificar las copias de seguridad

Uno de los errores más frecuentes consiste en asumir que una copia de seguridad podrá restaurarse correctamente sin haber realizado pruebas previas.

Las copias pueden resultar inutilizables debido a:

- errores durante el proceso de respaldo;
- daños en el medio de almacenamiento;
- corrupción de archivos;
- fallas del software de backup.

Por este motivo, las organizaciones deben realizar **pruebas periódicas de restauración** para comprobar que las copias son válidas y que el procedimiento de recuperación funciona correctamente.

Una copia de seguridad que nunca fue probada no garantiza que la información pueda recuperarse cuando sea realmente necesaria.

## 5.6. Continuidad del Negocio

Las organizaciones dependen cada vez más de sus sistemas informáticos para desarrollar sus actividades diarias. Una interrupción prolongada de estos servicios puede provocar pérdidas económicas, incumplimiento de obligaciones legales y afectar la confianza de clientes y proveedores. Por este motivo, además de proteger la información y realizar copias de seguridad, resulta necesario planificar cómo continuar operando cuando ocurre un incidente.

La **continuidad del negocio** reúne el conjunto de políticas, procedimientos y recursos destinados a garantizar que los procesos críticos de una organización continúen funcionando o puedan restablecerse en un tiempo aceptable después de un incidente.

Su objetivo principal consiste en:

- garantizar la disponibilidad de los servicios esenciales;
- reducir el tiempo de interrupción de las operaciones;
- minimizar las pérdidas económicas;
- proteger la información crítica;
- asegurar la continuidad de los procesos más importantes de la organización.

La continuidad del negocio no busca evitar que ocurran incidentes, sino preparar a la organización para responder adecuadamente cuando éstos se producen.

### 5.6.1. Relación con la Seguridad Informática

La continuidad del negocio forma parte de la gestión de la seguridad de la información.

Los controles estudiados anteriormente en esta unidad —como la redundancia, los sistemas RAID y las copias de seguridad— contribuyen directamente a mantener la disponibilidad de la información y facilitar la recuperación de los servicios.

Sin embargo, la continuidad del negocio posee un alcance más amplio, ya que considera no solo los recursos tecnológicos, sino también las personas, los procesos y la infraestructura necesaria para que la organización continúe operando.

### 5.6.2. Elementos de un programa de Continuidad del Negocio

Un programa de continuidad del negocio suele incluir:

- identificación de los procesos críticos;
- análisis de los riesgos que pueden afectar su funcionamiento;
- definición de estrategias para mantener la operación;
- procedimientos para responder ante incidentes;
- asignación de responsables;
- realización de pruebas y actualizaciones periódicas.

Estos elementos permiten que la organización actúe de manera planificada y coordinada cuando ocurre una situación que compromete el normal funcionamiento de sus actividades.

### 5.6.3. Relación con el Plan de Contingencia y la Recuperación ante Desastres

La continuidad del negocio constituye el marco general dentro del cual se desarrollan otros planes específicos.

Entre ellos se destacan:

- **Plan de Contingencia**, que establece las acciones inmediatas para responder a un incidente y mantener operativos los procesos críticos.
- **Plan de Recuperación ante Desastres (Disaster Recovery Plan)**, orientado a restaurar la infraestructura tecnológica y los sistemas de información después de un evento grave.

## 5.7. Plan de Contingencia

Un **Plan de Contingencia** es un documento que establece los procedimientos, responsabilidades y recursos necesarios para responder ante incidentes que puedan afectar el funcionamiento normal de la organización.

Su finalidad es mantener operativos los procesos críticos o restablecerlos en el menor tiempo posible, reduciendo el impacto sobre las actividades de la organización.

### 5.7.1. Objetivos del Plan de Contingencia

Un plan de contingencia busca:

- minimizar el impacto de los incidentes;
- proteger a las personas y los activos de la organización;
- mantener operativos los procesos críticos;
- reducir el tiempo de interrupción de los servicios;
- facilitar una recuperación rápida y ordenada.

El objetivo no consiste únicamente en recuperar los sistemas informáticos, sino en garantizar la continuidad de las actividades esenciales de la organización.

### 5.7.2. Etapas para la elaboración de un Plan de Contingencia

La elaboración de un plan de contingencia requiere seguir una serie de etapas que permitan identificar los riesgos, definir las acciones necesarias y documentar los procedimientos que deberán ejecutarse durante una emergencia.

Aunque cada organización puede adaptar este proceso a sus necesidades, generalmente comprende las siguientes etapas.

#### 5.7.2.1. 1. Definir el alcance del plan

El primer paso consiste en determinar qué áreas, procesos o servicios estarán comprendidos dentro del plan de contingencia. El alcance puede abarcar toda la organización o únicamente los procesos considerados críticos.

En esta etapa también se establecen los objetivos del plan y las personas responsables de su elaboración.

#### 5.7.2.2. 2. Identificar los procesos críticos

Se determinan las actividades esenciales para el funcionamiento de la organización. Estos procesos serán los primeros que deberán mantenerse operativos o recuperarse durante una contingencia.

#### 5.7.2.3. 3. Analizar los riesgos

Se identifican las amenazas y vulnerabilidades que pueden afectar los procesos críticos, evaluando las posibles consecuencias sobre la organización. Este análisis permite conocer qué situaciones deben contemplarse en el plan.

#### 5.7.2.4. 4. Definir las estrategias de respuesta

Para cada riesgo identificado se establecen las acciones que permitirán reducir el impacto del incidente y garantizar la continuidad de las operaciones.

Estas estrategias pueden incluir:

- utilización de equipos redundantes;
- restauración de copias de seguridad;
- utilización de sitios alternativos;
- reasignación temporal de funciones;
- procedimientos manuales de operación.

#### 5.7.2.5. 5. Elaborar los procedimientos

Una vez definidas las estrategias, se documentan los procedimientos que deberán seguirse durante una contingencia.

Estos procedimientos deben indicar claramente:

- las actividades a realizar;
- los responsables de cada tarea;
- los recursos necesarios;
- el orden en que deben ejecutarse las acciones.

El objetivo es que cualquier integrante del equipo pueda actuar correctamente aún bajo situaciones de presión.

### 5.7.2.6. 6. Realizar pruebas y mantener actualizado el plan

Un plan de contingencia solo resulta efectivo si puede ejecutarse correctamente cuando ocurre un incidente. Por este motivo, la organización debe realizar simulacros y pruebas periódicas para verificar su funcionamiento.

Asimismo, el plan debe actualizarse cuando se produzcan cambios importantes en:

- la infraestructura tecnológica;
- los procesos de negocio;
- el personal responsable;
- los sistemas de información;
- los riesgos identificados.

Un plan que nunca fue probado o que permanece desactualizado puede resultar ineficaz durante una emergencia real.

## 5.7.3. Importancia del Plan de Contingencia

Contar con un plan de contingencia proporciona múltiples beneficios para la organización, entre ellos:

- reduce el tiempo de interrupción de los servicios;
- disminuye las pérdidas económicas ocasionadas por incidentes;
- mejora la coordinación entre los distintos equipos de trabajo;
- facilita la toma de decisiones durante situaciones de emergencia;
- protege la información y los activos críticos;
- incrementa la capacidad de recuperación de la organización.

La elaboración del plan no garantiza que los incidentes no ocurran, pero sí permite enfrentarlos de manera organizada y eficiente.

## 5.7.4. Caso Práctico: Elaboración de un Plan de Contingencia

A continuación, se presenta un ejemplo sencillo que muestra cómo aplicar las etapas estudiadas para elaborar un Plan de Contingencia.

### 5.7.4.1. Situación

La empresa **TecnoSol S.A.** posee aproximadamente 40 empleados y desarrolla sistemas de gestión para pequeñas empresas.

Su infraestructura informática está compuesta por:

- un servidor principal donde funcionan las bases de datos;
- un servidor NAS utilizado para realizar copias de seguridad;
- veinte computadoras para el personal administrativo y técnico;
- conexión permanente a Internet.

La empresa brinda soporte técnico durante el horario comercial, por lo que una interrupción prolongada de sus sistemas afectaría directamente la atención a los clientes y el desarrollo de sus actividades.

La dirección decide elaborar un **Plan de Contingencia** para responder adecuadamente ante incidentes que puedan comprometer el funcionamiento de la organización.

## 5.7.4.2. Paso 1. Definir el alcance

El plan comprenderá los recursos tecnológicos y los procesos considerados esenciales para el funcionamiento de la empresa.

Se incluyen:

- servidor principal;
- servidor NAS;
- red informática;
- sistema de atención a clientes;
- servicio de correo electrónico corporativo.

## 5.7.4.3. Paso 2. Identificar los procesos críticos

Luego de analizar el funcionamiento de la organización, se determinan como procesos críticos:

- acceso a la base de datos;
- atención de clientes;
- desarrollo de software;
- correo electrónico corporativo.

Estos procesos deberán mantenerse operativos o recuperarse prioritariamente durante una contingencia.

## 5.7.4.4. Paso 3. Analizar los riesgos

Utilizando la metodología estudiada en la **Unidad 4**, se identifican los activos críticos, las amenazas que pueden afectarlos y las vulnerabilidades existentes.

A partir de esta información se determinan los riesgos que deberán contemplarse en el Plan de Contingencia.

Ejemplo simplificado de identificación de riesgos

| Activo | Amenaza | Vulnerabilidad | Riesgo identificado |
|---|---|---|---|
| Servidor principal | Corte del suministro eléctrico | No dispone de UPS | Interrupción del servicio y posible pérdida de información |
| Base de datos | Ataque de ransomware | Antivirus desactualizado | Información cifrada e indisponibilidad del sistema |
| Sala de servidores | Incendio | No posee sistema automático contra incendios | Destrucción de la infraestructura informática |
| Red informática | Falla del switch principal | No existe equipo de reemplazo | Interrupción de las comunicaciones internas |

**Importante:** el riesgo no es la amenaza en sí misma. El riesgo surge cuando una amenaza puede afectar a un activo aprovechando una vulnerabilidad existente y producir consecuencias para la organización.

# 5.7.4.5. Paso 4. Definir las estrategias de respuesta

Una vez identificados los riesgos, se establecen las acciones necesarias para reducir su impacto.

Estrategias definidas para cada riesgo

| Riesgo identificado | Estrategia de respuesta |
|---|---|
| Interrupción del servicio por corte eléctrico | Instalar UPS y grupo electrógeno para mantener operativos los servidores. |
| Información cifrada por ransomware | Realizar copias de seguridad diarias, mantener actualizado el antivirus y disponer de procedimientos de restauración. |
| Destrucción de la sala de servidores por incendio | Instalar detectores de humo, sistema automático contra incendios y conservar una copia externa de los backups. |
| Interrupción de la red informática | Mantener un switch de reemplazo y documentar el procedimiento de sustitución. |

Cada estrategia busca disminuir el impacto del riesgo y facilitar la continuidad de las operaciones.

# 5.7.4.6. Paso 5. Elaborar los procedimientos

Para cada estrategia definida se documentan los procedimientos que deberán ejecutarse durante una contingencia.

Por ejemplo, ante un **corte prolongado del suministro eléctrico**, el procedimiento podría ser:

1. Confirmar que la interrupción del suministro no puede resolverse de inmediato.
2. Verificar el funcionamiento de la UPS.
3. Encender el grupo electrógeno si la interrupción supera el tiempo de autonomía de la UPS.
4. Comprobar que los servidores continúan funcionando correctamente.
5. Verificar el acceso a la base de datos y a los servicios críticos.
6. Informar a los usuarios el estado de la contingencia.
7. Una vez restablecido el suministro eléctrico, retornar gradualmente a la operación normal.

Este procedimiento está perfectamente alineado con el riesgo y la estrategia definidos anteriormente.

# 5.7.4.7. Paso 6. Probar y actualizar el plan

Finalmente, la organización establece que:

- se realizará un simulacro de recuperación cada seis meses;
- se verificará periódicamente el funcionamiento de las copias de seguridad;
- el plan será actualizado cuando se incorporen nuevos sistemas o cambie la infraestructura tecnológica.

Un plan de contingencia solo resulta útil si ha sido probado y permanece actualizado.

# 5.7.4.8. Conclusión

Este ejemplo muestra que la elaboración de un Plan de Contingencia comienza con la identificación de los procesos críticos y el análisis de los riesgos que pueden afectarlos. A partir de esta información se definen estrategias de respuesta, se documentan los procedimientos y se realizan pruebas periódicas para garantizar que el plan pueda ejecutarse correctamente cuando ocurra una contingencia.

# 5.8. Recuperación ante Desastres (Disaster Recovery)

Los incidentes que afectan a una organización pueden variar desde pequeñas fallas técnicas hasta eventos de gran magnitud capaces de inutilizar completamente la infraestructura informática. Cuando un desastre provoca la interrupción de los servicios tecnológicos, resulta necesario ejecutar un conjunto de procedimientos destinados a restaurar la infraestructura, los sistemas y la información para que la organización pueda volver a operar normalmente.

La **Recuperación ante Desastres** (*Disaster Recovery* o **DR**) comprende el conjunto de estrategias, procedimientos y recursos destinados a restablecer los sistemas de información y la infraestructura tecnológica después de un desastre.

Su objetivo principal consiste en reducir el tiempo de interrupción de los servicios y minimizar la pérdida de información.

## 5.8.1. ¿Qué se considera un desastre?

En el ámbito de la seguridad informática, un desastre es cualquier evento que produce daños importantes sobre la infraestructura tecnológica e impide el funcionamiento normal de la organización.

Algunos ejemplos son:

- incendios;
- inundaciones;
- terremotos;
- cortes prolongados del suministro eléctrico;
- fallas graves del centro de datos;
- ataques de ransomware que afectan múltiples servidores;
- errores humanos que inutilizan sistemas críticos.

Estos eventos requieren procedimientos de recuperación más complejos que los utilizados para incidentes cotidianos.

## 5.8.2. Plan de Recuperación ante Desastres

El **Plan de Recuperación ante Desastres (DRP)** es el documento que describe las acciones necesarias para restaurar la infraestructura tecnológica después de un desastre.

Generalmente incluye:

- procedimientos para recuperar servidores;
- restauración de bases de datos;
- recuperación de las comunicaciones;
- utilización de copias de seguridad;
- responsables de cada actividad;
- orden de recuperación de los servicios.

Su elaboración forma parte de la estrategia general de continuidad del negocio.

## 5.8.3. Relación entre Continuidad del Negocio, Plan de Contingencia y Recuperación ante Desastres

La **Continuidad del Negocio**, el **Plan de Contingencia** y la **Recuperación ante Desastres** son conceptos estrechamente relacionados, pero no significan lo mismo.

La **Continuidad del Negocio** constituye el concepto más amplio. Su finalidad es garantizar que los procesos esenciales de una organización continúen funcionando, aun cuando ocurra un incidente que afecte el normal desarrollo de las actividades.

Para lograr este objetivo, la organización implementa diferentes estrategias y planes específicos, entre ellos el **Plan de Contingencia** y el **Plan de Recuperación ante Desastres**.

El **Plan de Contingencia** se activa en el momento en que ocurre un incidente. Su propósito consiste en responder de manera inmediata para reducir el impacto del evento y mantener operativos los procesos críticos de la organización.

Por ejemplo, si se produce un corte prolongado del suministro eléctrico, el plan de contingencia puede establecer el uso de UPS, la puesta en marcha de un grupo electrógeno y la comunicación inmediata con los responsables del área informática.

Una vez controlada la emergencia, comienza la etapa de **Recuperación ante Desastres**. En esta fase el objetivo ya no es únicamente mantener funcionando los servicios, sino restaurar completamente la infraestructura tecnológica afectada.

Esto puede implicar:

- reconstruir servidores;
- restaurar bases de datos;
- recuperar equipos dañados;
- reinstalar sistemas operativos;
- verificar la integridad de la información;
- volver gradualmente a la operación normal.

En consecuencia, ambos planes persiguen objetivos diferentes, aunque complementarios.

Mientras el **Plan de Contingencia** busca responder rápidamente para evitar que la organización detenga sus actividades, la **Recuperación ante Desastres** procura devolver la infraestructura tecnológica a su estado normal de funcionamiento.

Ambos forman parte de la estrategia general de **Continuidad del Negocio**.

# 5.8.3.1. Secuencia de actuación ante un incidente

La relación entre la **Continuidad del Negocio**, el **Plan de Contingencia** y la **Recuperación ante Desastres** también puede comprenderse analizando el momento en que cada uno actúa durante un incidente.

En términos generales, la secuencia es la siguiente:

**Continuidad del Negocio → Plan de Contingencia → Recuperación ante Desastres → Retorno a la normalidad**

Esta secuencia puede representarse en la siguiente figura


Como puede observarse, estos tres conceptos no compiten entre sí, sino que se complementan.

La **Continuidad del Negocio** constituye la estrategia general que prepara a la organización para afrontar incidentes.

Cuando el incidente ocurre, entra en funcionamiento el **Plan de Contingencia**, cuyo propósito consiste en responder rápidamente para minimizar el impacto y mantener operativos los procesos críticos.

Una vez controlada la emergencia, comienza la **Recuperación ante Desastres**, cuyo objetivo es reconstruir la infraestructura tecnológica y devolver la organización a su estado normal de funcionamiento.

En consecuencia, puede afirmarse que:

- la **Continuidad del Negocio** planifica;
- el **Plan de Contingencia** responde;
- la **Recuperación ante Desastres** restaura.

## 5.8.4. Ejemplo integrador

Supongamos que una empresa sufre un incendio en la sala de servidores.

**Antes del incendio**

La organización ya había implementado un programa de Continuidad del Negocio, identificando los procesos críticos, realizando análisis de riesgos y elaborando un Plan de Contingencia y un Plan de Recuperación ante Desastres.

**Durante el incendio**

Se activa el Plan de Contingencia:

- se evacúa el edificio;
- se protege al personal;
- se utilizan los sistemas alternativos;
- se informa a los usuarios;
- los servicios críticos continúan funcionando mediante el centro de datos de respaldo.

**Después del incendio**

Se pone en marcha el Plan de Recuperación ante Desastres:

- se reemplazan los servidores dañados;
- se restauran las bases de datos desde las copias de seguridad;
- se reinstalan los sistemas operativos;
- se verifica el funcionamiento de todos los servicios;
- finalmente, la organización vuelve a operar con normalidad.

Este ejemplo muestra que los tres conceptos forman parte de un mismo proceso y actúan en diferentes momentos frente a un incidente.

La siguiente tabla muestra una comparación entre los conceptos

| Aspecto | Continuidad del Negocio | Plan de Contingencia | Recuperación ante Desastres |
|---|---|---|---|
| Alcance | Toda la organización | Respuesta inmediata ante un incidente | Restauración de la infraestructura tecnológica |
| Objetivo | Mantener operativos los procesos críticos | Reducir el impacto de la contingencia | Recuperar completamente los sistemas afectados |
| Momento de aplicación | Antes, durante y después del incidente | Durante el incidente | Después de controlar la emergencia |
| Resultado esperado | Continuidad de las actividades | Mantener el servicio funcionando | Retorno a la operación normal |

# 5.9. Bibliografía de la Unidad 5


- NIST. **Special Publication 800-34 Rev. 1. Contingency Planning Guide for Federal Information Systems.**
- ISO 22301:2019. **Security and resilience — Business continuity management systems — Requirements.**
- ISO/IEC 27002:2022. **Information security, cybersecurity and privacy protection — Information security controls.**
- Stallings, William. **Effective Cybersecurity: A Guide to Using Best Practices and Standards.** Addison-Wesley.
- Whitman, Michael E.; Mattord, Herbert J. **Principles of Information Security.** Cengage Learning.