

1. INTRODUCCIÓN A LA INFRAESTRUCTURA DE TI

✦ *Universidad de La Sabana - 2025*

¿Qué es la Infraestructura de TI?

Conjunto de hardware, software, redes y servicios que soportan una organización. Es crucial para el funcionamiento de los negocios, ya que permite la continuidad operativa y evita pérdidas económicas y reputacionales.

Componentes de la Infraestructura de TI

1. Hardware:

- Servidores físicos.
- Equipos de cómputo.
- Routers y switches.
- Almacenamiento NAS (Network Attached Storage).
- Cámaras de seguridad y terminales POS.

2. Software:

- Sistemas Operativos.
- Aplicaciones empresariales (CRM, ERP).
- Soluciones de virtualización.

3. Redes:

- LAN (Local Area Network).
- WAN (Wide Area Network).
- VPN para conexión entre sucursales.
- Internet y redes inalámbricas WiFi.

4. Servicios:

- Seguridad informática.
 - Gestión de infraestructura.
 - Servicios Cloud.
 - Sistemas de monitoreo y respaldo.
-

Modelo de Capas en Infraestructura de TI

✦ *Permite estructurar y entender la infraestructura de una organización en diferentes niveles:*

1. Capa Física

- Incluye todo el hardware, dispositivos de energía y refrigeración.

2. Infraestructura Virtual

- Virtualización de servidores y aplicaciones mediante herramientas como VMware.

3. Servicios de Infraestructura

- Monitoreo, seguridad, copias de respaldo y recuperación ante desastres.

4. Capa de Aplicaciones

- Software de gestión empresarial como ERP, aplicaciones de domicilios y bases de datos.

Atributos No Funcionales de la Infraestructura

Son características que determinan la calidad de un sistema:

✓ Disponibilidad:

Capacidad del sistema para estar operativo y accesible cuando se necesita. Se mide en porcentaje y determina el tiempo que un sistema puede estar funcionando sin interrupciones.

✦ Factores que afectan la disponibilidad:

- Fallos de hardware o software.
- Errores humanos.
- Ataques cibernéticos.
- Desastres naturales.

✦ Ejemplo:

Un servicio en la nube con 99.999% de disponibilidad solo puede estar inactivo 5.26 minutos al año.

✓ Escalabilidad:

Capacidad de un sistema para manejar el crecimiento de la carga de trabajo sin afectar negativamente su rendimiento.

✦ Tipos de escalabilidad:

- Escalabilidad Vertical → Aumentar recursos en un solo servidor (más RAM, CPU).
- Escalabilidad Horizontal → Agregar más servidores a la infraestructura.

✦ Ejemplo:

Una tienda en línea escala horizontalmente agregando más servidores cuando hay eventos de alto tráfico como el Black Friday.

✓ Seguridad:

Conjunto de medidas diseñadas para proteger los datos, aplicaciones y comunicaciones contra accesos no autorizados y amenazas.

✦ Principales aspectos de seguridad:

- ✓ Confidencialidad → Solo personas autorizadas pueden acceder a los datos.
- ✓ Integridad → Garantiza que la información no sea alterada de manera no autorizada.
- ✓ Disponibilidad → Protege contra ataques que buscan dejar inoperativo un sistema.

✦ Ejemplo:

- Uso de firewalls y antivirus para evitar ataques de malware.
 - Implementación de autenticación multifactor (MFA) para evitar accesos no autorizados.
-

✓ Rendimiento:

Capacidad del sistema para responder rápidamente a las solicitudes e interacciones de los usuarios. Se mide en términos de tiempo de respuesta y capacidad de procesamiento.

✦ Factores que afectan el rendimiento:

- Carga del sistema → Cantidad de usuarios y procesos simultáneos.
- Capacidad del hardware → Procesador, RAM, almacenamiento.
- Optimización del software → Algoritmos eficientes y base de datos optimizada.

✦ Ejemplo:

- Un sitio web que tarda más de 3 segundos en cargar puede perder clientes.
 - Un servidor con bajo rendimiento puede retrasar la ejecución de procesos críticos en una empresa.
-

Redundancia

✦ *La redundancia es el mecanismo que permite evitar SPOFs y garantizar la disponibilidad de los servicios.*

¿Qué es la Redundancia?

Es la duplicación de componentes críticos en la infraestructura de TI para garantizar que, si uno falla, otro asuma su función sin interrumpir la operación.

Tipos de Redundancia:

1 Redundancia de Hardware:

- Ejemplo: Servidores en clúster, fuentes de poder dobles, discos RAID.

2 Redundancia de Red:

- Ejemplo: Múltiples conexiones a Internet, balanceo de carga en routers.

3 Redundancia de Datos:

- Ejemplo: Replicación de bases de datos en diferentes ubicaciones.

4 Redundancia de Software:

- Ejemplo: Copias de aplicaciones en servidores distintos.

Beneficios de la Redundancia

- ✓ Evita la interrupción de servicios en caso de fallos.
- ✓ Minimiza el impacto de ataques o errores humanos.
- ✓ Permite realizar mantenimiento sin afectar la operación.

✦ Ejemplo Real:

- Un servidor web con (replicación servers) balanceo de carga y múltiples nodos puede atender más usuarios sin riesgo de colapso.

2. DISPONIBILIDAD EN INFRAESTRUCTURA DE TI

✦ Conceptos fundamentales sobre la continuidad y resiliencia de sistemas tecnológicos.

Niveles de Disponibilidad (% de tiempo operativo)

🌈 Ejemplo con los "nueves":

- 90% → 36.5 días de caída por año.
- 99% → 3.65 días por año.
- 99.9% → 8.7 horas por año.
- 99.999% → 5.2 minutos por año.
- 99.9999% → 31.5 segundos por año.

Cálculo de Disponibilidad

- MTBF (Mean Time Between Failures): Tiempo promedio entre fallos.
- MTTR (Mean Time To Repair): Tiempo promedio para reparar fallas.
- ¿Qué es un SPOF?
 - Un Single Point of Failure (SPOF) es un elemento crítico dentro de una infraestructura tecnológica que, si falla, afecta todo el sistema sin posibilidad de continuar operando.
 - Ejemplo Real:
 - ✦ *Imagina una empresa que tiene un único servidor para su sitio web sin respaldo. Si ese servidor falla, el sitio web dejará de estar disponible hasta que se repare.*
 - Características de un SPOF:
 - No tiene redundancia.
 - Si falla, detiene la operación.
 - Aumenta el riesgo de caída total del servicio.
 - Requiere mitigación con redundancia o alta disponibilidad.

✦ Fórmula de disponibilidad:

$$\text{Disponibilidad} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} \times 100$$

Ejercicio: *Calcular la disponibilidad de dispositivos con datos de MTBF y MTTR.*

Tipos de Disponibilidad


1. Disponibilidad en Serie

- Si un componente falla, todo el sistema se cae.
- Ejemplo: Una cadena de servidores sin redundancia.

2. Disponibilidad en Paralelo

- Si un componente falla, otro puede tomar su lugar.
- Ejemplo: Clúster de servidores con balanceo de carga.


Amenazas a la Disponibilidad en Infraestructura de TI

 *La disponibilidad es un atributo clave en la infraestructura de TI, ya que garantiza que los sistemas y servicios estén operativos cuando se necesiten. Sin embargo, existen múltiples amenazas que pueden comprometer la disponibilidad, desde fallos técnicos hasta ataques cibernéticos o factores externos impredecibles.*

A continuación, se detallan las principales amenazas a la disponibilidad y las estrategias para mitigar estos riesgos:

Principales Amenazas a la Disponibilidad

1 Fallos de Hardware/Software

 Descripción: Los componentes físicos y lógicos de un sistema pueden presentar fallos que afecten la disponibilidad de los servicios. Ejemplos comunes incluyen:

- Fallo en servidores o almacenamiento (discos duros dañados, fuentes de poder defectuosas, sobrecalentamiento).
- Errores en software crítico (fallas en actualizaciones, errores de programación, incompatibilidad de versiones).
- Fallos en la infraestructura de red (switches defectuosos, routers dañados, enlaces de fibra cortados).

Ejemplo real:

Si el servidor central de una empresa falla sin contar con un sistema de respaldo, los empleados no podrán acceder a sus archivos ni los clientes podrán utilizar la plataforma en línea.

Impacto:

- Pérdida de datos críticos.
 - Interrupción total o parcial del servicio.
 - Necesidad de intervención manual para restaurar operaciones.
-

2 Errores Humanos

Descripción:

El factor humano sigue siendo una de las principales causas de fallos en la disponibilidad de TI. Algunos errores comunes incluyen:

- Configuraciones incorrectas en sistemas o redes.
- Eliminación accidental de datos o archivos importantes.
- Desactivación involuntaria de servicios clave.
- Olvido de aplicar actualizaciones de seguridad que terminan exponiendo vulnerabilidades.

Ejemplo real:

Un administrador de TI cambia una configuración en un firewall y bloquea accidentalmente el tráfico de red, dejando a toda la empresa sin acceso a Internet.

Impacto:

- Pérdida temporal o permanente de servicios.
- Necesidad de corregir el error y restaurar sistemas.
- Pérdida de confianza en el equipo de TI.

3 Ataques Externos (Ciberseguridad)

Descripción:

Los sistemas de TI están en constante riesgo de ataques cibernéticos diseñados para comprometer la disponibilidad. Los más comunes son:

- Ataques DDoS (Denegación de Servicio Distribuida): Sobrecargan un servidor o red con tráfico falso para dejarlo inoperativo.
- Ransomware: Secuestra archivos o sistemas completos, exigiendo un rescate para su liberación.
- Intrusiones y hackeos: Exploit de vulnerabilidades para alterar el funcionamiento de los sistemas.

Ejemplo real:

En 2021, un ataque de ransomware afectó a Colonial Pipeline, la mayor red de oleoductos en EE.UU., provocando una crisis en el suministro de combustible y pérdidas millonarias.

Impacto:




- Caída total de servicios.
- Pérdida de datos y exposición de información confidencial.
- Daño a la reputación de la empresa.

Ciberseguridad y Gestión de Riesgos

 *Protección de datos, redes y sistemas contra ataques o accesos no autorizados.*

Principales Amenazas de Ciberseguridad:

1 Ataques de Denegación de Servicio (DDoS)

- Sobrecargan un sistema con tráfico malicioso.
 Ransomware
- Secuestra archivos y exige un pago para su recuperación.
 Phishing
- Engaños para robar credenciales de usuarios.
 Malware y Virus
- Software malicioso que compromete sistemas.

Gestión de Riesgos en Ciberseguridad

- Identificar amenazas: Analizar posibles riesgos (ejemplo: robo de datos, ataques).
- Mitigar riesgos: Implementar firewalls, autenticación multifactor, cifrado de datos.
- ⚡ Monitoreo continuo: Usar SIEM (Security Information and Event Management) para detectar incidentes en tiempo real.

📌 Ejemplo Real:

- Facebook sufrió un ataque en 2019, exponiendo 540 millones de cuentas de usuarios debido a fallos en su infraestructura.

Factores Externos

● Descripción:

Existen factores externos e impredecibles que pueden afectar la disponibilidad de la infraestructura de TI. Ejemplos incluyen:

- Desastres naturales (terremotos, incendios, huracanes).
- Cortes de energía prolongados sin fuentes de respaldo.
- Fallas en proveedores de telecomunicaciones (fallos en ISP, interrupción de enlaces de fibra óptica).
- Interrupciones en la cadena de suministro (escasez de equipos de TI, chips, componentes electrónicos).

📌 Ejemplo real:

Durante el huracán Sandy en 2012, muchas empresas en Nueva York quedaron sin servicio debido a la destrucción de centros de datos y redes eléctricas.

⚠️ Impacto:

- Inaccessibilidad a sistemas críticos.
- Necesidad de recuperación manual en sitios alternativos.
- Pérdidas económicas y operativas significativas.

✅ Estrategias de Mitigación

🚨 *Para garantizar la disponibilidad de los sistemas de TI y minimizar el impacto de estas amenazas, se implementan diversas estrategias. A continuación, se detallan las más efectivas:*

1 Redundancia

📖 Descripción:

Implementación de componentes duplicados para garantizar que, si un sistema falla, otro pueda tomar su lugar sin afectar la operación.

🔥 Ejemplos:

- Servidores en clúster con balanceo de carga.
- Discos RAID para asegurar tolerancia a fallos en almacenamiento.
- Fuentes de alimentación redundantes en servidores.
- Enlaces de red duplicados para garantizar conexión ininterrumpida.

⚡ Beneficio:

Garantiza operación continua incluso si un componente clave falla.

2 Alta Disponibilidad (HA – High Availability)

📖 Descripción:

Diseñar arquitecturas resilientes que minimicen el tiempo de inactividad mediante tecnologías como:

- Balanceadores de carga para distribuir tráfico entre varios servidores.
- Failover automático que transfiere servicios a otro sistema si el principal falla.
- Replicación de bases de datos en diferentes centros de datos.

🔥 Ejemplo real:

Google y Amazon tienen centros de datos en múltiples ubicaciones. Si uno falla, otro asume la carga sin afectar a los usuarios.

⚡ Beneficio:

Minimiza la interrupción de los servicios en caso de fallos.

3 Planes de Recuperación ante Desastres (DRP) y Continuidad del Negocio (BCP)

📖 Descripción:

Son estrategias documentadas que establecen procedimientos de acción ante incidentes críticos.

- **DRP (Disaster Recovery Plan)** → Enfocado en la restauración técnica tras un desastre.
- **BCP (Business Continuity Plan)** → Asegura la continuidad operativa del negocio.

🔥 Ejemplos de DRP y BCP:

- Copias de seguridad programadas en sitios geográficamente separados.
- Centros de datos alternativos para migrar operaciones rápidamente.
- Procedimientos definidos para recuperación en menos de 24 horas.

⚡ **Beneficio:**

Reduce significativamente el tiempo de recuperación tras un incidente grave.

🔌 **Monitoreo y Alertas**

📺 **Descripción:**

El uso de herramientas de monitoreo ayuda a detectar fallos en tiempo real antes de que impacten la operación.

🔧 **Herramientas recomendadas:**

- Zabbix / Nagios / Datadog → Monitoreo de infraestructura.
- Prometheus + Grafana → Visualización de métricas en servidores y redes.
- SIEM (Security Information and Event Management) → Análisis de incidentes de seguridad.

🔧 **Ejemplo real:**

Un banco utiliza monitoreo avanzado para detectar actividad anómala en sus servidores antes de sufrir un ataque DDoS.

⚡ **Beneficio:**

Reduce el tiempo de respuesta ante incidentes, evitando caídas prolongadas.

3. GESTIÓN DE INFRAESTRUCTURA DE TI

🔧 *Cómo administrar y optimizar los recursos tecnológicos de una organización.*

Tipos de Redes

- LAN (Local Area Network): Redes locales en oficinas y casas.
 - WAN (Wide Area Network): Redes a nivel global como Internet.
 - WLAN (Wireless LAN): Redes inalámbricas WiFi.
 - MAN (Metropolitan Area Network): Redes que cubren ciudades o campus.
 - PAN (Personal Area Network): Redes personales, como Bluetooth.
-

Subnetting y Asignación de IPs

🔧 *Dividir redes en subredes más pequeñas para mejorar seguridad y optimización de recursos.*

- Clases de IP privadas:
 - Clase A: 10.0.0.0 – 10.255.255.255
 - Clase B: 172.16.0.0 – 172.31.255.255
 - Clase C: 192.168.0.0 – 192.168.255.255
- Máscaras de subred:
 - /24 → 254 hosts.

- /25 → 126 hosts.
- /23 → 510 hosts.

Ejercicio: *Dividir una red /23 en 4 subredes con máscara /25.*

Equipos de Red

- NIC (Tarjeta de Red): Punto de conexión entre dispositivos y red.
- Switches: Capa 2 (LAN) y Capa 3 (con enrutamiento).
- Routers: Conectan redes diferentes y manejan NAT y DHCP.
- Firewall: Protege el tráfico de red.

4. FRAMEWORKS Y BUENAS PRÁCTICAS EN INFRAESTRUCTURA

📌 *Normas y marcos de referencia para la gestión eficiente de TI.*

Framework	Propósito	Enfoque Principal	Beneficios	Casos de Uso
COBIT (Control Objectives for Information and Related Technologies)	Gobernanza de TI y cumplimiento normativo.	Establece controles y buenas prácticas para asegurar que TI agregue valor al negocio y gestione riesgos.	<ul style="list-style-type: none">✓ Asegura cumplimiento normativo (ISO 27001, PCI DSS, GDPR).✓ Permite medir y gestionar riesgos en TI.✓ Facilita la toma de decisiones estratégicas.	<ul style="list-style-type: none">🏦 Bancos, aseguradoras, entidades gubernamentales.🏢 Empresas con alto riesgo regulatorio.🔍 Organizaciones que necesitan auditorías y control de TI.
ITIL (Information Technology Infrastructure Library)	Gestión de servicios de TI.	Mejora la calidad, disponibilidad y eficiencia de los servicios de TI, asegurando que estos soporten los objetivos del negocio.	<ul style="list-style-type: none">✓ Optimiza la entrega de servicios de TI.✓ Reduce tiempos de respuesta ante incidentes.✓ Mejora la experiencia del usuario y la continuidad del negocio.	<ul style="list-style-type: none">🏢 Empresas de servicios tecnológicos y soporte TI.🏢 Organizaciones que buscan mejorar la gestión de incidentes y cambios.📡 Empresas de telecomunicaciones, software y retail.
TOGAF (The Open Group Architecture Framework)	Desarrollo de arquitecturas empresariales.	Proporciona un marco estructurado para diseñar, planificar, implementar y gestionar infraestructuras tecnológicas alineadas con el negocio.	<ul style="list-style-type: none">✓ Estandariza la arquitectura empresarial.✓ Elimina redundancias tecnológicas.✓ Facilita la integración de sistemas.	<ul style="list-style-type: none">🏢 Organizaciones con sistemas dispersos que requieren integración.🏢 Empresas que buscan optimizar su infraestructura TI.🏢 Entidades gubernamentales y grandes corporaciones.
DevOps (Development & Operations)	Integración de desarrollo y operaciones de software.	Automatiza procesos de desarrollo, pruebas y despliegue, eliminando barreras entre los equipos de desarrollo y operaciones.	<ul style="list-style-type: none">✓ Reduce tiempos de lanzamiento de software.✓ Automatiza pruebas y monitoreo.✓ Mayor estabilidad en despliegues con menos errores.	<ul style="list-style-type: none">💻 Empresas de desarrollo de software.🚀 Startups tecnológicas con ciclos de entrega rápida.🛒 Empresas de e-commerce con infraestructura escalable.
CMMI (Capability Maturity Model Integration)	Mejora de procesos en desarrollo de software y gestión de proyectos.	Define niveles de madurez para optimizar eficiencia y calidad en el desarrollo de software.	<ul style="list-style-type: none">✓ Estandariza procesos de desarrollo.✓ Reduce errores en software y sobrecostos.✓ Mejora la calidad y cumplimiento de plazos.	<ul style="list-style-type: none">🏢 Empresas con equipos de desarrollo desorganizados.⏰ Empresas que no cumplen plazos ni estándares de calidad.🏢 Empresas de tecnología y proyectos de ingeniería de software.

📌 Características Detalladas de Cada Framework

Aquí están las características más detalladas y explicadas de cada uno de los frameworks.

◆ Características de COBIT

✦ **Objetivo:** Asegurar que TI aporte valor al negocio y cumpla regulaciones.

1 Separación entre Gobernanza y Gestión de TI:

- **Gobernanza:** Se centra en la toma de decisiones, evaluación de riesgos y alineación con los objetivos del negocio.
- **Gestión:** Se enfoca en la implementación y operación de TI.

2 Modelo de Control y Cumplimiento Normativo:

- COBIT se alinea con regulaciones como ISO 27001 (Seguridad de la Información), PCI DSS (Protección de datos de tarjetas) y GDPR.
- Facilita auditorías de seguridad y cumplimiento normativo.

3 Gestión de Riesgos Tecnológicos:

- Permite evaluar riesgos en seguridad, continuidad y desempeño de TI.
 - Proporciona métricas clave para tomar decisiones informadas.
-

♦ **Características de ITIL**

✦ **Objetivo:** Optimizar la entrega y operación de servicios de TI.

1 Ciclo de Vida del Servicio:

- **Estrategia del Servicio:** Definir qué servicios ofrecer y su valor para el negocio.
- **Diseño del Servicio:** Planificar la estructura, procesos y estándares.
- **Transición del Servicio:** Implementar cambios y mejoras sin interrumpir la operación.
- **Operación del Servicio:** Gestionar incidentes, problemas y solicitudes de usuarios.
- **Mejora Continua:** Monitoreo y optimización constante.

2 Gestión de Incidentes y Problemas:

- Define procesos estructurados para atender fallas rápidamente.
- Registra incidentes en herramientas como ServiceNow o Jira ITSM.

3 Gestión de Cambios (Change Management):

- Evaluación de impacto antes de implementar cambios.
 - Uso de un Comité de Cambios (CAB) para decisiones críticas.
-

♦ **Características de TOGAF**

✦ **Objetivo:** Estandarizar la arquitectura empresarial y facilitar la integración de sistemas.

1 Cuatro Dominios Claves de TOGAF:

- **Arquitectura de Negocio:** Define procesos y estructura organizacional.

- Arquitectura de Datos: Maneja la gestión y flujo de datos.
- Arquitectura de Aplicaciones: Establece cómo se conectan los sistemas de software.
- Arquitectura Tecnológica: Infraestructura de servidores, redes y dispositivos físicos.

2 Método de Desarrollo de Arquitectura (ADM - Architecture Development Method):

- Consiste en 8 fases estructuradas para el diseño e implementación de arquitecturas de TI.

3 Eliminación de Redundancias Tecnológicas:

- Unifica sistemas y evita duplicación de datos o procesos.
-

♦ Características de DevOps

✚ **Objetivo:** Acelerar el desarrollo de software y mejorar la entrega continua.

1 Integración y Despliegue Continuo (CI/CD):

- Continuous Integration (CI): Automatiza la integración y prueba de código.
- Continuous Deployment (CD): Despliega nuevas versiones sin interrupciones.

2 Uso de Contenedores y Virtualización:

- Docker y Kubernetes permiten que las aplicaciones sean escalables y portátiles.

3 Monitoreo y Observabilidad:

- Se usan herramientas como Prometheus, Grafana, Datadog para monitorear errores y desempeño.

⚡ **Automatización de Infraestructura:**

- Herramientas como Terraform y Ansible gestionan entornos de producción con código.
-

♦ Características de CMMI

✚ **Objetivo:** Estandarizar procesos de desarrollo de software y medir su madurez.

1 Cinco Niveles de Madurez:

- Nivel 1: Inicial → No hay procesos definidos ni controlados.
- Nivel 2: Gestionado → Se documentan procesos básicos y se controlan proyectos.
- Nivel 3: Definido → Procesos estándar establecidos en la organización.
- Nivel 4: Cuantitativamente Gestionado → Se usan métricas y datos para optimización.
- Nivel 5: Optimizado → Innovación y mejora continua basada en análisis.

2 Revisión de Código y Estándares de Programación:

- Se implementan patrones de diseño para mejorar calidad y mantenimiento.

3 Monitoreo del Desempeño de Desarrollo:

- Se usan herramientas de análisis de datos para detectar problemas en la producción.
-

● Data Centers y Tiers

✦ *Los data centers se clasifican en niveles (Tiers) según su disponibilidad y redundancia.*

Clasificación de Data Centers según el Uptime Institute

Tier	Disponibilidad (%)	Tiempo de Inactividad Anual	Características
Tier I	99.671%	28.8 horas	No tiene redundancia, solo un camino de energía y refrigeración.
Tier II	99.741%	22 horas	Tiene respaldo en componentes clave, pero un único punto de fallo.
Tier III	99.982%	1.6 horas	Redundancia N+1, permite mantenimiento sin afectar la operación.
Tier IV	99.995%	26.3 minutos	Redundancia 2N, tolerante a fallos y máxima disponibilidad.

Ejemplo de cada Tier

- ✦ Tier I → Un pequeño data center empresarial con una única fuente de energía.
- ✦ Tier II → Un data center de una compañía mediana con respaldo parcial.
- ✦ Tier III → Amazon Web Services (AWS) usa data centers Tier III para garantizar alta disponibilidad.
- ✦ Tier IV → Google y Microsoft usan data centers Tier IV para máxima redundancia.

✓ ¿Cómo elegir un Data Center?

- Si es crítico para el negocio, elegir Tier III o IV.
 - Si no requiere alta disponibilidad, un Tier II puede ser suficiente.
-

✦ Servidores Comunes: Tipos, Funciones y Características

✦ *Los servidores son componentes esenciales en la infraestructura de TI, ya que permiten gestionar, almacenar y distribuir información en redes empresariales y en la nube.*

◆ ¿Qué es un Servidor?

Un servidor es un equipo (físico o virtual) que proporciona servicios y recursos a otros dispositivos o usuarios dentro de una red. Se utiliza para gestionar datos, aplicaciones, sitios web y diversos procesos de negocio.

✦ Ejemplo Real:

- Cuando visitas Google, un servidor web procesa tu solicitud y te envía la página en tu navegador.
-

🖨 Tipos de Servidores Comunes y sus Funciones

Cada tipo de servidor cumple una función específica en la infraestructura de TI. Aquí están los más utilizados:

Tipo de Servidor	Función Principal	Ejemplo de Uso
Servidor DNS (Domain Name System)	Traduce nombres de dominio en direcciones IP para facilitar el acceso a sitios web.	🔴 <i>Google DNS (8.8.8.8), Cloudflare DNS (1.1.1.1)</i>
Servidor DHCP (Dynamic Host Configuration Protocol)	Asigna automáticamente direcciones IP a los dispositivos dentro de una red.	🔴 <i>Routers domésticos y empresariales asignan IPs dinámicas a usuarios.</i>
Servidor de Archivos (File Server)	Almacena y permite compartir archivos entre usuarios dentro de una red.	🔴 <i>Servidores NAS en empresas para compartir documentos y copias de seguridad.</i>
Servidor Web	Aloja y entrega sitios web a través de HTTP/HTTPS.	🔴 <i>Apache, Nginx, Microsoft IIS.</i>
Servidor de Correo	Maneja el envío y recepción de correos electrónicos.	🔴 <i>Microsoft Exchange, Postfix, Gmail Servers.</i>
Servidor de Aplicaciones	Ejecuta aplicaciones empresariales y servicios en la nube.	🔴 <i>Oracle WebLogic, Tomcat, JBoss.</i>
Servidor de Base de Datos	Almacena, gestiona y administra datos de aplicaciones.	🔴 <i>MySQL, PostgreSQL, Microsoft SQL Server.</i>
Servidor de Virtualización	Permite ejecutar múltiples máquinas virtuales en un solo hardware.	🔴 <i>VMware vSphere, Microsoft Hyper-V, Proxmox.</i>
Servidor Proxy	Actúa como intermediario entre usuarios y servicios de Internet, mejorando seguridad y rendimiento.	🔴 <i>Squid Proxy, Nginx como reverse proxy.</i>
Servidor de Juegos	Aloja sesiones de videojuegos en línea para múltiples jugadores.	🔴 <i>Servidores de Minecraft, Call of Duty, Fortnite.</i>
Servidor de Autenticación (Active Directory, LDAP)	Controla accesos a la red verificando credenciales de usuarios.	🔴 <i>Active Directory en empresas para gestionar accesos.</i>

- Servidor DNS → Gestiona la resolución de nombres de dominio internos.
- Servidor DHCP → Asigna direcciones IP a empleados automáticamente.
- Servidor de Archivos → Almacena documentos compartidos para usuarios internos.
- Servidor de Correo → Maneja los correos electrónicos corporativos.
- Servidor de Base de Datos → Gestiona los datos de clientes y transacciones.
- Servidor de Aplicaciones → Aloja software interno de gestión empresarial (CRM, ERP).
- Servidor Proxy → Filtra y mejora la seguridad en las conexiones a Internet.

Modelo OSI

Capa	Función Principal	Ejemplo de Protocolo o Tecnología
Capa 7 – Aplicación	Permite la interacción del usuario con la red.	✦ HTTP, HTTPS, FTP, SMTP, DNS
Capa 6 – Presentación	Transforma datos para que las aplicaciones los interpreten correctamente.	✦ TLS, SSL, JPEG, GIF, MP4, XML, JSON
Capa 5 – Sesión	Administra conexiones entre aplicaciones (inicio, mantenimiento y cierre de sesión).	✦ NetBIOS, RPC, PPTP, SQL Session
Capa 4 – Transporte	Asegura la entrega de datos entre dispositivos con control de errores y segmentación.	✦ TCP, UDP
Capa 3 – Red	Se encarga del direccionamiento y el enrutamiento de paquetes.	✦ IP, ICMP, ARP, RIP, OSPF, BGP
Capa 2 – Enlace de Datos	Define cómo se transmiten los datos en la red local, organizándolos en tramas.	✦ Ethernet, Wi-Fi (802.11), VLAN, MAC, PPP
Capa 1 – Física	Transmite bits a través de cables, ondas de radio o fibra óptica.	✦ Fibra óptica, Cable

EJERCICIOS RESUELTOS

Voy a resolver todos los ejercicios de las presentaciones. Te avisaré cuando estén listos. 🇮🇹 🇪🇺 🇺🇸 ⌚

Resultados de los Ejercicios de Disponibilidad

Aquí están los cálculos de disponibilidad para los sistemas con diferentes MTBF y MTTR:

- Disponibilidad de Procesos: 99.92%
- Disponibilidad de Almacenamiento: 99.95%
- Disponibilidad de Seguridad: 99.96%
- Disponibilidad en Serie (todos los sistemas deben estar activos para que funcione): 99.82%
- Disponibilidad en Paralelo (el sistema sigue funcionando si al menos uno de los elementos está activo): 99.99999998% 🚀

✦ Conclusión:

- En serie: La disponibilidad baja porque si un componente falla, todo el sistema falla.
- En paralelo: Se logra casi un 100% de disponibilidad, ya que hay redundancia.

Voy a continuar resolviendo los otros ejercicios relacionados con subnetting y planificación de infraestructura. ⌚ 💻

Parece que hubo un problema al definir la red original con una máscara de /23. Voy a corregirlo y continuar con la división en 4 subredes con /25. ⌚

Resultados del Ejercicio de Subnetting

Se ha dividido la red 192.168.101.0/23 en 4 subredes con máscara /25:

1. Subred 1: 192.168.100.0/25
2. Subred 2: 192.168.100.128/25
3. Subred 3: 192.168.101.0/25
4. Subred 4: 192.168.101.128/25

✦ Conclusión:

- Ahora cada subred tiene 126 hosts utilizables (recordando que la primera y última dirección son para la red y el broadcast).
- Se ha logrado dividir la red original de forma más eficiente y organizada.

Voy a continuar con la resolución de los ejercicios de planificación de infraestructura. 🕒 💻

Ejercicio: Planificación de Infraestructura para "Pollito con Papas"

✦ **Objetivo:** Diseñar una infraestructura tecnológica utilizando el modelo de capas y garantizar disponibilidad, escalabilidad, seguridad y rendimiento.

1 Propuesta de Infraestructura

Capas implementadas:

1. Capa Física 💻
 - Servidores físicos en un centro de datos.
 - Equipos de red: switches, routers y firewalls.
 - Almacenamiento NAS para copias de seguridad.
 - Sistemas de energía redundante.
2. Capa de Infraestructura Virtual 💻 🔗
 - Virtualización con VMware o Proxmox.
 - Contenedores Docker/Kubernetes para aplicaciones.
 - Balanceadores de carga para distribuir tráfico.
3. Capa de Servicios de Infraestructura 🗝️
 - Monitoreo y alertas con Zabbix o Prometheus.
 - Copia de seguridad automática con políticas de DRP/BCP.
 - Redundancia en servidores y almacenamiento.
4. Capa de Aplicaciones 🇮🇹
 - Sistema POS para puntos de venta.
 - Aplicación móvil de domicilios.

- ERP para gestión de inventarios y finanzas.
-

2 Estrategias para Garantizar Disponibilidad, Escalabilidad, Seguridad y Rendimiento

✦ Disponibilidad:

- Arquitectura redundante con servidores en diferentes ubicaciones.
- Backup en la nube y centros de datos alternativos.
- Alta disponibilidad con failover automático.

✦ Escalabilidad:

- Escalabilidad horizontal: agregar más servidores cuando la demanda crezca.
- Contenedores Docker/Kubernetes para escalar dinámicamente.
- Microservicios en lugar de aplicaciones monolíticas.

✦ Seguridad:

- Firewall y VPN para proteger la red interna.
- Autenticación multifactor (MFA) para accesos críticos.
- Cifrado de datos en almacenamiento y en tránsito (TLS/SSL).
- Cumplimiento de normativas como PCI DSS para pagos con tarjeta.

✦ Rendimiento:

- Optimización de base de datos (indexación, particionamiento).
 - Uso de CDN para reducir tiempos de carga.
 - Monitoreo proactivo para detectar cuellos de botella.
-

3 Justificación para la Junta Directiva

💡 ¿Por qué esta inversión es rentable?

- Evita pérdidas por caídas del sistema que impactan ventas.
- Mejora la experiencia del usuario con tiempos de respuesta rápidos.
- Reduce costos a largo plazo al evitar fallos e interrupciones.
- Facilita el crecimiento del negocio sin necesidad de rediseñar la infraestructura.

🚀 **Conclusión:** Con esta infraestructura, Pollito con Papas tendrá una plataforma robusta, segura y escalable, garantizando su competitividad en el mercado digital.