# Resumen primer corte

## Infraestructura de TI

Componentes de hardware, software, redes y servicios que soportan una organización

Fundamental para el proceso del negocio

Importante para experiencia amigable, continuar su operación, evita pérdidas, mejorar la toma de decisiones

### Componentes

- **Hardware:** Todo lo físico como servidores, equipos de cómputo, routers, etc...
- **Software:** Puente entre hardware y usuarios finales

> El hardware es lo que golpeamos cuando el software no funciona

- **Redes:** Sistema que conecta todos componentes para intercambiar información
- **Servicios:** Elementos que permiten gestionar, optimizar y porteger la infraestructura

  Lo que necesitamos: protegerla, optimizarla, personal que la maneje. Apoya la infraestructura para que pueda funcionar

### Modelo de capas

- Capa física: hardware

- Capa de infraestructura virtual: ejecución de más de un servicio, aplicación o sistema operativo en una sola máquina física
- Capa de aplicaciones: toda aplicacion que ayude al desarrollo de las operaciones y dependen de la infraestructura
- Capa de servicios de infraestructura: servicios como seguridad, monitoreo, respaldo, recuperación de desastres, administración de la configuración como firewall, montioreo, copias de seguridad

## Atributos no funcionales :

Lo que esperamos de nuestra infraestructura, mide la calidad del servicio

- Disponibilidad: de la información cuando se necesite, se mide en un porcentaje
- Escalabilidad: adaptable al flujo de los usuarios. Horizontal más nodos, vertical más recursos
- Seguridad: proteger datos aplicaciones y comunicaciones contra accesos no autorizados y amenazas
- Rendimiento: qué tan rápido responde a las solicitudes e interacciones

---

# Disponibilidad y estrategias de mitigación

## Disponibilidad

### MTBF : Mean Time Between Failures

Tiempo en que un dispositivo va a funcionar correctamente sin interrupción

Si es todo un dispositivo se usa el de menos duración porque es la primera falla

### MTTR : Mean Time To Repair

Tiempo que demora en repararse el componenete cuando se llega al final de su vida óptima

## Cálculo disponibilidad

$$Disponibilidad = \frac{MTBF}{MTBF + MTTR}$$

## Disponibilidad en serie

Se calcula multiplicando la disponibilidad de cada componente

$$D_{\mathrm{A}} \times D_{\mathrm{B}} \times ... \times D_{\mathrm{N}}$$

Si un componente falla, todo el sistema falla. Disminuye a medida que se agregan más componentes

> ☝🏾 "Entre más dispositivos, menos disponibilidad"

## Disponibilidad en paralelo

Con uno ya funciona

Solo no sirve si caen los 4

Disponibilidad más alta

$$\mathrm{Total} = 1 - [(1 - D_1) \times (1 - D_2) \times \cdots \times (1 - D_n)]$$

## Amenazas de la disponibilidad

- Fallos de hardware y sftware
- Errores humanos: configuraciones incorrectas, fallos operativos, malas prácticas
- Ataques extrenos
- Factores externos no controlables

## Estrategias de mitigación

### Alta disponibilidad

Arquitecturas diseñadas para maximizar el tiempo de actividad en un sistema, configuraciones resilientes

Ejemplo: replicación de datos tenemos dos bases de datos que se sincronizan en tiempo real, Failover, redundancia geográfica

## Planes de recuperación

Procedimiento y estrategias pararestaurar operaciones críticas y minimizar el impacto de interrupciones

Disaster Recovery Plan: Acciones específicas para recuperar sistmas y datos después de un desastre

> Cómo nos recuperamos de un evento disruptivo, cada organización lo ve diferente

Business Continuity Plan: Busca mantener las funciones esenciales de un negocio durante la operación

## Otras estrategias

- Monitoreo y alertas
- Automatización de respuestas
- Pruebas de estrés y simulaciones
- Educación y formación del personal

> La alta disponibilidad no garantiza un buen desempeño pero un mal desempeño da la impresión de mala disonibilidad

## Seguridad y disponibilidad

Si somos víctimas de un ataque o un incidente de seguridad de la infromación podemos comprometer nuestra disponibilidad

Se requiere medidas como un Firewall, controles de acceso, monitoreo

# Gestión de infraestructura

## Red

Interconexión de nodos hasta que es global y forma el Internet, permite la comunicación y el intercambio de recursos, información y servicios, ya sea mediante cables o ondas de radio

## LAN : Local Area Network

Redes limitadas a áreas pequeñas, como casas, oficinas o centros comerciales

Más común: casas, dispositivos se conectan para acceder a Internet, manejan direcciones privadas (192.168.x.x) y públicas (192.16.x.x)

## WAN : Wide Area Network

Redes que cubren grandes distancias y que permiten conectar múltiples redes LAN. INTERNET o bancos para conectar todas sus sucursales con el sistema central

## WLAN: Wireless LAN

Red LAN inalambrica

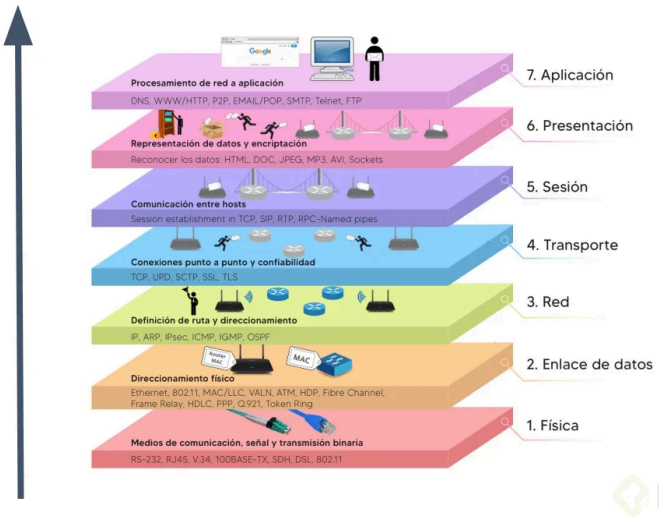
## MAN : Metropolitan Area Network

Conexión de varias redes LAN en una misma área. Ejemplo: campus universitario donde concectan oficinas, bibliotecas

## PAN : Personal Area Network

Red muy pequeña y personal. Conecta con dispositivos cercanos

## Modelo OSI




- **Capa 1 - Física**: hardware (cables)
- **Capa 2 - Enlace de Datos**: Convierte la red en 0s y 1s para que viajen por el cable (MAC)
- **Capa 3 - Red**: IP y enrutamiento
- **Capa 4 - Transporte**: Decide cómo enviar la información
  - **TCP**: Más confiable, pero más lento
  - **UDP**: Más rápido
- **Capa 5 - Sesión**: Establece y mantiene la comunicación entre dispositivos
- **Capa 6 - Presentación**: Prepara los datos para la aplicación, también puede cifrar
- **Capa 7 - Aplicación**: Donde el usuario interactúa con servicios (HTTP, HTTPS, correo)

## ¿Qué es subnetting?

Dividir una red en redes más pequeñas para optimizar la asignación de direccione sy mejorar la eficiencia en la comunicación

Mejora la seguridad al segmentar redes y facilita la administración de redes grandes

# Rango de IP privadas

- Clase A: 10.0.0.0 a 10.255.255.255
- Clase B: 172.16.0.0 a 172.31.255.255 → Universidad
- Clase C: 192.168.0.0 a 192.168.255.255 → Casa

# Máscara de subred

Nos permite identificarcuantos hosts podemos tener en una red definida

## Hosts permitidos por máscara

| | |
|---|---|
| /24 | 254 |
| /25 | 126 |
| /26 | 62 |
| /27 | 30 |
| /28 | 14 |
| /29 | 6 |
| /30 | 2 |

# Componentes

## NIC o tarjeta de red

Punto de conexión entre un dispositivo y la red

- NIC Cableada: Utiliza conectores RJ45, se conecta a la LAN por cable
- NIC Inalámbrica: Utiliza señales de radiofrecuencia para la comunicación con puntos de acceso

La dirección MAC de las NIC son únicas

## Switches

Multitoma de la red, conecta varios dispositivos en una red, utiliza direcciones MAC para llegar al destino correcto

- Capa 2 (switch tradicional): usa direcciones mac y funciona dentro de una misma LAN
- Capa 3 (con enrutamiento): puede manejar IPs y hacer la función deun router

Tipos de switches:

- No administrable: conectar y ya, no tiene opciones de configuración
- Administrable: permite configurar VLANs, seguridad de puertos, permisos, y más

### Router

Enruta, conecta diferentes redes y dirige los paquetes hacia sus destinos

- Doméstico: combina varias funciones como DHCP, Firewall, y hasta wifi
- Empresearial: Maneja grandes volúmenes de tráfico y múltiples rutas

**Funciones**

- NAT: navegamos internet con una IP pública, la traducción de IP privada a publica para internet la hace nat
- DHCP: Asigna direcciones IP dinámicamente a los dispositivos

### Firewall

Controla el tráfico entrante y saliente según reglas definidas

## Roles básicos de servidores

### Servidor DNS

Traduce los nombres de dominio por la IP relacionada

### Servidor DHCP

Asigna automáticamente direcciones IP a dispositivos en una red, evitando configuraciones manuales y posibles conflictos

Reservas DHCP son direcciones que siempre se van a asignar a una MAC específica

### Servidor de archivos

Permite almacenar y compartir archivos de manera centralizada a través de protocolos

### Servidor web

Aloja sitios y aplicaciones web

### Servidor de correo

Gestiona envío y recepción de correos

- SMTP: enviar

Recibir

- POP3: recibe y lo borro
- IMAP: lo muestra en las dos bicaciones

### Servidor de autenticación

Gestiona el acceso a la red verificando credenciales, lleva mejor el control de roles y permisos

**Controlador de dominio**: encargado de gestionar los permisos de acceso a los recursos dentro de un dominio de red

---

# Gobernanza de TI

Estrategias, herramientas y procesos que puede tener una organización para garantizar la eficacia de la tecnología para alcanzar los objetvios

## TOGAF (The Open Group Architecture Framework)

Marco de referencia para desarrollar arquitecturas empresariales eficientes y alineadas con los objetivos de una organización. Su objetivo es reducir costos y riesgos

**Dominios**

- **Arquitectura de negocio:** Procesos y estructura organizacional

- **Arquitectura de datos:** Modelo de gestión de la información
- **Arquitectura de aplicaciones:** Software y su integración
- **Arquitectura tecnológica:** Infraestructura

Aplicativos centralizados permite que no hayan redundancia

### ADM de TOGAF

Proceso en 8 fases:

1. Visión de arquitectura → Definir objetivos y expectativas del negocio
2. Arquitectura de negocio → Procesos clave
3. Arquitectura de datos → Estructura y flujos de datos
4. Arquitectura de aplicaciones → Sistemas de software
5. Arquitectura tecnológica → Hardware y redes
6. Oportunidades y soluciones → Evaluar costos y beneficios
7. Plan de migración → Diseñar la implementación
8. Gobernanza y gestión → Supervisar y optimizar el modelo

¿Quiénes usan TOGAF? Empresas de cualquier tamaño

### Beneficios

- Debe concer objetivo de la empresa
- Reduce costos y elimina redundancias
- Mejor interoperabilidad entre sistemas
- Estandariza la gestión de TI

## ITIL - Informaiton Technology Infraestructure Library

Marco de buenas prácticas para la gestión eficiente de servicios de TI con enfoque en la mejora continua y necesidades del negocio

### Principios

- Enfocarse en el valor → Entrega de valor al cliente
- Comenzar donde estás → No reinventar procesos, sino optimizar lo que ya funciona
- Progresar iterativamente con retroalimentación → Implementar mejoras en pequeños pasos
- Colaborar y promover visibilidad → Involucrar a todas las partes interesadas
- Pensar y trabajar de forma holística → Considerar a toda la organización y no solo TI
- Mantenerlo simple y práctico → Evitar burocracia innecesaria
- Optimizar y automatizar → Usar tecnología para mejorar eficiencia sin perder calidad

### Dimensiones de la gestión de servicios

- Organización y personas: Roles y responsabilidades en TI
- Información y tecnología: Datos, Herramientas, Plataformas
- Socios y proveedores: Relaciones con terceros
- Procesos: Cómo se entregan los servicios

### Objetivos clave

- Definir claramente los servicios que ofrece TI
- Gestionar incidentes y solicitudes de manera eficiente
- Optimizar el uso de recursos tecnológicos
- Asegurar la disponibilidad y continuidad de los servicios

## COBIT - Control Objective for Information and Related Technologies

Marco de gobernanza y gestión de TI desarrollado por ISACA, que alinea la tecnología con los objetivos organizacionales

☝🏽 Tecnología aporta valor al negocio cuando nos integramos con los objetivos de la organización

## Principios

- Satisfacer las necesidades de las partes interesadas
- Cubrir toda la organización, no solo TI
- Aplicar un enfoque basado en procesos
- Separar la gobernanza de la gestión

| Gobernanza de TI | Gestión de TI |
|---|---|
| Enfoque estratégico | Enfoque táctico |
| Involucra a la alta dirección | Involucra sólo a equipos técnicos |
| Define principios, políticas y estructura | Implementa procesos y soluciones tecnológicas |

- Integrarse con otras normas y marcos de referencia
- Crear valor a través del gobierno de TI

## Gestión de riesgos con COBIT

- Seguridad de la información (protección contra ciberataques)
- Disponibilidad de servicios (prevención de fallos en sistemas)
- Cumplimiento regulatorio (cumplir con HIPAA, ISO 27001, PCI DSS, etc.)
- Alineación estratégica (garantizar que TI aporta valor al negocio)

# Diferencias

| Característica | COBIT | ITIL | TOGAF |
|---|---|---|---|
| Propósito | Gobernanza de TI y control | Gestión de servicios de TI | Arquitectura empresarial |
| Foco principal | Alineación TI-Empresa, cumplimiento | Eficiencia en servicios de TI | Diseño y desarrollo de arquitectura TI |
| Usuarios clave | Directivos, auditores | Equipos de TI, Soporte | CTO, Arquitectos empresariales |
| Ejemplo | Cumplir normativas, controlar riesgos | Optimizar soporte técnico y gestión de cambios | Definir Arquitectura de TI a largo plazo |

## Mejor ejemplo

> El banco del pollito utiliza COBIT para cumplir con regulaciones, ITIL para gestionar incidencias en soporte técnico y TOGAF para diseñar la arquitectura de su infraestructura tecnológica

## DevOps

Metodología que integra desarrollo y operaciones para mejorar eficiencia, reducir tiempos de despliegue y minimizar errores en producción

**Beneficios:**

- Menor tiempo entre desarrollos y despliegues
- Automatización en pruebas y monitoreo
- Alineación entre desarrollo y operaciones
- Implementaciones seguras y escalables

# DevSecOps

Extiende DevOps incorporando seguridad desde el inicio del desarrollo

Ejemplo: Seguridad en desarrollo de software

- Evitar SQL Injection validando entradas
- Uso de autenticación multifactor (MFA)
- Monitoreo y análisis de logs para detectar anomalías

## Herramientas clave

- Integracion y entrega continua facilitar automatización de pruebas
- Infraestructura como código: Permite gestionar servidores, redes y recursos mediante código
- Contenedores: Permiten empaquetar aplicaciones y sus dependencias para que funcionen de manera consistente
- Monitoreo y Logging: Detectar problemas y comportamientos anómalos en tiempo real
- Seguridad: Logs, integrar herramientas y prácticas de seguridad durante todo el ciclo de vida de software. Permite detectar errores y vulnerabilidades mucho antes de salir a producción.
  Hash se usa para decir log es real y podemos usar en una investigación

# CMMI - Capability Maturity Model integration

Marco de referencia para evaluar y mejorar la madurez de los procesos organizacionales

## Niveles de madurez

1. Inicial→ No cuenta con procesos definidos ni control
2. Gestionando→ Se documentan procesos basicos y controlan proyectos
3. Definido → Procesos estándar definidos en la organización
4. Cuantitativamente gestionado → Se utilizan métricas para mejorar procesos

5. Optimizado→ Mejora continua basada en innovación

### Beneficios de CMMI

- Reducción de costos y retrasos en proyectos.
- Aseguramiento de calidad en productos y servicios.
- Mejor toma de decisiones basada en métricas.
- Alineación de TI con estrategias empresariales.

# Seguridad por capas

Como protegemos nuestra infraestructura

## Seguridad física

- Controles de acceso, biometría, cámaras de seguridad
- Protección contra desastres naturales (piso elevado, energía redundante)

## Seguridad perimetral

- Firewalls, IDS/IPS, VPNs seguras
- Uso de WPA3 para redes inalámbricas

## Seguridad en la red interna

- VLANs, listas de control de acceso (ACL)
- Firewall interno para segmentación de red

## Seguridad en los dispositivos (Host)

- Parches de seguridad y actualizaciones constantes
- Antivirus y monitoreo de logs
- Hardenización: eliminar configuraciones por defecto

## Seguridad en aplicaciones:

- Desarrollo seguro y validación de entradas
- Gestión adecuada de accesos y autenticación

## Seguridad de los datos

- Cifrado de información
- Copias de seguridad y estrategias DLP (Data Loss Prevention)