Primer corte

Introducción

- Atributos no funcionales gestión de infraestructura frameworks
- Virtualización, sistemas operativos, gestión de riesgos, gestión de infraestructura
- Gestión de infraestructura, cloud

Infraestructura de TI

Son los componentes de hardware, software, redes y servicioes que soportan una organización

Fundamental para el proceso del negocio

Importante para:

- Ofrecer una experiencia amigable con clientes, empleados y partes involucradas
- Permite a las organizaciones continuar su operación
- Evita pérdidas económicas y/o reputacionales
- Mejora la toma de decisiones

Componentes

Hardware

Todo lo físico como servidores, equipos de cómputo, routers, etc...

Software

Puente entre hardware y usuarios finales como sistemas operativos, aplicaciones empresariales como CRM , ERP, entre otros

☝🏾 El hardware es lo que golpeamos cuando el software no funciona

Redes

Sistema que conecta todos los componentes de la infraestructura de TI para intercambiar información

Primer componente: la red

Servicios

Elementos que permiten gestionar, optimizar y porteger la infraestructura como soluciones de virtualización, servicios en la nube y herramientas y políticas de seguridad

Segundo componente: los servicios

Lo que apoya la infraestructura para que pueda funcionar

Lo que necesitamos: protegerla, optimizarla, personal que la maneje

▼ Caso *Pollito con papas*

¿Qué necesitamos?

- Plataforma puede estar alojada en nube o en infra

Hardwware

Cajas registradora

Terminales POS: puente entre la caja registradora y el datáfono para colocar el precio exacto sin digitarlo

Datáfono

Cámaras de seguridad

Servidores

Computadores

NAS: pila de discos, varios discos para hacer copia de seguridad

Software

Sistema POS: el que tiene la cajita anterior

Aplicación de domicilios

Sistema de invetarios

Sistema de monitoreo de cámaras

Redes

LAN cada sucursal

VPN para concetar sucursales

Internet

WiFi clientes

Servicios

Virtualización

Servicios cloud

Área de TI

Firewall

IPS

> ☝🏾 Tarjeta presente es cuando se mete en el datáfono, no presente es cuando se meten los datos en internet

Modelo de capas

Más fácil identidicar un problema

Tenemos:

- Capa física: todos los dispositivos con los que cuenta la infraestructura incluyendo los de energía y enfriamiento. en resumen: hardware
- Capa de infraestructura virtual: ejecución de más de un servicio, aplicación o sistema operativo en una sola máquina física. virtualbox/vmware, servidores virtuales, contenedores virtuales, redes virtuales

- Capa de aplicaciones: toda aplicacion que ayude a el desarrollo de las operaciones y dependen de la infraestructura como desarrollos, aplicación de domicilios, bases de datos, herramientas de colaboración
- Capa de servicios de infraestructura: proporciona 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

Con estos definimos la calidad del sistema

- Disponibilidad: de la información cuando se necesite, se mide en un porcentaje
- Escalabilidad: adaptable al flujo de los usuarios (picos como black friday, crecimiento de la empresa). Horizontal más nodos, vertical más recursos
- Seguridad: proteger los datos aplicaciones y comunicaciones contra accesos no autorizados y amenazas. Puede incluir autenticación, autorización, cifrado, monitoreo de amenazas...
- Rendimiento: qué tan rápido responde a las solicitudes e interacciones, que el servidor no vaya a echar candela. Se mide en tiempo de respuesta y capacidad de procesamiento

Actividad

Organización elegida: Upper

> Aplicación colombiana de transporte en Cartagena (también tienen su sede administrativa aquí), Barranquilla y Santa Marta, tienen app para conductores y para pasajeros, prestan servicios de taxi, helicóptero y mototaxi, por lo que deben conectarse con las empresas de taxi y helicóptero con las que tienen convenio

Dibujen la infraestructura que propondrían de la organización teniendo en cuenta las 4 capas vistas

¿Cómo garantizan la disponibilidad, escalabilidad, seguridad y rendimiento de su infraestructura?

Esto cuesta dinero, véndale a la junta directiva su propuesta y convénzalos de por qué esta propuesta es atractiva y cómo en vez de gastar, van a ahorrar.

Disponibilidad y estrategias de mitigación !

Disponibilidad

Hablemos de 9s

Disponibilidad (%)	Downtime por año
99.0%	3.65 días
99.9%	0.36 días
99.99%	8.76 horas
99.999%	5.26 minutos
99.9999%	31.5 segundos

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 duraciónporque es la primera falla

Ejemplo: MTBF del iphone 15 pro es de 1 millón de hora

MTTR : Mean Time To Repair

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

Cálculo disponibilidad

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

Donde:

- **MTBF (Mean Time Between Failures)**: Tiempo medio entre fallos
- **MTTR (Mean Time to Repair)**: Tiempo medio de reparación
- **Disponibilidad**: Probabilidad de que un sistema esté operando correctamente en un momento dado

Si:

$$\mathrm{MTBF} = 1,000,000\ \mathrm{h}$$
$$MTTR = 24h$$
$$D_A = \frac{1,000,000}{1,000,000 + 24}$$
$$DA = \frac{1,000,000}{1,000,024} = 0.999976 \times 100\% = 99.9976\%$$

Ejemplo

Componente	MTBF	MTTR	Disponibilidad
Cisco	789,465 h	3 días = 72 h	99.9908%
PC	50,000 h	18 h	99.96401%
Servidor	250,000 h	4 días = 96 h	99.9616%
Impresora	50,000 h	1 día = 24 h	99.95202%

Ahora, de todo:

(Libro) → (Router) → (Servidor) → (Impresora)

99.9908% → 99.964% → 99.9616% → 99.952%

Todo depende de todo, si uno falla, todo falla

Para disponibilidad de todas:

1. Disponibilidad en *int* no en %
2. Multiplicarlas entre sí

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

La disponibilidad disminuye a medida que se agregan más componentes

Es decir que para el ejemplo:

$$D_{\text{cisco}} \times D_{\text{pc}} \times D_{\text{serv}} \times D_{\text{impr}} = 99.8264\%$$

99.8264% → **Disponibilidad de todo el sistema**

> ☝🏽 "Entre más dispositivos, menos disponibilidad"

Disponibilidad en paralelo

- Con uno ya funciona
- Solo no sirve si caen los 4
- Disponibilidad más alta

Se calcula como:

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

Es decir que para el ejemplo:

$$= 0.999999999999938753216$$

Es de casi el 100%

Ejercicio de disponibilidad

Calcular disponibilidad en serie y jugar con paralelos para encontrar el mejor modelo

Componente	MTBF	MTTR	Costo
Seguridad	7 años → 61320 h	24 h	$9,000

Componente	MTBF	MTTR	Costo
Almacenamiento	30 años → 262,800 h	6 días → 144 h	$20,000
Energía	-	-	100%
Procesos	10 años → 87,600 h	3 días → 72 h	$10,000

Disponibilidad de cada dispositivo

Componente	Disponibilidad
Seguridad	0,99960876
Almacenamiento	0,99945235
Energía	1,00000000
Procesos	0,99917876

Disponibilidad total en serie

$$D_{total} = 99.9609\% \times 99.9452\% \times \ 99.9179\% \\ = 0,99824086089 = 99,82409\%$$

Resultado: La disponibilidad es menor al umbral deseado

Ahora, mejoremos la disponibilidad con redundancia

Podemos ver que la disponibilidad de todas las instancias es menor que la pedida entonces agrego una a cada uno, sí o sí

Para esto agregamos componentes redundantes en paralelo

Si duplicamos cada componente (*dos de cada uno*), la nueva disponibilidad por dispositivo será:

Componente	Disponibilidad
Seguridad	99,999985%
Almacenamiento	99,999970%
Energía	100%
Procesos	99,999933%

Ahora, la nueva disponibilidad total es:

$$D_{total} = 99,9998873\%$$

Esta ya supera la disponibilidad del umbral

Aumenta los costos por

Componente	Costo
Seguridad	$ 18,000
Almacenamiento	$ 40,000
Energía	
Procesos	$ 20,000

Amenazas de la disponibilidad

- Fallos de hardware y sftware: se nos daña algún componente, como que se dañe la fuente de poder
- Errores humanos: configuraciones incorrectas, fallos operativos, malas prácticas como dejar admin admin en el router
- Ataques extrenos: intrusione sdeliberadas que agectan la operación, malware, et
- Factores externos: no controables como desastres naturales, cortes de energía, problemas de conectividad

Estrategias de mitigación

Alta disponibilidad

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

Ejemplo: replicación de datos tenemos dos bases de datos que se sincronizan en tiempo real, Failover, redundancia geográfica: una parte de la infra en un sitio geográfico y otra en otro lugar

Planes de recuperación

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

DRP (Desaster Recovery Plan): Acciones especígicas para recuperar sistmas y datos después de un desastre

Cómo nos recuperamos de un evento disruptivo como cuando se inundó el campus

Cada organización lo ve diferente

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

Como irnos a virtualidad cuando no podemos ir virtualmente

Otras estrategias

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

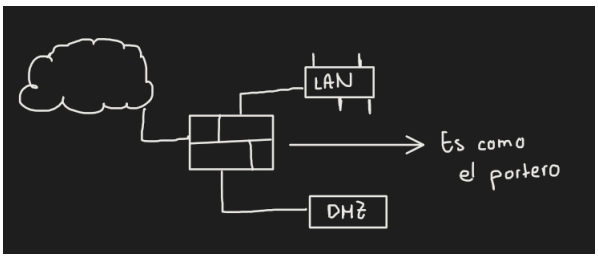
Desempeño y disponibilidad

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



Dejamos primero reglas de tráfico que queremos permitir y luego que niegue todo lo demás. Es mejor identificar lo que tenemos que permitir

Funciona con las IPs de origen o destino, y con puertos

Gestión de infraestructura

¿Qué es una red?

Tengo a pepito y a sutanito, entre los dos se conectan. Tienen una comunicación de doble vía y entre los dos se comunican. Luego llegan los primos y también se conectan 😛

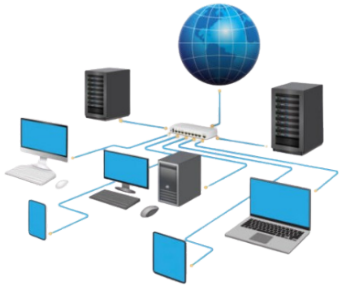
Cuando varios nodos se conectan entre sí, crecen tanto que se conecta todo el mundo y se convierte en internet

Conjunto de dispositivos interconectados que comparten recursos, información o servicios

Pueden ser físicas (cables) o inalámbricas (ondas de radio)

Permiten comunicación entre dispositivos y usuarios

¿Qué es una red LAN?



Local Area Network

Redes que se limitan a áreas pequeñas como redes en casas, oficinas, instituciones educaticas, centros comerciales, entre otros

La LAN más común es la de las casas y a las que se conectan nuestros dispositivo para salir a internet

Maneja direcciones de tipo privado 192.168.x.x

Publicas 192.16.x.x

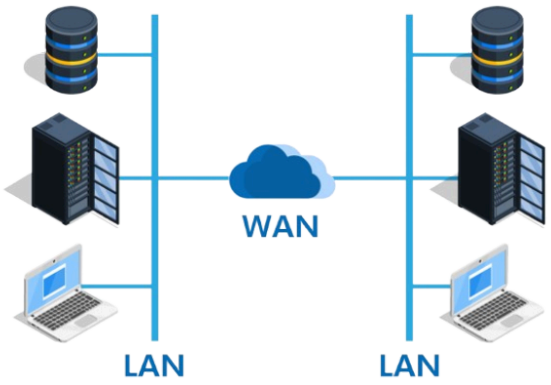
¿Qué es una red WAN?

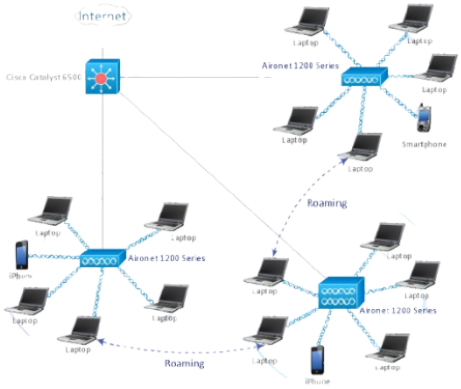
Wide Area Network

Redes que cubren grandes distancias y que permiten conectar múltiples redes LAN

El mejor ejemplo es INTERNET

Otro ejemplo es la utilizada por los bancos para conectar todas sus sucursales con el sistema central





¿Qué es una red WLAN?

Wireless LAN

Red LAN inalambrica, no utiliza cables sino que trabaja mediante WiFi para conectar sus dispositivos

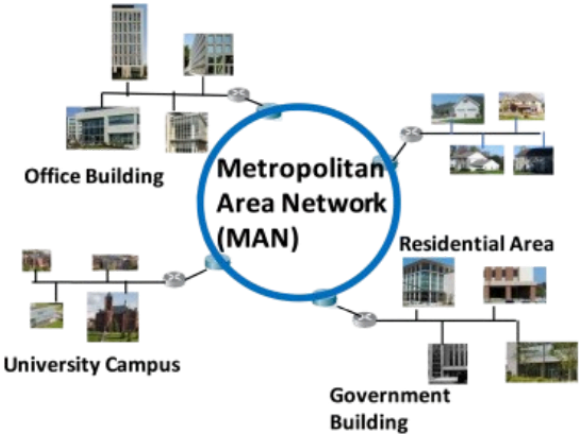
Se pueden conectar de forma inalambrica

¿Qué es una red MAN?

Metropolitan Area Network

Conexión de varias redes LAN en una misma área

Ejemplo: campus universitario donde concectan oficinas, bibliotecas



¿Qué es una red PAN?

Personal Area Network

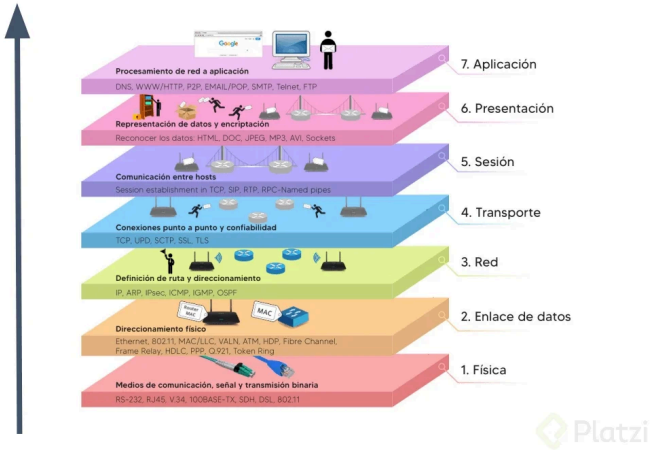
Red muy pequeña y personal

Conecta con dispositivos cercanos

Como cuando conectamos a relojes inteligentes, los audífonos, etc

Diferencias entre OSI y TCP/IP

Saberlo de memoria !!



Capa 1 tiene los cables

Capa 2 se encarga de volver la red en 0 y 1 para que se vayan por el cable. También encontramos la MAC

Capa 3 tiene la IP y el enrutamiento, tracert nos muestra la ruta

Capa 4 es transporte cuál es la mejor manera de enviar nestra información y hacia dónde queremos llevarla

TCP no es tan rápido pero es más confiable porque llega completo, UDP es más rápido

Capa 5 establece la sesión y busca mantenerla lo más posible

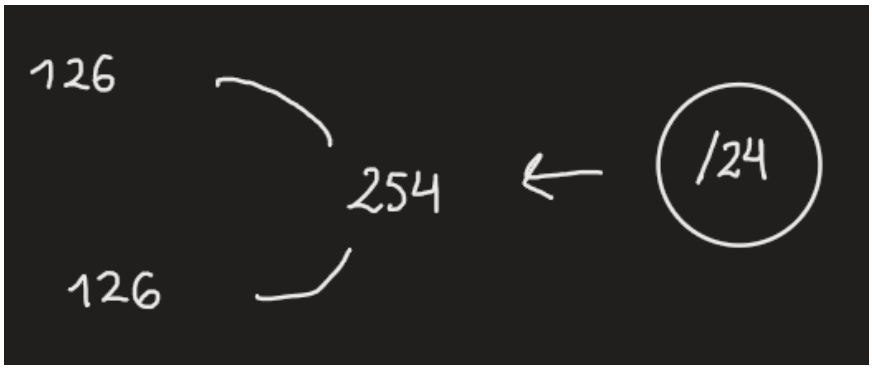
Capa 6 es presentación, los datos fueron procesados de tal manera que ya la aplicación los puede procesar, también puede cifrarlos. Como youtube que mira qué tan congestionado está el canal y de ahí mira qué calidad de video poner

Capa 7 es aplicación, donde el usuario final ya interactua con servicios de correo, http, https

¿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

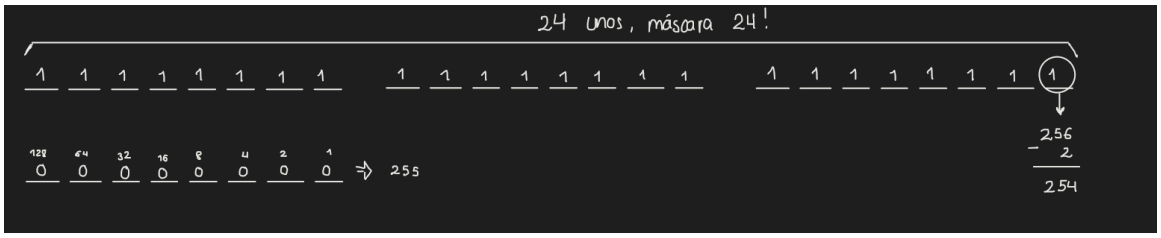


Rango de IP privadas

- 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

Si tengo la red

$$192.168.50.0/24$$

Puedo utilizar el rango de IPs:

$$192.168.50.1 - 192.168.50.254$$

El 1 es el getaway y el 255 el broadcast

Ejercicio

Red con submáscara de 25

$$192.168.50.0/25$$

$$192.168.50.0 - 192.168.50.127$$

Red con submáscara de 23

$$192.168.50.0/23$$

$$192.168.50.0 - 192.168.51.255$$

Compumundohipermegared ha crecido y el departamento de infraestructura ha decidido separar las principales áreas de la organización en redes separadas. Por este motivo han decidido dividir en 4 la red corporativa que cuenta con el siguiente direccionamiento:

$$192.168.101.0/23$$

¿Cuál sería el nuevo diseño de la red teniendo en cuenta lo requerido por el área de infraestructura?

La red con máscara 23 tiene 510 IPs disponibles, necestiamos cuatro entonces dividí esos 512 entre 4 y me dio 128 por lo que las cuatro subredes me quedaron de la siguiente forma:

- 192.168.101.1-192.168.101.126
- 192.168.101.129-192.168.101.254
- 192.168.102.1-192.168.102.126
- 192.168.102.129-192.168.102.254
- 192.168.101.0/25
- 192.168.101.128/25
- 192.168.102.0/25
- 192.168.102.128/25

De esta manera tenemos que:

Subred	Dirección de Red	Rango de hosts (IPs Utilizables)	Dirección de Broadcast
Subred 1	192.168.101.0/25	192.168.101.1 - 192.168.101.126	192.168.101.127
Subred 2	192.168.101.128/25	192.168.101.129 - 192.168.101.254	192.168.101.255
Subred 3	192.168.102.0/25	192.168.102.1 - 192.168.102.126	192.168.102.127
Subred 4	192.168.102.128/25	192.168.102.129 - 192.168.102.254	192.168.102.255

Componentes

NIC o tarjeta de red

Actúa como punto de conexión entre un dispositivo y la red

Existen dos tipos:

- 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

```
ipconfig /all
```

Switches

Multitoma de la red

Conecta varios dispositivos en una red, utiliza direcciones MAC para llegar al destino correcto

Exiten para capa 2 y capa 3:

- 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

Existen 2 principales tipos de routers:

Doméstico: combina varias funciones como DHCP, Firewall, y hasta wifi

Empresearial: Maneja grandes volúmenes de tráfico y múltiples rutas

Funciones de los router

- NAT: Permite que todos los dispositivos conectados naveguen a través de una misma IP pública. Navegamos internet con una IP pública, la traducción de nuestra privada a el 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

Primero consultan el caché, si no encuentran revisan otros servidores, los comunes son:

- Google: 8.8.8.8
- OpenDNS: 208.67.222.222

```
nslookup google.com 8.8.8.8
```

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 como SMB (Windows) o NFS (Linux)

Servidor web

Aloja sitios y aplicaciones web

Ejemplos:

- Apache HTTP Server (Linux)
- NGINX
- IIS (Windows Server)

Externo es el hosting de godaddy, etc...

En windows se maneja IIS

Servidor de correo

Gestiona envío y recepción de correos

- SMTP: enviar

Recibir

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

Los conocidos son Microsoft Exchange Server, Postfix

Servidor de autenticación

Gestiona el acceso a la red mediante la verificación de credencial. Active Directory

Este servicio permite centralizar la gestión de accesos y llevar un mejor control de los roles y permisos de los usuarios. Se le bloquea la cuenta a un usuario que se va

Controlador de dominio o directorio activo

Controlador de dominio: ciñe a las políticas de la empresa, centraliza la autenticación. Le bloquean el usuario, le resetean la contraseña, gestionan

permisos, limitan intentos de contraseña

Resumen OSI

Gobernanza de TI !

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

Busca facilitar la comunicación entre diferentes áreas de negocio de TI

El principal objetivo es reducir costos y riesgos

No busca cubrir TI en sí, sino la forma en la que TI apoya los objetivos empresariales

Cuenta con 4 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

Pregunta

Imagina una empresa que cuenta con un aplicativo para nómina, otro para gestión documental, otro para contabilidad, otro para tecnología. ¿Qué consecuencias podría traer esta cantidad de sistemas separados? En esta clase no quieren a

SIGA, pero es un sistema que abarca muchos procesos de la universidad en conjunto.

- **Integración deficiente y fragmentación de datos:** Los sistemas separados dificultan la unificación de datos, generando inconsistencias y duplicaciones
- **Ineficiencia operativa:** Se requiere ingresar los mismos datos en diferentes plataformas, aumentando el tiempo de trabajo y errores
- **Costos elevados en mantenimiento, capacitación, soporte...:** Cada sistema requiere su propio mantenimiento, licencias y actualizaciones
- **Toma de decisiones con mayor complejidad:** La falta de visión consolidada dificulta la toma de decisiones estratégicas
- **Problemas de seguridad y cumplimiento:** Cada sistema necesita controles de acceso propios eso aumenta los riesgos de vulnerabilidades y problemas de cumplimiento

ADM de TOGAF

Hay 8 fases definidas:

1. Visión de arquitectura → Definir objetivos y expectativas del negocio

   Debemos saber la ivsión de la organización a donde queremos llegaar los obejtivos etc. TI debe entender el para qué, para qué necesitamos el firewall, tener la red así y así y así, y cómo ayuda a cumplir con la operacion estratégica

2. Arquitectura de negocio → Procesos clave

   Como como TI apoyamos las expectativas del negocio

3. Arquitectura de datos → Estructura y flujos de datos
4. Arquitectura de aplicaciones → Sistemas de software

   Aplicacion todo lo que sea software

5. Arquitectura tecnológica → Hardware y redes

   Tech hardware y software para saber como nos está yendo

6. Oportunidades y soluciones → Evaluar costos y beneficios

Siempre mostrar que la infraestructura es una inversion no un costo ya que apoya al negocio

7. Plan de migración → Diseñar la implementación

   Diseño implementación

   Si sirve no lo toque: no se deja sin tocar por años

8. Gobernanza y gestión → Supervisar y optimizar el modelo

¿Quiénes usan TOGAF?

Empresas de todos los tamaños (grandes y pequeñas):

- Empresas de tecnología como Google o Microsoft
- Entidades financieras
- Entidades gubernamentales
- Organizaciones con sistemas de TI complejos

Beneficios de TOGAF : ¿Qué es lo que busca TOGAF?

- Debe concer objetivo de la empresa
- Reducir costos y tiempos eliminando redundancias
- Mejor interoperabilidad entre sistemas y aplicaciones
- Mejor gobernanza en la gestión de TI

Pregunta

La universidad de Los Alpes planea digitalizar sus servicios administrativos y académicos, pero cada facultad cuenta con su propio sistema por aparte. Así como cada dependencia en la Universidad. ¿Teniendo en cuenta el uso de TOGAF, como ayudarían a la Universidad de Los Alpes a mejorar sus procesos y qué beneficios les traería el uso de TOGAF?

Creando una única plataforma universitaria para matrículas, pagos y notas, optimizando el flujo de información y evitando duplicación de registros

- **Análisis de la situación actual:** Identificar sistemas independientes usados por facultades, evaluar comunicación y limitaciones de los sistemas, detectar

redundancias e ineficiencias.

- **Definir la arquitectura objetivo:** Crear una arquitectura integrada para todas las facultades y unificar la información académica, administrativa y financiera
- **Desarrollar un plan de migración:** Implementar la integración gradualmente según fases de TOGAF, establecer arquitectura de negocio, datos, aplicaciones y tecnología
- **Gobernanza y gestión de cambio:** Implementar un modelo de gobernanza de TI y capacitar usuarios y establecer indicadores de rendimiento

Beneficios

- Estandarización de procesos
- Mejor interoperabilidad entre sistemas y plataformas
- Reducción de costos (redundantes)
- Información consolidada
- Mayor eficiencia operativa en procesos clave

> ☝🏽 Tener info en diferentes sistemas genera incomodidad en todos y cuando los empleados no están felices se van

ITIL - Informaiton Technology Infraestructure Library

Es un marco de buenas prácticas para la gestión de servicios de TI

Buscamos servicios eficientes y mejora continua

Enfoque en las necesidades de negocio

En la actualidad ha dejado de ser adoptado solo para tecnología, también en gestión de servicios

Principios

Hay que partir desde donde ya estamos

- 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

Un proyecto grande no es ya para ya, se hacen mejoras de a pocos

La idea es que la tecnología nos ayude a ser mas eficientes, pero mejorando la calidad de los servicios

- 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

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

Pregunta

Si tú trabajaras en el área de TI de una organización, ¿cómo abordarías las siguientes situaciones?

- Un usuario olvidó su contraseña y necesita acceso urgente a su correo electrónico

    - **Verificación de identidad**: Confirmar identidad mediante preguntas de seguridad, SMS o email alternativo
    - **Restablecimiento de contraseña**:
        - Si tiene portal de autoservicio, guiarlo en la recuperación
        - Si no, generar nueva contraseña temporal y forzar cambio en primer inicio de sesión
- El Firewall corporativo dejó de funcionar, y la navegación tanto interna como externa no se encuentra funcionando
    - Escalamiento inmediato al equipo de seguridad y redes
    - Identificación de la causa
        - Problema de hardware (fallo físico del firewall)
        - Problema de software (error de configuración o actualización fallida)
        - Ataque de seguridad (DDoS, intrusión)
    - Plan de contingencia activado:
        - Si hay redundancia (HA), activar el dispositivo de respaldo
        - Si no configurar regla temporal en routers o firewall en la nube
    - Plan de rollback (si la falla ocurrió tras un cambio reciente): revertir a la configuración anterior
    - Registro del incidente en sistema de gestión: documentar tiempo de inactividad y acciones tomadas
    - **Medidas preventivas**:
        - Implementar redundancia con firewalls en alta disponibilidad (HA).
        - Definir procedimientos de prueba antes de cambios críticos.
        - Monitoreo y alertas tempranas para detectar fallos antes de que impacten.
- Se requiere actualizar el sistema de facturación, pero hay un riesgo de interrupción del servicio

- Evaluación del impacto y riesgo: actualización crítica o menor, afecta procesos de negocio esenciales? plan de rollback en caso de fallas
- Evaluar con el comité de cambios y aprobarlo
- Programar actualización fuera de horario laboral o en ventana de mantenimiento, notificar a las áreas afectadas con anticipación
- Realizar la actualización en un entorno de pruebas y si todo funciona bien implementar en producción
- Supervisar rendimiento del sistema. tener un equipo de soporte listo para responder a fallas y si algo sale mal rollback

COBIT - Control Objective for Information and Related Technologies

De nuevo es importante conocer el objetivo del negocio para que el área de TI agregue valor a la organización

Objetivo es garantizar que la tecnología y los sistemas de información aporten valor al negocio, alineándose con los objetivos de la organización

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

NO es un marco operativo como los anteriores, es un marco de gobernanza y gestión de TI desarrollado por ISACA

- Define controles y buenas prácticas en el uso de TI
- Facilita el cumplimiento de normas y regulaciones (ISO 27001, PCI DSS, etc.)
  - **PCI DSS** es un estándar de seguridad para el procesamiento de pagos

    Diseñado para proteger la información sensible durante las transacciones

    ¿Qué datos contienen las tarjetas de crédito (TC)?

    1. Número de tarjeta (16 dígitos)
    2. Fecha de vencimiento

3. CVV (Código de seguridad)
4. Nombre del titular

   Regula el manejo de esta información, establece que NO se puede almacenar el CVV

   Puede guardar solo los primeros 6 dígitos y los últimos 4 dígitos del número de tarjeta, pero no se debe almacenar el CVV ni los datos completos de la tarjeta.

- Ayuda a la alta dirección a gestionar riesgos tecnológicos

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

- Marco integrado con otras normas
- 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

Pregunta

El restaurante “El balde de carnada” enfrenta problemas de seguridad, pérdida de datos y cumplimiento normativo. La alta dirección requiere fortalecer la gobernanza de TI para evitar sanciones y así poder garantizar la continuidad del negocio. ¿Qué recomendaciones le darías a Plancton para poder mitigar los problemas que están presentando?

Lo pueden usar como guía:
https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

- Definir políticas y procedimientos de TI, asegurar el cumplimiento normativo con ISO 27001 y PCI DSS, asignar roles y responsabilidades claras en seguridad y cumplimiento.
- **Seguridad perimetral y de red:** Implementar un firewall robusto, usar IDS/IPS para detectar intrusos, configurar VPNs seguras para accesos remotos
- **Seguridad en dispositivos y endpoints:** Mantener sistemas operativos y software actualizados, implementar antivirus y monitoreo de amenazas, hardening en servidores y equipos críticos
- **Protección de datos y prevención de pérdidas (DLP):** Implementar respaldos automáticos y encriptación de datos, aplicar control de acceso basado en roles (RBAC), configurar sistemas DLP para evitar fuga de información sensible
- **Plan de recuperación ante desastres (DRP) y continuidad del negocio (BCP):** Implementar copias de seguridad automatizadas, desarrollar un plan de contingencia con recuperación rápida, realizar pruebas periódicas de recuperación de datos
- **Cumplimiento normativo y protección de datos:** Implementar un Sistema de Gestión de Seguridad de la Información con ISO 27001, cumplir con PCI DSS si se procesan pagos con tarjeta, capacitar al personal en ciberseguridad y buenas prácticas de manejo de datos
- **Comité de Seguridad y Gobernanza de TI:** Crear un Comité de Seguridad de la Información, definir una política clara de seguridad y procesos de auditoría. realizar auditorías internas y externas periódicas

DevOps

Enfoque que busca integrar el esarrollo y las operaciones para mejorar la entrega de software y la eficiencia operativa

Busca eliminar barreras entre equipos automatizar procesos y garantizar entregas rápidas y de calidad

Beneficios

- Menor tiempo entre desarrollos y despliegues
- Automatización en pruebas y monitoreo
- Alineación entre desarrollo y operaciones
- Infraestructura adaptable
- Implementaciones más seguras y menos errores en producción

> 🔑 En ambientes de prueba y desarrollo podemos usar datos reales? NO, se puede filtrar info si tenemos datos reales

DevSecOps

Integrar devops con seguridad desde inicio hasta final del desarrollo

Busca que se incorpore seguridad desde el inicio hasta el final del desarrollo

¿Qué pasaría si se implementa seguridad únicamente al final del desarrollo?

SQL Injection es una técnica de ataque donde un atacante introduce código SQL malicioso en las entradas de una aplicación para manipular la base de datos. Algunos aspectos importantes:

- Es una vulnerabilidad común que ocurre cuando las aplicaciones no validan o sanitizan adecuadamente las entradas del usuario
- Permite a los atacantes:
  - Acceder a datos no autorizados
  - Modificar información en la base de datos
  - Ejecutar comandos administrativos

Para prevenir SQL Injection se deben usar consultas parametrizadas, validar entradas y aplicar el principio de mínimo privilegio en la base de datos. No dejar poner <> “” ==

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

Evalua y mejora la madurez de los procesos organizacionales

Busca optimizar procesos internos para más eficiencia y calidad, reducir riesgos, mejorar competitvidad en el mercado

Niveles de madurez

1. Inicial→ No cuenta con procesos definidos ni controles - NO TIENE NADA
2. Gestionando→ Se documentan procesos basicos y controlan proyectos - Implementación nada, solo documentos
3. Definido → Procesos estándar definidos en la organización - Procesos estándar
4. Cuantitativamente gestionado → Se utilizan métricas para mejorar procesos - Tener mejoras continuas y medimos con esas métricas
5. Optimizado→ Mejora continua basadaen innovación - Siempre estamos en pro de la mejora continua

Beneficios de CMMI

- Gestión de proyectos eficiente reduciendo retrasos y sobrecostos

- Aseguramiento de la calidad estableciendo estándares para los productos y servicios
- Mejora en la toma de decisiones a través de métricas
- Mayor alineación entre TI y las estrategias organizacionales

Pregunta: CMMI y Pollito con Papas

Pollito con papas se encuentra presentando retrasos en las entregas de su App domicilios, se ha evidenciado:

- El equipo de desarrollo no cumple con los plazos
- Cambios constantes en los requisitos
- Los procesos no se documentan
- No cuentan con un repositorio estructurado
- Cada desarrollador utiliza su propio estilo de codificación
- No se realizan revisiones periódicas de código

¿Qué le propones a Pollito con papas para pasar de un nivel inicial a un nivel Definido, y luego Optimizado?

- Capacitación del equipo de desarrollo
- Documentación de procesos y roles: definir flujo de trabajo, roles y entregables
- Repositorio estructurado
- Estandarización del código y patrones de diseño
- Revisiones periódicas de código
- Implementación de CI/CD: automatizar pruebas y despliegues
- Monitoreo continuo y métricas de desarrollo
- Business Intelligence (BI)

Seguridad por capas

Como protegemos nuestra infraestructura

Lo primero son las puertas con portero y candado que se abre con el ojo 😛

Seguridad física

Hay que contar con controles adecuados para quienes acceden a las instalaciones

Tener porterias cámaras de seguridad, accesos de biometría, entre otros

Reja electrificada

Piso alto para evitar inundaciones

Seguridad perimetral - Los que quieren entrar por la red

Se debe tener controles adecuados para proteger red interna de otras redes o peligros que hay en internet

- WPA2
- WPA3
- WEP NO ROTA

Internet y alguien quiere entrar, debería tener un firewall gracias a reglas predefinidas

Si alguien quiere entrar desde intenet debe tener una vpn

Ejemplos: Firewall, IDS, VPN, Seguridad en la red inalámbrica.

Red Interna

Se debe contar con los controles adecuados para proteger la red interna de otros elementos que se encuentran desde la misma

Ejemplos: VLAN, Listas de control de acceso, Firewall Interno.

Seguridad en el Host

Se debe contar con los controles adecuados para proteger los equipos de cómputo y servidores que se encuentran en la organización

Parches

Antivirus

Logs

Hardenización: Quitar configuraciones y usuarios por defecto, no dejar puertas abiertas en los dispositivos

Seguridad en aplicaciones

Se debe contar con los controles adecuados para proteger la información que está involucrada con los desarrollos de la organización

App en la organización y hay datos, capacitación al desarrollador

Ejemplos: Desarrollo seguro, codificación segura, gestión de accesos adecuada

Seguridad de los datos

Se debe contar con los controles adecuados para proteger los datos que se encuentran en la organización tanto como en tránsito como en almacenamiento

Ejemplos: Cifrado de la información, Copias de seguridad, DLP

Pregunta

Pollito con papas ha crecido y desea lanzar una gran plataforma digital que contiene:

- App Domicilios
- Sistema de gestión de pedidos y logística
- Puntos Pollito con Papas – Fidelización

Sin embargo, cuentan con problemas como el uso de diferentes tecnologías para sus procesos, no cuentan con una arquitectura definidos, aplicación móvil lenta y con errores, las pruebas y controles de calidad fallan, el área de TI toma decisiones sin métricas, y no cuentan con documentación adecuada.

Finalmente, pollito con papas al manejar datos de tarjeta de crédito deben certificarse en PCI DSS e ISO 27001.

¿Cómo ayudarías a nuestro camarón Serki de Malambo a mejorar su plataforma digital teniendo en cuenta los Frameworks vistos?

1. **Definir arquitectura empresarial con TOGAF**

   Problema: Tecnologías dispares sin arquitectura definida

Acciones:

- Diseñar una arquitectura centralizada e interoperable
- Unificar sistemas bajo un modelo de capas (infraestructura, datos, aplicaciones, servicios)
- Establecer estándares tecnológicos
- Planificar migración gradual y controlada

Ejemplo: Conectar la App de Domicilios con el Sistema de Gestión de Pedidos usando APIs y Microservicios

2. **Mejorar la Calidad de Servicio con ITIL**

   Problema: Fallos frecuentes y control de calidad deficiente

   Acciones:

   - Definir y gestionar servicios como "servicios de TI"
   - Implementar gestión de Incidentes y problemas
   - Monitorear y optimizar el rendimiento con métricas
   - Garantizar alta disponibilidad y failover

   Ejemplo: Implementar un Service Desk para seguimiento de errores en la app

3. **Fortalecer Gobernanza de TI con COBIT**

   Problema: Decisiones de TI sin métricas ni documentación.

   Acciones:

   - Estandarizar procesos de TI basados en datos
   - Definir controles de acceso y seguridad
   - Alinear TI con los objetivos de negocio
   - Medir desempeño de TI con KPIs

   Ejemplo: Usar BI para monitorear métricas como disponibilidad y tiempos de respuesta

4. **Mejorar despliegues con DevOps**

   Problema: Fallos en pruebas y calidad de software.

Acciones:

- Implementar CI/CD para evitar errores en lanzamientos
- Automatizar pruebas de calidad
- Usar contenedores (Docker, Kubernetes) para escalabilidad
- Monitorear continuamente el rendimiento de la app

Ejemplo: Configurar pipelines de CI/CD con pruebas automatizadas antes de despliegues

5. **Estandarizar desarrollo de software con CMMI**

   Problema: Falta de documentación y procesos en el desarrollo.

   Acciones:

   - Definir procesos claros con roles y responsabilidades
   - Implementar revisiones de código y estándares de programación
   - Monitorear la eficiencia en el desarrollo

   Ejemplo: Estandarizar frameworks y lenguajes para mantener orden en el código

6. **Cumplir con PCI DSS e ISO 27001 para Seguridad**

   Problema: Gestión de pagos y datos sin cumplimiento normativo

   Acciones:

   - Cifrar datos sensibles y segmentar redes
   - Implementar autenticación multifactor (MFA)
   - Establecer políticas de retención y eliminación de datos
   - Monitorear actividades sospechosas y realizar auditorías regulares

   Ejemplo: Crear un entorno seguro para pagos evitando almacenamiento no certificado de datos de tarjetas

Resultados esperados:

- Arquitectura definida y unificada
- Eficiencia en servicios TI

- Gobernanza estructurada
- Automación y calidad en el desarrollo
- Cumplimiento de normativas de seguridad