FACULTAD DE INGENIERÍA

Universidad Nacional de Jujuy

Unidad 5

Disponibilidad y Continuidad del Negocio

Apunte de Cátedra · Seguridad y Auditoría Informática

Contenidos de la Unidad 5

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.

Asegura que los recursos permanezcan operativos y accesibles durante el tiempo requerido para las actividades de la organización.

Parte del modelo CIA

Confidencialidad

Protege frente a accesos no autorizados

Integridad

Garantiza que no sea modificada indebidamente

Disponibilidad

Procura que pueda utilizarse cuando se requiere

5.1.2 Importancia de la Disponibilidad

Ejemplo: Un hospital con historias clínicas digitales. Si el sistema deja de funcionar en una emergencia, aunque los datos sean confidenciales e íntegros, los médicos no pueden acceder a ellos. El problema es de disponibilidad.

Consecuencias de la interrupción de un servicio

- Suspensión de actividades operativas
- Pérdidas económicas
- Disminución de la productividad
- Incumplimiento de contratos o requisitos legales
- Pérdida de confianza de clientes
- Daños a la imagen institucional

5.1.3 Factores que afectan la disponibilidad

Fallas de hardware

Discos, servidores, RAM, fuentes, switches, routers

Fallas de software

Errores de programación, SO, actualizaciones defectuosas

Errores humanos

Eliminación accidental, configuraciones incorrectas

Ataques informáticos

DoS/DDoS, ransomware, malware, sabotaje

Desastres / ambiente

Incendios, inundaciones, terremotos, cortes eléctricos

Comunicaciones

Fallas de ISP, enlaces, saturación de ancho de banda

5.2.1 Redundancia

Consiste en incorporar componentes adicionales que permitan mantener el funcionamiento de un sistema cuando uno de sus elementos deja de operar. Objetivo: eliminar los puntos únicos de falla es decir, aquellos componentes cuya avería provocaría la interrupción completa de un servicio.

Puede aplicarse a

- Servidores
- Discos de almacenamiento
- Fuentes de alimentación
- Enlaces de comunicaciones
- Dispositivos de red
- Centros de datos

Redundancia – Ventajas y limitaciones

Ventajas

- Disminuye la probabilidad de interrupción
- Incrementa la disponibilidad
- Facilita el mantenimiento
- Mejora la continuidad operativa
- Reduce el impacto de fallas de hardware
- Elimina puntos únicos de falla

Limitaciones

- Incremento del costo de equipamiento
- Mayor complejidad de administración
- Necesidad de sincronizar información
- Costos de mantenimiento más altos
- Se reserva para sistemas críticos

5.2.2 Alta Disponibilidad (High Availability)

Estrategia para mantener un servicio operativo la mayor parte del tiempo, minimizando interrupciones por fallas o mantenimiento. La redundancia es uno de sus mecanismos, pero no el único.

Puede incorporar

- Servidores redundantes
- Almacenamiento redundante
- Balanceadores de carga
- Múltiples enlaces
- Monitoreo continuo
- Failover automático

Disponibilidad expresada como porcentaje (“nueves”)

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

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

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

5.2.3 Tolerancia a Fallos

Capacidad de un sistema para continuar funcionando correctamente aun cuando uno o más de sus componentes presenten una falla. El servicio no se interrumpe de forma perceptible para los usuarios.

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.

Características

- Componentes redundantes que operan simultáneamente
- Detección automática de la falla
- Mantiene el servicio sin interrupciones
- Reduce al mínimo la pérdida de información
- Incrementa la confiabilidad del sistema

5.2.4 Diferencias entre los tres conceptos

Concepto	Qué hace	Nivel de protección
Redundancia	Mecanismo básico sobre el cual se apoyan las demás estrategias. Consiste en incorporar componentes adicionales que puedan reemplazar a aquellos que presenten una falla	Básico – elimina puntos únicos de falla
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.	Reduce tiempo de inactividad
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.	Máximo – casi imperceptible para los usuarios

La redundancia es la base; la Alta Disponibilidad la integra con otros mecanismos; la tolerancia a fallos es el nivel más elevado de disponibilidad.

Relación y qué estrategia conviene

Redundancia → Alta Disponibilidad → Tolerancia a Fallos

La elección depende de

Criticidad del servicio

¿Una interrupción es aceptable?

Presupuesto

Tolerancia a fallos es más costosa

Complejidad

Más mecanismos = más administración

Sector

Banca, salud, telecomunicaciones suelen exigir HA o FT

5.3 Sistemas RAID – Concepto

RAID (Redundant Array of Independent Disks) es una tecnología que combina varios discos físicos en una única unidad lógica para mejorar el rendimiento, la capacidad y/o la tolerancia a fallos del almacenamiento.

No reemplaza a las copias de seguridad: protege contra fallas de disco, no contra borrado, ransomware o desastres del sitio.

Objetivos principales

Rendimiento

Paralelismo de lectura/escritura

Capacidad

Unión de discos en un volumen mayor

Tolerancia a fallos

Supervivencia ante falla de uno o más discos

5.3.1.1 ¿Cómo funciona RAID?

En un sistema convencional, toda la información se almacena en un único disco. Si ese disco falla, se pierde el acceso hasta reemplazarlo y recuperar los datos.

En un sistema RAID la información se distribuye entre varios discos según un esquema determinado.

Según el nivel RAID, el sistema puede:

Striping (reparto)	Repartir la información entre varios discos para aumentar la velocidad de acceso.
Mirroring (espejo)	Almacenar copias idénticas de los datos en diferentes discos.
Paridad	Generar información de paridad que permita reconstruir los datos cuando un disco falla.

5.3.1.2 Componentes de un sistema RAID

Un sistema RAID está compuesto, generalmente, por:

Discos físicos

Donde se almacena la información. Pueden ser discos rígidos o unidades SSD.

Controlador RAID

Encargado de administrar la distribución de los datos entre los discos, reconstruir información ante fallas y presentar el conjunto como una única unidad lógica.

Sistema operativo

Visualiza el conjunto de discos como una única unidad lógica de almacenamiento. Desde el punto de vista del usuario, trabaja con un único volumen.

5.3.1.3 RAID por Hardware y RAID por Software

RAID por Hardware

Controladora RAID dedicada (integrada o tarjeta de expansión).

Ventajas:
- Mayor rendimiento
- Menor uso del procesador
- Mayor confiabilidad
- Administración independiente del SO

Desventaja:
- Mayor costo (controladora especializada)

RAID por Software

Administrado por el sistema operativo, sin controladora específica.

Ventajas:
- Menor costo
- Mayor flexibilidad
- No requiere hardware especializado

Limitaciones:
- Usa recursos del procesador
- Rendimiento depende del SO
- Puede ser inferior en alta demanda

Comparación Hardware vs Software RAID

Aspecto	Hardware	Software
Procesamiento	Controladora dedicada	CPU del servidor
Rendimiento	Generalmente superior	Depende del SO y carga
Costo	Más elevado	Menor (sin hardware extra)
Flexibilidad	Dependiente de la controladora	Mayor (funciones del SO)
Independencia del SO	Sí	No

La elección depende del presupuesto, del rendimiento requerido y de la criticidad de los servicios.

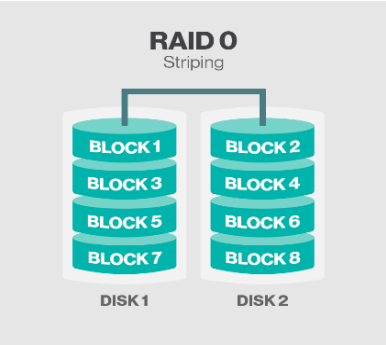
RAID 0 y RAID 1

RAID 0 – Striping

Datos repartidos (striped) entre varios discos.

- Máximo rendimiento
- Sin redundancia
- Falla de un disco = pérdida total
- Capacidad = suma de los discos

Uso: edición de video, temporales donde el rendimiento importa más que la seguridad.

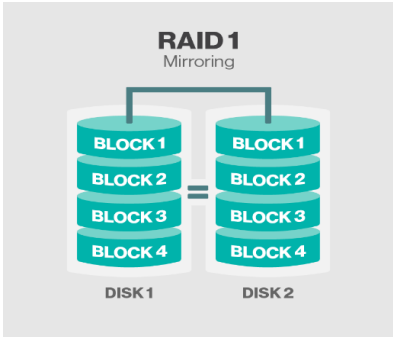


RAID 1 – Mirroring

Copia exacta (espejo) en dos o más discos.

- Alta tolerancia a fallos
- Lectura rápida (puede usar varios discos)
- Escritura similar a un disco
- Capacidad = la del disco más pequeño

Uso: sistemas operativos, datos críticos con poco volumen.



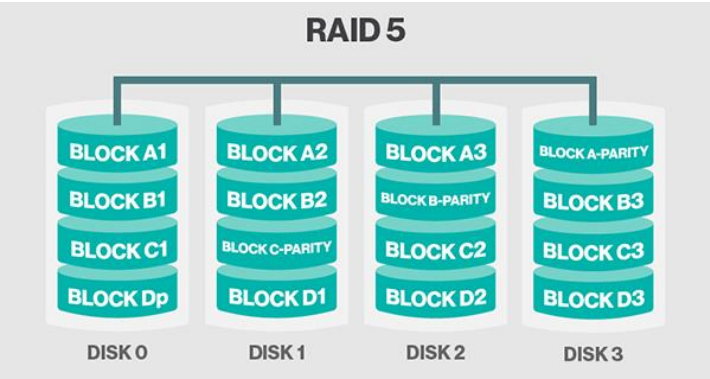
RAID 5 y RAID 6

RAID 5 – Paridad distribuida

Datos + paridad repartidos en ≥3 discos.

- Tolera falla de 1 disco
- Buen equilibrio capacidad/rendimiento/protección
- Capacidad ≈ (n−1) discos
- Escritura un poco más lenta por paridad

Uso: servidores de archivos, bases de datos de tamaño medio.

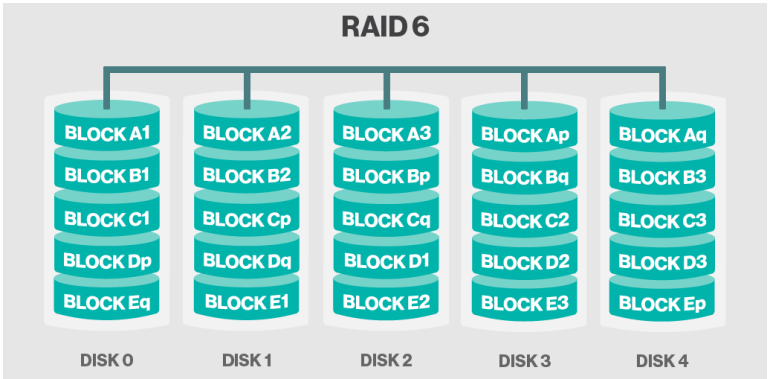


RAID 6 – Doble paridad

Dos bloques de paridad independientes.

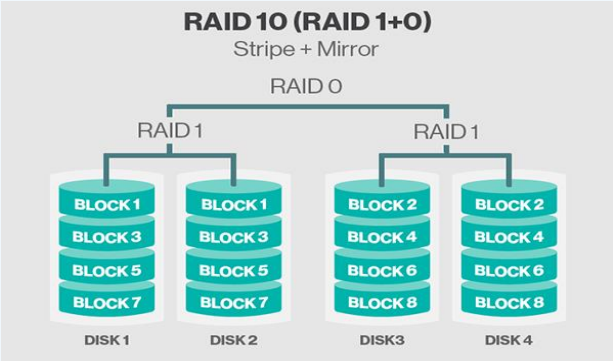
- Tolera falla de 2 discos
- Más seguro que RAID 5
- Capacidad ≈ (n−2) discos
- Escritura más lenta

Uso: almacenamiento crítico, archivos grandes, entornos que no pueden perder datos.



RAID 10 (1+0) y comparación

RAID 10 combina espejo (RAID 1) + striping (RAID 0). Requiere ≥4 discos. Ofrece alto rendimiento y tolerancia a fallos (puede sobrevivir a la falla de un disco de cada par). Capacidad = 50 % de la suma. Ideal para bases de datos de alto rendimiento.



Nivel	Mín. discos	Tolerancia	Capacidad útil
RAID 0	2	Ninguna	100 %
RAID 1	2	1 disco	50 %
RAID 5	3	1 disco	(n−1)/n
RAID 6	4	2 discos	(n−2)/n
RAID 10	4	1 por par	50 %

5.3.9 Recomendaciones según tipo de aplicación

SO / aplicaciones críticas

RAID 1 o RAID 10 – máxima protección y buen rendimiento

Bases de datos de alto rendimiento

RAID 10 – equilibrio óptimo entre velocidad y tolerancia

Servidores de archivos / general

RAID 5 o RAID 6 – buen uso de capacidad con protección

Archivado / datos muy críticos

RAID 6 – doble paridad para mayor seguridad

Temporales / solo rendimiento

RAID 0 – solo si se acepta pérdida total ante falla

Regla general

RAID no sustituye backups. Siempre combinar ambos.

5.3.9 Recomendaciones según tipo de aplicación

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.

Regla general

RAID no sustituye backups. Siempre combinar ambos.

5.4 Copias de Seguridad (Backups)

Un backup es una copia de la información almacenada en un medio distinto al original, destinada a restaurar los datos en caso de pérdida, corrupción, borrado accidental, ataque o desastre.

Objetivos

- Recuperar información eliminada accidentalmente
- Minimizar la pérdida de datos ante fallas de hardware
- Restaurar archivos dañados o corrompidos
- Garantizar la continuidad de las operaciones
- Recuperar información después de un ataque informático
- Cumplir requisitos legales o normativos relacionados con la conservación de información

5.4.5 RAID y Backups: diferencias

Aspecto	RAID	Backup
Qué protege	Falla de disco(s)	Pérdida, borrado, corrupción, ransomware, desastre
Ubicación	Mismo sistema / sitio	Puede estar fuera del sitio
Recuperación histórica	No (estado actual)	Sí (versiones anteriores)
Sustituye al otro	No	No

Ambos son complementarios. RAID reduce el tiempo inactivo por falla de disco; el backup permite recuperar la información ante casi cualquier incidente.

5.4.6 Tipos de Copias de Seguridad

Completa (Full)

Copia de todos los datos seleccionados. Más lenta y ocupa más espacio; restauración más simple.

Incremental

Solo datos modificados desde el último backup completo o incremental. Rápida y compacta; restauración en cadena.

Diferencial

Datos modificados desde el último backup completo. Intermedia en tamaño/tiempo; restauración = full + último diferencial.

5.4.7 Estrategia de Respaldo 3-2-1

Regla práctica ampliamente recomendada para reducir el riesgo de pérdida total de información.

3

Tres copias

Los datos originales + al menos dos copias de seguridad

2

Dos medios distintos

Por ejemplo disco local + cinta, o NAS + nube

1

Una copia fuera del sitio

Protege frente a incendio, robo o desastre en la sede

5.4.8 Medios de Almacenamiento para Backups

Discos / NAS (dispositivo de almacenamiento conectado a la red que permite almacenar y compartir información entre múltiples usuarios y equipos)

Rápidos, fáciles de restaurar. Costo moderado. Ideal para copias locales.

Cintas magnéticas

Alta capacidad y larga vida. Acceso más lento. Grandes organizaciones.

Nube

Fuera del sitio, alta disponibilidad. Depende de Internet y costo periódico.

Combinación

Local (rápida) + externa/nube (protección ante desastre del sitio).

5.5 Recuperación de la Información

Restaurar los datos de una copia de seguridad para devolver un sistema a un estado operativo tras pérdida, corrupción o indisponibilidad. El backup solo es útil si se puede restaurar correctamente.

Cuándo es necesario recuperar

- Eliminación accidental
- Fallas de hardware
- Corrupción de BD
- Errores de software
- Ransomware
- Desastres naturales

Importante

Verificar periódicamente las copias con pruebas de restauración.

Una copia que nunca se probó no garantiza que la información se pueda recuperar cuando haga falta.

5.6 Continuidad del Negocio

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. No busca evitar incidentes, sino preparar la respuesta.

Elementos de un programa de continuidad

- Identificación de procesos críticos
- Análisis de riesgos
- Definicion de estrategias para mantener la operación
- Procedimientos de respuesta
- Asignación de responsables
- Realizacion de pruebas y actualizaciones periódicas

5.7 Plan de Contingencia

Documento que establece los procedimientos, responsabilidades y recursos necesarios para responder ante incidentes que puedan afectar el funcionamiento normal. Objetivo: mantener operativos los procesos críticos o restablecerlos en el menor tiempo posible.

Objetivos

- Minimizar el impacto de los incidentes
- Proteger personas y activos
- Mantener procesos críticos
- Reducir tiempo de interrupción
- Facilitar recuperación rápida y ordenada

5.7.2 Etapas para elaborar un Plan de Contingencia

1. **Definir el alcance**
   Áreas, procesos o servicios incluidos; objetivos y responsables
2. **Identificar procesos críticos**
   Actividades esenciales que deben mantenerse o recuperarse primero
3. **Analizar los riesgos**
   Amenazas y vulnerabilidades (metodología Unidad 4)
4. **Definir estrategias de respuesta**
   Redundancia, restauración de backups, sitios alternativos, procedimientos manuales
5. **Elaborar procedimientos**
   Actividades, responsables, recursos y orden de ejecución
6. **Probar y actualizar**
   Simulacros periódicos; actualizar ante cambios de infraestructura o personal

5.7.4 Caso práctico: TecnoSol S.A.

Empresa de ~40 empleados. Servidor principal (BD), NAS de backups, 20 PCs, Internet permanente. Soporte en horario comercial → interrupción afecta clientes.

Riesgo	Estrategia de respuesta
Corte eléctrico (sin UPS)	UPS + grupo electrógeno
Ransomware (antivirus desactualizado)	Backups diarios + antivirus + restauración
Incendio en sala de servidores	Detectores + extinción + copia externa
Falla del switch principal	Switch de reemplazo + procedimiento documentado

5.8 Recuperación ante Desastres (Disaster Recovery)

Conjunto de estrategias, procedimientos y recursos para restablecer los sistemas de información y la infraestructura tecnológica después de un desastre. Objetivo: reducir el tiempo de interrupción y minimizar la pérdida de información.

¿Qué se considera un desastre?

- Incendios e inundaciones
- Terremotos
- Cortes prolongados de energía
- Fallas graves del centro de datos
- Ransomware masivo
- Errores que inutilizan sistemas críticos

5.8.3 Relación entre los tres conceptos

Continuidad del Negocio → Plan de Contingencia → Recuperación ante Desastres → Normalidad

Aspecto	Continuidad del Negocio	Plan de Contingencia	Recuperación ante Desastres
Alcance	Toda la organización	Respuesta inmediata	Infraestructura tecnológica
Objetivo	Procesos críticos operativos	Reducir impacto	Restaurar sistemas
Momento	Antes, durante y después	Durante el incidente	Después de controlar la emergencia
Resultado	Continuidad de actividades	Mantener el servicio	Retorno a la operación normal

5.8.4 Ejemplo integrador: incendio en sala de servidores

Antes

Programa de Continuidad del Negocio ya implementado: procesos críticos identificados, análisis de riesgos, Plan de Contingencia y DRP elaborados.

Durante

Se activa el Plan de Contingencia: evacuación, protección del personal, sistemas alternativos / centro de respaldo, información a usuarios.

Después

Plan de Recuperación ante Desastres: reemplazo de servidores, restauración de BD desde backups, reinstalación de SO, verificación y retorno a la normalidad.