Trabajo Final Modulo 1

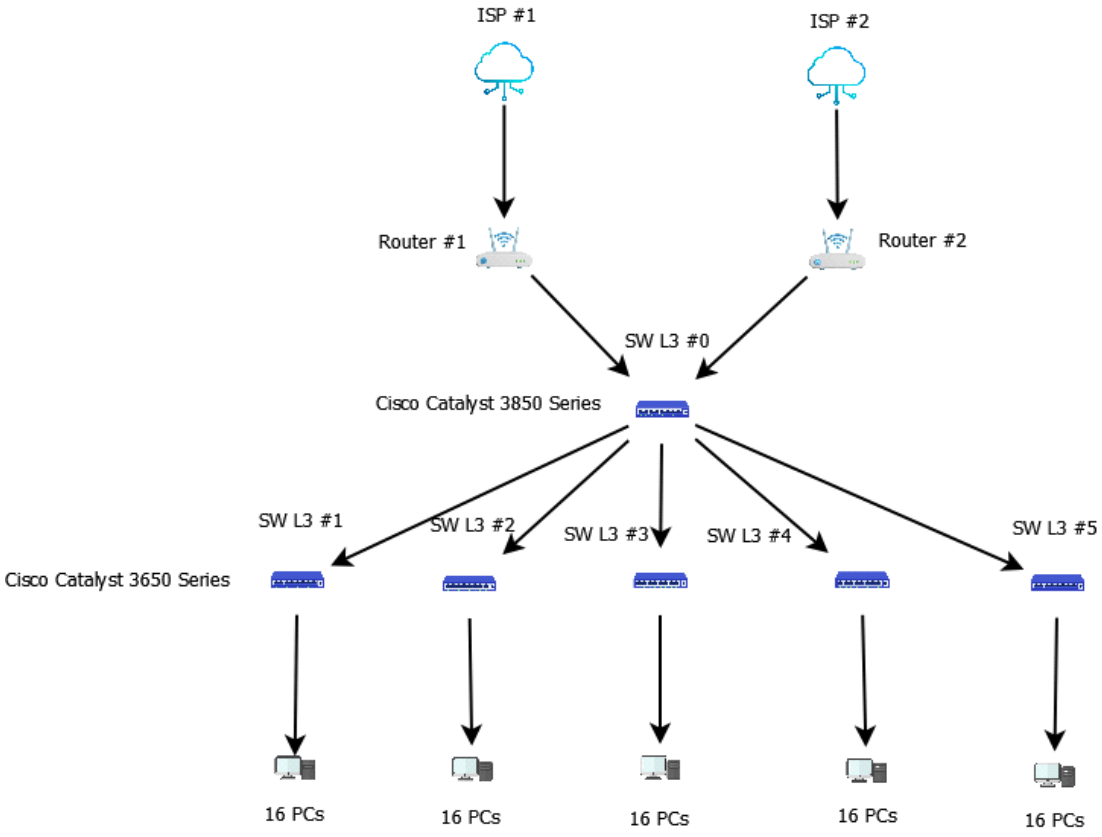
Curso: Experto Universitario en Seguridad de la Información

Alumno: Rodrigo Vila

Consigna:

Se debe presentar una topología que respete lo siguiente: Dos routers, cada uno conectado a un ISP (proveedor de servicio) distinto, y en nuestra red (LAN) hacia ellos a través de un switch de capa 3. Contra ese switch de capa 3 hay 5 switches más conectados, también de capa 3, de los cuales en cada SW, están tomados todos los puertos con PCs (16) (razonemos de cuantos puertos serán los switches y cuántos puertos necesitamos para poder conectarlos entre sí). No hay implementado ningún dispositivo de seguridad, ni ningún servicio, desarrollar la idea de poner y que agregar (sin límites), respetando únicamente la topología seleccionada, sumando a diagramar la topología de cómo lo armaron.

Primera etapa del desarrollo de la Topología, sin seguridad aplicada:



En este caso, cada uno de los cinco switches de capa 3 adicionales está conectado al Switch L3 principal. Cada uno de estos switches de capa 3 adicionales (Switch L3 #1, #2, #3, #4, y #5) está conectado a PCs. Dado que tenemos 16 PCs conectadas a cada uno de estos switches, necesitaremos al menos 17 puertos en cada uno de los switches adicionales para conectar las PCs y un puerto adicional para la interconexión con el Switch L3 principal.

Por lo tanto, cada uno de los cinco switches de capa 3 adicionales deberá tener al menos 18 puertos. Esto permitirá la conexión de las 16 PCs y la interconexión con el Switch L3 principal.

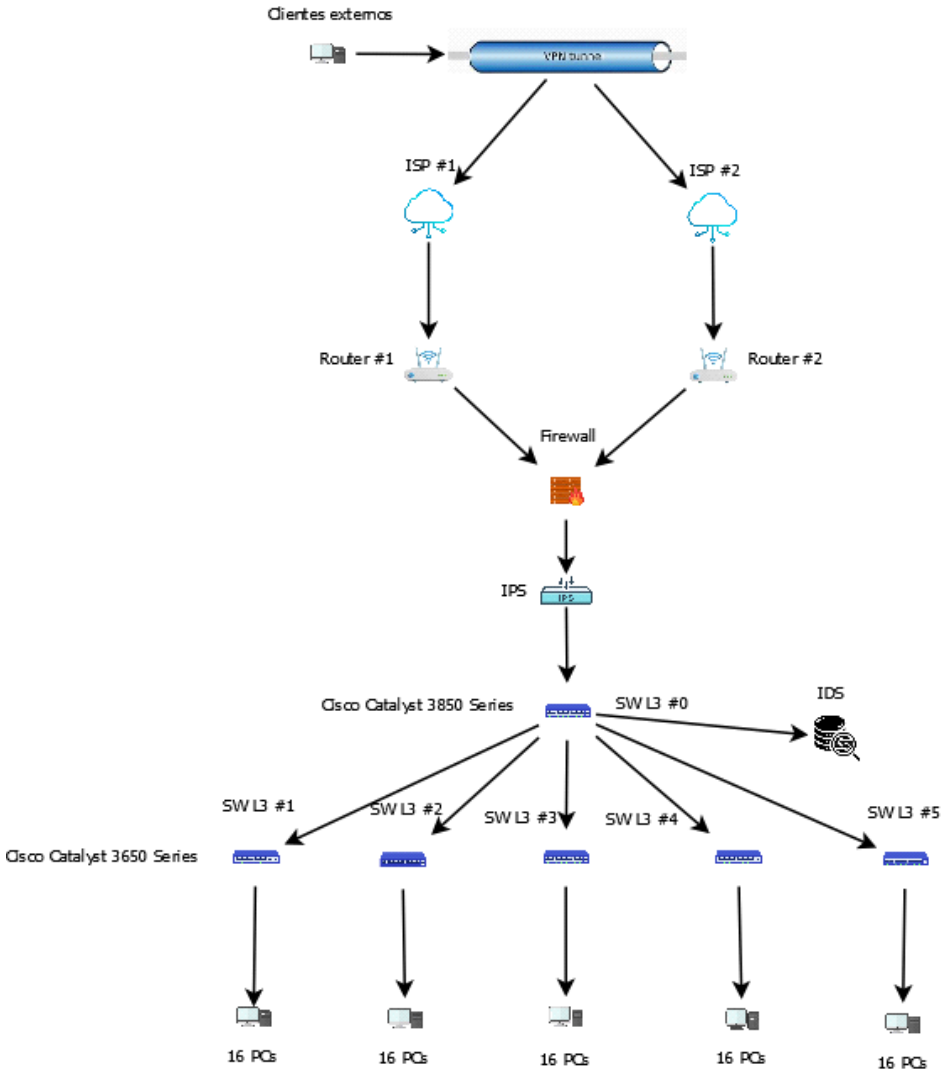
Para el SW L3 #0 elegí el modelo Cisco Catalyst 3850 Series: Esta serie de switches modulares ofrece modelos con diferentes configuraciones de puertos, incluidos modelos con hasta 48 puertos Gigabit Ethernet y opciones de puertos adicionales para enlaces ascendentes.

Para los SW del #1 al #5 elegí el modelo Cisco Catalyst 3650 Series: Este switch ofrece modelos con al menos 24 puertos Gigabit Ethernet y opciones de puertos adicionales para enlaces ascendentes.

Al contar con dos ISP y dos Routers antes del Switch, vamos a suponer que es una red con alto volumen de tráfico, y que todos los equipos conectados son críticos, ya que contamos con dos proveedores de Internet por si uno se interrumpe, vamos a priorizar la colocación de dispositivos de seguridad comprendiendo que todos los equipos conectados merecen un alto rendimiento de seguridad aplicada.

Por eso procedo a colocar un Firewall que filtre todas las conexiones entrantes, seguido de un IPS para mayor seguridad a costa de quizás un poco menos de rendimiento fluido en la red.

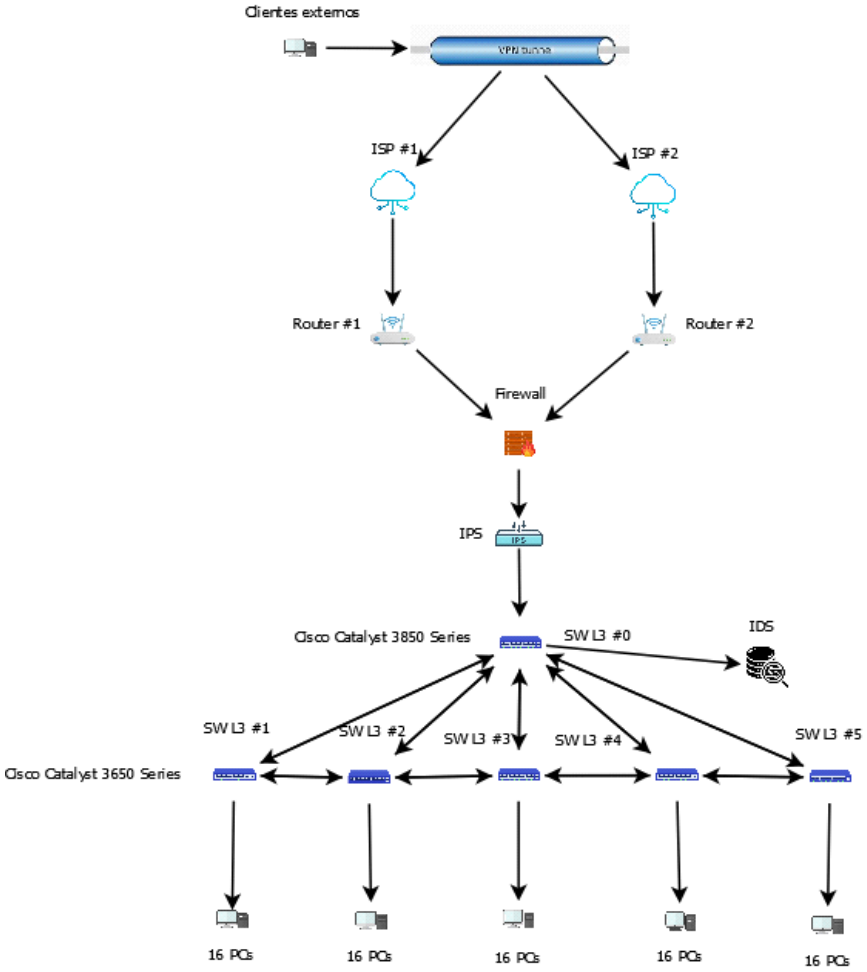
Segunda etapa del desarrollo de la Topología con seguridad aplicada:



- A la red se accede desde el exterior con inicio de sesión único (SSO) y conectando a una VPN mediante autentificación por hardware (Yubikey).
- El Firewall contiene reglas de ACLs para filtrar el tráfico de red y evitar accesos no autorizados.
- Cada host tiene un HIDS configurado que controla el acceso a los servicios requeridos.
- El administrador de red se ocupa de mantener el software y los sistemas operativos de cada host actualizados.
- Cada host posee software Antivirus y Antimalware.

- La compañía mantiene una política de contraseñas seguras, compuestas por Mayúsculas, minúsculas, números y símbolos.

Tercera etapa del desarrollo de la Topología:



En esta etapa se enlazaron los Switch entre sí para mejorar la redundancia y disponibilidad de la red en caso de que algún enlace se vea interrumpido.

Se configura en los Switches el protocolo de redundancia Spanning Tree Protocol (STP) para evitar bucles en la red.

Asignación de direcciones IP:

Subredes y rangos de direcciones IP:

- Subred 1: 192.168.1.0/24 (254 hosts)
  - Router 1: 192.168.1.1
  - Switch L3 #0: 192.168.1.2

    - PCs (16): 192.168.1.3 - 192.168.1.18
- Subred 2: 192.168.2.0/24 (254 hosts)
    - Router 2: 192.168.2.1
    - Switch L3 #1: 192.168.2.2
    - PCs (16): 192.168.2.3 - 192.168.2.18

- Subred 3: 192.168.3.0/24 (254 hosts)
    - Switch L3 #2: 192.168.3.1
    - PCs (16): 192.168.3.2 - 192.168.3.17

- Subred 4: 192.168.4.0/24 (254 hosts)
    - Switch L3 #3: 192.168.4.1
    - PCs (16): 192.168.4.2 - 192.168.4.17

- Subred 5: 192.168.5.0/24 (254 hosts)
    - Switch L3 #4: 192.168.5.1
    - PCs (16): 192.168.5.2 - 192.168.5.17

Explicación de las IPs asignadas:

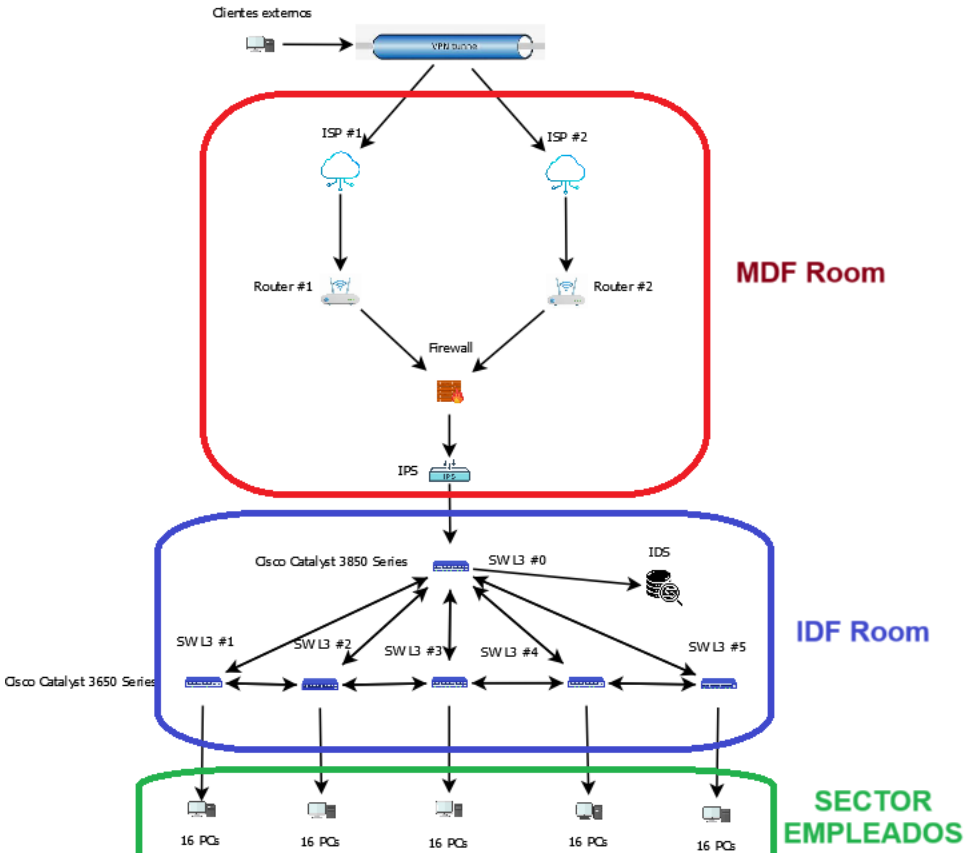
- Subredes: el diagrama muestra cinco subredes: 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, 192.168.4.0/24 y 192.168.5.0/24. Cada subred utiliza una máscara /24, lo que significa que tiene 254 direcciones de host utilizables (excluyendo la dirección de red y la dirección de transmisión).
- Routers: el router 1 tiene una dirección IP de 192.168.1.1, que se encuentra dentro de la subred 192.168.1.0/24. De manera similar, el router 2 tiene una dirección IP 192.168.2.1, que se encuentra dentro de la subred 192.168.2.0/24. Esto permite que los routers se comuniquen directamente con los dispositivos en sus respectivas subredes.
- Switches L3: El Switch L3 #0 tiene una dirección IP de 192.168.1.2, el Switch L3 #1 tiene una dirección IP de 192.168.2.2, el Switch L3 #2 tiene una dirección IP de 192.168.3.1, el Switch L3 #3 tiene una dirección IP de 192.168.4.1 y el Switch L3 #4 tiene una dirección IP de 192.168.5.1. Cada Switch L3 tiene una dirección

IP dentro de la subred de los dispositivos a los que se conecta. Esto permite que los switches L3 enruten el tráfico entre diferentes subredes.

- PC: A las PC se les asignan direcciones IP dentro de sus respectivas subredes. Por ejemplo, es probable que la PC03 esté conectada al Switch L3 #1 y tenga una dirección IP 192.168.2.5, que se encuentra dentro de la subred 192.168.2.0/24.

Seguridad física de la red:

Cuarta etapa del desarrollo de la Topología:



Como figura en la imagen, la red se encontraría distribuida en 3 sectores. Por un lado la conexión de los ISP, los 2 Routers principales, el Firewall principal y el IPS, se encontrarían dentro del MDF Room.

Los Switch, y el IDS se encontrarían dentro del IDF Room, también podrían ir aquí servidores importantes. Supongamos que las PCs conectadas al SW L3 #1 son servidores críticos. Colocaría un Firewall extra con ACLs configuradas entre el SW L3 #1 y los 16 Servidores. Los 4 Switches restantes quedarían como terminales de empleados en el sector de escritorios de la oficina.

Eso en un caso hipotético si hubiese colocado servidores en el IDF Room, pero no lo hice, asique en este caso estarían todas las PCs en los escritorios del Sector Empleados. Siendo esta oficina un punto “cliente” de la red de una corporación.

Tanto el MDF Room como el IDF Room contarían con un sistema de refrigeración dual con un equipo de backup por si uno falla. También con equipos UPS para garantizar el funcionamiento en caso de corte del suministro de energía eléctrica. Ambos sistemas controlados mediante un BMS (Building Management System).

A estos cuartos solo puede acceder personal autorizado, protegiendo el acceso con readers RFID o apertura remota desde un SOC (Security Operations Center).

Glosario y desarrollo de conceptos:

- **¿Qué es y cómo funciona el protocolo STP?:**

El Protocolo de Árbol de Expansión (STP, por sus siglas en inglés, Spanning Tree Protocol) es un protocolo de red utilizado para evitar bucles de red en topologías de red Ethernet. Los bucles pueden causar problemas como congestión de red, transmisión de paquetes infinita y otros problemas de rendimiento. El STP es una parte integral del estándar IEEE 802.1D y ha sido mejorado en varias versiones, como Rapid Spanning Tree Protocol (RSTP) y Multiple Spanning Tree Protocol (MSTP).

La forma en que funciona el STP es relativamente simple pero efectiva. Aquí un resumen de cómo opera:

1. **Descubrimiento de topología**: Los dispositivos que implementan STP intercambian mensajes de Protocolo de Configuración de Árbol (BPDU, por sus siglas en inglés, Bridge Protocol Data Units) entre sí para construir un mapa de la topología de la red. Estos mensajes contienen información sobre los enlaces de la red, como identificadores de puertos y costos de ruta.
2. **Selección del puente raíz**: Basándose en la información de las BPDUs, cada dispositivo en la red elige un "puente raíz" que actúa como punto central de la topología de la red. Este puente raíz es el punto de referencia para determinar las rutas más cortas hacia el resto de los dispositivos.
3. **Selección de caminos más cortos**: Una vez que se ha elegido el puente raíz, cada dispositivo determina el camino más corto hacia el puente raíz a través de los diferentes enlaces disponibles. Esto se hace calculando el costo de cada ruta, que generalmente se basa en la velocidad del enlace. Los enlaces con menor costo se consideran los caminos preferidos.
4. **Bloqueo de puertos**: Una vez que se han seleccionado los caminos más cortos, STP identifica y bloquea los enlaces redundantes que no son necesarios para alcanzar el puente raíz. Esto elimina los bucles de la red, ya que solo se utiliza un camino activo entre cualquier par de dispositivos.

5. **Reconvergencia**: Si ocurre algún cambio en la topología de la red, como la falla de un enlace o la adición de un nuevo dispositivo, STP vuelve a calcular los caminos más cortos y ajusta la topología de la red en consecuencia. Durante este proceso, puede haber un breve período de tiempo en el que la red esté en un estado de reconvergencia mientras se actualizan las tablas de reenvío.

En resumen, el STP es un protocolo fundamental para garantizar la estabilidad y la eficiencia en las redes Ethernet al prevenir los bucles y proporcionar caminos redundantes para la resiliencia de la red.

- **¿Qué es un MDF?:**

MDF es la abreviatura de "Main Distribution Frame" (Marco de Distribución Principal) en inglés. También es conocido como Main Distribution Point (MDP) o Main Cross-Connect (MCX). Un MDF es un elemento esencial en la infraestructura de telecomunicaciones de un edificio o instalación.

El MDF es un armario o gabinete (en este caso un cuarto entero), que alberga el equipo de conexión central para una red de telecomunicaciones o una red de área local (LAN). Es el punto central donde llegan y se distribuyen los cables de comunicación de largo alcance, como los cables de fibra óptica, los cables de cobre provenientes del proveedor de servicios de telecomunicaciones o los cables de interconexión interna de la red.

Las funciones principales de un MDF incluyen:

- Conexión de entrada: Los cables de comunicación externos (líneas de teléfono, líneas de fibra óptica, etc.) llegan al MDF y se conectan a los paneles de conexiones correspondientes.
- Distribución interna: Los cables conectados en el MDF se distribuyen hacia los puntos de conexión secundarios, como los IDF (Intermediate Distribution Frame) ubicados en diferentes áreas o pisos del edificio.
- Gestión de conexiones: Los técnicos pueden realizar cambios, agregar o quitar conexiones fácilmente en el MDF utilizando patch panels u otros dispositivos de gestión de conexiones.

En resumen, el MDF sirve como punto central de conexión para la infraestructura de telecomunicaciones de un edificio o instalación, facilitando la organización, distribución y gestión eficientes de las conexiones de red.

- **¿Qué es un IDF?:**

IDF significa "Intermediate Distribution Frame" (Marco de Distribución Intermedio) en inglés. Es un término comúnmente utilizado en el ámbito de las redes y las telecomunicaciones para referirse a un armario o gabinete que se encuentra entre el

MDF (Main Distribution Frame o Marco de Distribución Principal) y los dispositivos finales de red.

Los IDF se utilizan para distribuir conexiones de red desde el MDF a áreas específicas o locales dentro de un edificio o campus. Por lo general, los IDF se encuentran en lugares estratégicos dentro de un edificio para minimizar la longitud de los cables y facilitar la conexión de dispositivos finales, como computadoras, teléfonos IP, puntos de acceso Wi-Fi, cámaras de seguridad, entre otros.

Los IDF suelen contener patch panels, switches, routers y otros dispositivos de red necesarios para conectar los dispositivos finales a la infraestructura de red principal. Son puntos intermedios clave en la arquitectura de red que permiten una gestión eficiente de la conectividad y facilitan la escalabilidad y el mantenimiento de la red.

- **¿Qué es un BMS?:**

BMS es la abreviatura de "Building Management System" en inglés, que se traduce al español como "Sistema de Gestión de Edificios". También es conocido como Sistema de Automatización de Edificios (BAS, por sus siglas en inglés, Building Automation System) o Sistema de Control de Edificios (BCS, por sus siglas en inglés, Building Control System).

Un BMS es un sistema computarizado que controla y supervisa las operaciones y funciones de diversos sistemas dentro de un edificio o instalación. Estos sistemas pueden incluir HVAC (Calefacción, Ventilación y Aire Acondicionado), iluminación, sistemas eléctricos, sistemas de seguridad, sistemas contra incendios, control de acceso, sistemas de gestión de energía, entre otros.

Las funciones principales de un BMS incluyen:

- Control y automatización: El BMS controla y regula los diferentes sistemas del edificio automáticamente, ajustando la temperatura, la iluminación, la ventilación y otros parámetros según las necesidades del edificio y las preferencias de los ocupantes.
- Monitoreo y supervisión: El sistema monitorea constantemente el rendimiento y el estado de los sistemas del edificio, detectando y respondiendo a problemas como fallos del equipo, fugas de agua, intrusiones, incendios, entre otros.
- Optimización de la energía: El BMS ayuda a optimizar el uso de energía en el edificio, ajustando los sistemas de HVAC y la iluminación para maximizar la eficiencia energética y minimizar los costos operativos.
- Seguridad y gestión de emergencias: El sistema puede integrar funciones de seguridad, como la detección de intrusos, el control de acceso y la detección de incendios, para garantizar la seguridad de los ocupantes del edificio y coordinar respuestas rápidas en caso de emergencia.

En resumen, un BMS es una herramienta fundamental para la gestión eficiente de edificios comerciales, industriales y residenciales, permitiendo un control centralizado, monitoreo en tiempo real y automatización de una amplia gama de sistemas y funciones para mejorar la comodidad, la seguridad y la eficiencia operativa del edificio.

- **¿Qué es un SOC?**

SOC es la abreviatura de "Security Operations Center", que se traduce al español como "Centro de Operaciones de Seguridad". Un SOC es una instalación física o virtual donde se lleva a cabo la supervisión, detección, análisis y respuesta a amenazas de seguridad cibernética en una organización.

Las funciones principales de un SOC incluyen:

- Monitoreo de seguridad: El SOC monitorea de manera continua la red, los sistemas y las aplicaciones de una organización en busca de actividades sospechosas o maliciosas que puedan indicar una violación de seguridad.
- Detección de amenazas: Utilizando herramientas de seguridad como sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de gestión de eventos e información de seguridad (SIEM) y análisis de comportamiento, el SOC identifica y analiza posibles amenazas de seguridad.
- Análisis e investigación: Una vez que se detecta una amenaza, los analistas de seguridad del SOC investigan y analizan la naturaleza y el alcance de la amenaza para comprender mejor el riesgo y determinar la mejor respuesta.
- Respuesta a incidentes: Basándose en el análisis de amenazas, el SOC coordina y ejecuta acciones para mitigar los incidentes de seguridad, como la cuarentena de sistemas afectados, la remediación de vulnerabilidades y la implementación de medidas de seguridad adicionales.
- Mejora continua: El SOC también es responsable de la mejora continua de las capacidades de seguridad de la organización, mediante la revisión de incidentes pasados, la evaluación de la efectividad de las medidas de seguridad y la implementación de cambios y actualizaciones necesarias.

En resumen, un SOC desempeña un papel crucial en la protección de una organización contra las amenazas de seguridad cibernética al proporcionar una capacidad centralizada para monitorear, detectar, analizar y responder a incidentes de seguridad de manera oportuna y efectiva.

- **¿Que son los lectores RFID?**

Los lectores RFID (Radio-Frequency Identification, Identificación por Radiofrecuencia) son dispositivos electrónicos diseñados para leer y comunicarse con etiquetas RFID.

Estas etiquetas, también conocidas como transpondedores o tags, contienen chips de memoria y antenas que les permiten almacenar y transmitir datos a través de señales de radiofrecuencia.

Los lectores RFID funcionan emitiendo señales de radiofrecuencia que energizan las etiquetas RFID cercanas. Cuando una etiqueta RFID recibe la energía de la señal del lector, responde transmitiendo sus datos almacenados de vuelta al lector. El lector recoge estos datos y los procesa según las necesidades de la aplicación específica.

Existen diferentes tipos de lectores RFID, que se pueden clasificar según su alcance de lectura, su capacidad de comunicación y su capacidad para leer etiquetas activas o pasivas. Algunas características comunes de los lectores RFID incluyen:

- Alcance de lectura: Varía desde lectores de corto alcance, que solo pueden leer etiquetas a distancias cortas (generalmente hasta varios centímetros o metros), hasta lectores de largo alcance, que pueden leer etiquetas a distancias más grandes (varios metros o incluso varios kilómetros, en algunos casos).
- Frecuencia de operación: Los lectores RFID pueden operar en diferentes rangos de frecuencia, como baja frecuencia (LF), alta frecuencia (HF), ultra alta frecuencia (UHF) y frecuencia muy alta (VHF), cada uno con sus propias características y aplicaciones específicas.
- Capacidad de lectura: Algunos lectores RFID pueden leer múltiples etiquetas simultáneamente, mientras que otros están diseñados para leer una sola etiqueta a la vez.
- Interfaz de comunicación: Los lectores RFID pueden tener diferentes interfaces de comunicación, como USB, Ethernet, Wi-Fi o Bluetooth, que les permiten integrarse con sistemas de gestión de datos o redes de comunicación existentes.

Los lectores RFID se utilizan en una amplia variedad de aplicaciones, que incluyen control de acceso, seguimiento de inventario, gestión de activos, identificación de productos, pagos sin contacto, seguimiento de vehículos, gestión de documentos, entre otros. Su capacidad para proporcionar identificación rápida y sin contacto los hace muy útiles en entornos donde se requiere automatización, eficiencia y seguridad.

- **¿Qué significa SSO?:**

SSO significa "Single Sign-On", que se traduce al español como "Inicio de Sesión Único". Es un método de autenticación que permite a un usuario acceder a múltiples sistemas o aplicaciones utilizando un único conjunto de credenciales de inicio de sesión, como un nombre de usuario y una contraseña, en lugar de tener que ingresar credenciales separadas para cada sistema o aplicación.

El objetivo principal del SSO es mejorar la experiencia del usuario al simplificar el proceso de inicio de sesión y reducir la carga de recordar múltiples conjuntos de credenciales. Además de la comodidad para los usuarios, el SSO también puede

mejorar la seguridad y la gestión de identidades en una organización al permitir una autenticación centralizada y un mejor control de acceso.

Cómo funciona el SSO:

- Autenticación inicial: Cuando un usuario intenta acceder a un sistema o aplicación protegida por SSO, se le solicita que inicie sesión proporcionando sus credenciales de inicio de sesión únicos.
- Generación de token de sesión: Una vez que el usuario ha sido autenticado con éxito, el servidor de autenticación genera un token de sesión que contiene la información de autenticación del usuario.
- Acceso a otras aplicaciones: Cuando el usuario intenta acceder a otra aplicación o sistema dentro del mismo entorno de SSO, el token de sesión previamente generado se utiliza para autenticar al usuario sin necesidad de ingresar credenciales adicionales.
- Renovación y cierre de sesión: El token de sesión puede tener una duración limitada. Cuando expira, el usuario puede ser redirigido nuevamente al proceso de autenticación inicial para obtener un nuevo token. Además, el usuario puede cerrar sesión en todas las aplicaciones o sistemas protegidos por SSO con un solo clic.

El SSO se utiliza ampliamente en entornos corporativos, educativos y en línea para mejorar la productividad de los usuarios, reducir la carga administrativa de las contraseñas y mejorar la seguridad mediante una autenticación centralizada y controlada.

- **¿Qué es una VPN?:**

Una VPN, o Red Privada Virtual en español, es una tecnología que permite establecer una conexión segura y encriptada entre dos puntos a través de una red pública, como Internet. Esta conexión segura permite que los datos sean transmitidos de manera privada y segura a través de la red pública.

Las VPNs se utilizan principalmente por dos razones principales:

- Seguridad y Privacidad: Al utilizar una VPN, todos los datos que se transmiten entre el dispositivo del usuario y el servidor remoto están encriptados. Esto significa que incluso si los datos son interceptados, no pueden ser leídos por terceros. Esto es especialmente útil cuando se utiliza una red Wi-Fi pública o no segura, ya que protege la información confidencial del usuario, como contraseñas, correos electrónicos y datos bancarios.
- Acceso Remoto: Las VPNs también se utilizan para permitir a los usuarios acceder de forma segura a recursos internos de una red privada desde ubicaciones remotas. Por ejemplo, un empleado que trabaja desde casa puede

conectarse a la VPN de su empresa para acceder a archivos y aplicaciones internas como si estuviera físicamente en la oficina.

Además de estas razones principales, las VPNs también pueden utilizarse para eludir la censura en línea y para acceder a contenido georrestringido al simular la ubicación del usuario en una región diferente.

En términos de funcionamiento, una VPN utiliza protocolos de tunelización y encriptación para crear un "túnel" seguro a través de la red pública. Los datos son encapsulados en paquetes seguros antes de ser transmitidos a través del túnel, lo que garantiza su privacidad y seguridad.

Existen varias formas de implementar una VPN, incluyendo VPNs basadas en software que pueden ser instaladas en dispositivos individuales, así como VPNs empresariales que pueden ser implementadas en la infraestructura de red de una organización. Además, hay servicios VPN comerciales que ofrecen acceso a servidores VPN en todo el mundo a través de suscripciones pagas.

- **¿Qué es una Yubikey?:**

Una YubiKey es un dispositivo de seguridad física que se utiliza para autenticación de dos factores (2FA) y para mejorar la seguridad de cuentas en línea. Fabricada por la empresa Yubico, la YubiKey es una llave de hardware pequeña y portátil que se conecta a un puerto USB o utiliza tecnología inalámbrica como NFC (Near Field Communication) para comunicarse con dispositivos compatibles.

La YubiKey funciona generando códigos únicos o criptográficos que se utilizan como una segunda capa de seguridad además de las contraseñas tradicionales. Algunos de los métodos de autenticación que ofrece una YubiKey incluyen:

- OTP (One-Time Password): La YubiKey puede generar códigos OTP de un solo uso cuando se presiona su botón. Estos códigos son utilizados en conjunto con una contraseña para autenticar al usuario en servicios en línea.
- U2F (Universal 2nd Factor): La YubiKey es compatible con el estándar U2F, que permite la autenticación de dos factores con un solo toque en el dispositivo. Esto proporciona una capa adicional de seguridad para cuentas en línea al requerir la presencia física de la YubiKey para autenticar al usuario.
- FIDO2: La YubiKey también es compatible con FIDO2, un estándar de autenticación de próxima generación que permite la autenticación sin contraseñas. Con FIDO2, los usuarios pueden autenticarse utilizando la YubiKey sin necesidad de ingresar una contraseña.

La YubiKey es especialmente útil para proteger cuentas sensibles en línea, como cuentas de correo electrónico, redes sociales, servicios financieros y servicios en la nube. Al agregar una capa adicional de autenticación basada en hardware, la YubiKey

ayuda a prevenir el acceso no autorizado a las cuentas incluso si las contraseñas son comprometidas.

En resumen, una YubiKey es un dispositivo de seguridad física versátil y altamente confiable que proporciona autenticación de dos factores y mejora la seguridad en línea al proteger las cuentas contra el acceso no autorizado.

Software utilizado para diagramar la red y generar las imágenes:

Dia (software): https://es.wikipedia.org/wiki/Dia_(programa)

Bibliografía:

Durante el proceso de investigación para este trabajo práctico, utilicé una variedad de recursos, incluyendo tecnologías de inteligencia artificial como ChatGPT y Gemini.

- **ChatGPT**: Utilicé el modelo de lenguaje de inteligencia artificial ChatGPT, desarrollado por OpenAI, para explorar y generar ideas sobre el tema de mi investigación. ChatGPT proporcionó sugerencias y perspectivas útiles que enriquecieron mi comprensión del tema y me ayudaron a formular preguntas y enfoques relevantes.
- **Gemini**: Además, utilicé la plataforma Gemini para explorar y acceder a recursos académicos, artículos de investigación y otros documentos relacionados con mi tema de estudio. Gemini me proporcionó acceso a una amplia gama de fuentes confiables y actualizadas que contribuyeron significativamente a mi investigación.

Al utilizar ChatGPT y Gemini, pude obtener una variedad de perspectivas y recursos que enriquecieron mi investigación y me permitieron abordar de manera efectiva los objetivos de mi trabajo práctico.

Estas plataformas fueron utilizadas de forma ética para ayudarme en la comprensión de conceptos y el desarrollo de este trabajo.

La base fundamental de este trabajo es el conocimiento que estoy obteniendo a través del estudio en esta cursada, mi experiencia trabajando en redes de oficinas y como seguridad física y electrónica para dos grandes empresas del sector tecnológico.

Rodrigo Vila.-