MINISTERIO DEL PODER POPULAR PARA LA EDUCACIÓN UNIVERSITARIA

UNIVERSIDAD RAFAEL URDANETA

FACULTAD DE INGENIERÍA

CÁTEDRA: SEGURIDAD INFORMÁTICA

PERIODO: 2024-C

PROFESOR: JUBERT PEREZ

PROYECTO 1

SEGURIDAD INFORMÁTICA

Integrantes

Vargas, Wanfredo - C.I. 29.977.093

Jaraba, Luis - C.I. 30.200.228

Crespo, Luis - C.I. 30.167.842

INDICE

Contenido

INTRODUCCION

Este proyecto aborda el diseño e implementación de la infraestructura de red y seguridad informática para un edificio de 20 pisos, con distintas áreas funcionales, desde atención al cliente hasta administración, desarrollo, mercadeo y gerencia. La principal meta es asegurar una red segura, robusta y eficiente, que permita manejar una amplia gama de aplicaciones y servicios para más de 10 millones de clientes simultáneamente, con la flexibilidad y capacidad necesarias para soportar las operaciones diarias de la organización.

El documento parte de una estructura sólida basada en la distribución de usuarios y equipos por cada piso, abarcando la instalación de un centro de datos que funcione como el núcleo tecnológico del edificio. En este centro se centralizan servidores robustos, con capacidad para manejar grandes cantidades de información y tráfico de usuarios, asegurando disponibilidad constante y protección avanzada mediante técnicas de redundancia, enfriamiento y respaldo de energía. Además, el diseño incluye el almacenamiento de 20 TB anuales para aplicaciones web orientadas al cliente, lo que implica una infraestructura preparada para soportar altos volúmenes de tráfico y almacenamiento seguro.

Una característica clave del proyecto es la diferenciación de roles y accesos entre los distintos departamentos. Los desarrolladores tienen acceso exclusivo a los servidores de desarrollo, el equipo de control de cambios gestiona tanto servidores de desarrollo como de producción y QA, mientras que áreas como recursos humanos, administración y mercadeo solo acceden a las aplicaciones internas específicas de sus funciones. La gerencia, por su parte, maneja aplicaciones estratégicas como finanzas, ventas e indicadores de gestión, garantizando un acceso controlado y seguro.

La seguridad es un componente esencial, tanto lógica como física. A nivel lógico, el uso de firewalls avanzados, encriptación de datos y sistemas de autenticación basados en Active Directory aseguran que la información confidencial esté protegida. Cada departamento tiene su propio dominio y políticas de seguridad específicas, permitiendo una gestión controlada y centralizada. A nivel físico, se incorporan cámaras de vigilancia, control de acceso biométrico y sistemas de detección y extinción de incendios, creando un entorno seguro para los equipos críticos.

También para la topología de la red implementada, se utilizó una arquitectura de red en estrella que facilita la interconexión eficiente entre todos los pisos del edificio.

Cada departamento se configura como una subred individual, asegurando así una comunicación controlada y fluida. La zona desmilitarizada (DMZ) y la zona militarizada (MZ) proporcionan capas adicionales de seguridad para servidores de aplicaciones y bases de datos, evitando accesos no autorizados.

Finalmente, el cálculo detallado del ancho de banda requerido para soportar hasta 10 millones de usuarios simultáneos, asegurando que la infraestructura esté preparada para manejar la carga de trabajo esperada, mientras que la estructura de costos ofrece un análisis exhaustivo de los recursos necesarios, incluyendo hardware, consumo energético y consideraciones adicionales como licencias de software y mantenimiento.

REQUERIMIENTOS

El edificio de 20 pisos cuenta con una planta específica que divide las áreas de trabajo según los roles y funciones de cada departamento. A continuación, se describen los detalles de los dispositivos y usuarios asignados a cada piso, así como los requisitos para implementar un sistema de red robusto, seguro y eficiente que pueda manejar el tráfico y las operaciones de los distintos departamentos.

PISO	ASIGNADO A	USUARIOS	EQUIPOS
PB	Atencion al cliente	20	20 PC
1-5	Desarrolladores	60	60 PC
6-9	Salas de concepto	4	- 4 PC - Servidores, switches, router…
10-15	- RRHH - Administracion	10	10 PC
15-18	Mercadeo	10	10 PC
19-20	Gerencia	6	6 PC y laptops

Para satisfacer las necesidades operativas del edificio, se deben cumplir los siguientes requerimientos técnicos y de seguridad:

1. Centro de datos: Es imprescindible instalar un centro de datos en el edificio, que constituirá el corazón de la infraestructura tecnológica. Este centro de datos debe estar equipado con servidores robustos que puedan manejar eficientemente el procesamiento de datos y garantizar el funcionamiento ininterrumpido de aplicaciones y servicios. Además, debe contar con sistemas de respaldo, redundancia y enfriamiento, así como protección contra fallas de energía (UPS).

Ubicación: Entre los pisos 6-9 donde se pueden centralizar servidores y equipos de red y protegerlos mediante seguridad física y lógica. Requisitos de almacenamiento: los servidores deben tener capacidad suficiente para almacenar 20 TB de datos por año generados por las aplicaciones web orientadas al cliente.

2. Aplicaciones web para clientes: El edificio alberga aplicaciones web desarrolladas para más de 10 millones de clientes. Debido a que estas aplicaciones procesan grandes cantidades de datos y son de misión crítica, deben garantizar disponibilidad las 24 horas del día, los 7 días de la semana y protección contra ataques cibernéticos. Requisitos de almacenamiento: 20 TB de almacenamiento por año. Requisitos de tráfico: la infraestructura debe diseñarse para soportar un alto tráfico de usuarios simultáneos, lo que requiere una conexión a Internet sólida y servidores potentes.
3. Acceso controlado a los servidores: El acceso a los servidores está restringido según el rol del usuario, Desarrolladores: Tiene acceso exclusivo a los servidores de desarrollo, lo que te permite realizar pruebas, actualizaciones y desarrollar nuevas funciones sin interferencias. Control de cambios: los equipos de control de cambios son los únicos que tienen acceso a los servidores de desarrollo, producción y control de calidad. Esto garantiza que cualquier cambio en el sistema se controle e implemente de forma estructurada y segura. RRHH y administración: Sólo tienen acceso a aplicaciones internas que estén relacionadas con sus tareas, como, por ejemplo: análisis de nómina, recursos humanos, administración y marketing. Esto garantiza que el acceso a los datos se limite a sus funciones y responsabilidades, garantizando la privacidad de los datos y la confidencialidad de la información.
4. El área de gestión tiene acceso exclusivo a aplicaciones críticas para la toma de decisiones estratégicas
5. Contrato con Microsoft: Dado que tiene un contrato con Microsoft, es recomendado utilizar las herramientas y servicios de la suite Microsoft Azure, Active Directory, Windows Defender, entre otras herramientas que permiten la integración con soluciones de nube híbrida y servicios avanzados de almacenamiento y procesamiento. Esto también proporciona una gestión de licencias simplificada para software como Windows Server y SQL Server.
6. DMZ (Zona Desmilitarizada) y MZ (Zona Militarizada): Es imperativo configurar adecuadamente las zonas de seguridad DMZ y MZ para segmentar la red y aislar

los servicios externos de los sistemas internos más críticos. La DMZ se utiliza para alojar servicios públicos para aplicaciones web que interactúan con clientes, como servidores de aplicaciones y firewalls de primer nivel. Zona desmilitarizada (DMZ): aloja servidores que están expuestos al tráfico de Internet, como: Servidores web y de correo electrónico, con un firewall que controle las conexiones externas. Zona Militarizada (MZ): Contiene los servidores más sensibles, como los utilizados para la base de datos y la gestión de aplicaciones internas críticas, y protege estos sistemas de ataques directos.

7. Seguridad lógica: La seguridad lógica se implementa mediante el uso de firewalls avanzados, sistemas de autenticación sólidos como Active Directory para administrar el acceso de los usuarios a través de credenciales seguras y cifrado de datos para garantizar que la información confidencial esté siempre protegida. Control de acceso: se implementa una política de acceso basada en roles (RBAC) para garantizar que los usuarios solo tengan acceso a los recursos que necesitan para desempeñar su función. Auditoría y monitoreo: Todo acceso a los sistemas debe ser monitoreado y registrado para garantizar la trazabilidad de los eventos de seguridad.
8. Seguridad física. Además de la seguridad lógica, se debe garantizar la seguridad física del centro de datos y áreas críticas mediante el uso de cámaras de vigilancia que permitirán monitorear todas las áreas importantes del edificio, control de acceso biométrico para el sistema se aplicará en áreas que requieran un estricto control de acceso físico, como centros de cómputo, oficinas de dirección y administración, ademas de un sistema de detección y extinción de incendios: Se instalarán detectores de humo en todo el edificio, junto con un sistema de extinción de gas inerte para evitar daños a los equipos.

Con estos requisitos, se garantiza que la infraestructura del edificio cumplirá con los más altos estándares de seguridad, rendimiento y disponibilidad, ofreciendo una solución escalable y confiable para las necesidades de 10 millones de clientes y múltiples departamentos que operan dentro del edificio.

ESQUEMA DE LA RED

El edificio de veinte pisos fue completamente modelado utilizando Cisco Packet Tracer. Se organizó cada departamento que ocupa múltiples niveles, permitiendo una configuración clara y eficiente.

El centro de cómputo incluye un enrutador central que gestiona la conexión entre todos los pisos. Cada departamento está configurado como una subred individual, y para garantizar la interconexión entre estas subredes, se asignó un enrutador específico para cada área. Esto asegura una comunicación fluida y controlada dentro de cada sección del edificio y optimiza la seguridad de la red.

Para las aplicaciones web, los servidores de producción están conectados mediante un switch que enlaza directamente con el enrutador del proveedor de servicios de Internet (ISP). Estos servidores, junto con la interfaz pública, están ubicados en una zona desmilitarizada (DMZ), lo cual proporciona una barrera de seguridad adicional contra posibles accesos no autorizados, protegiendo las aplicaciones críticas.

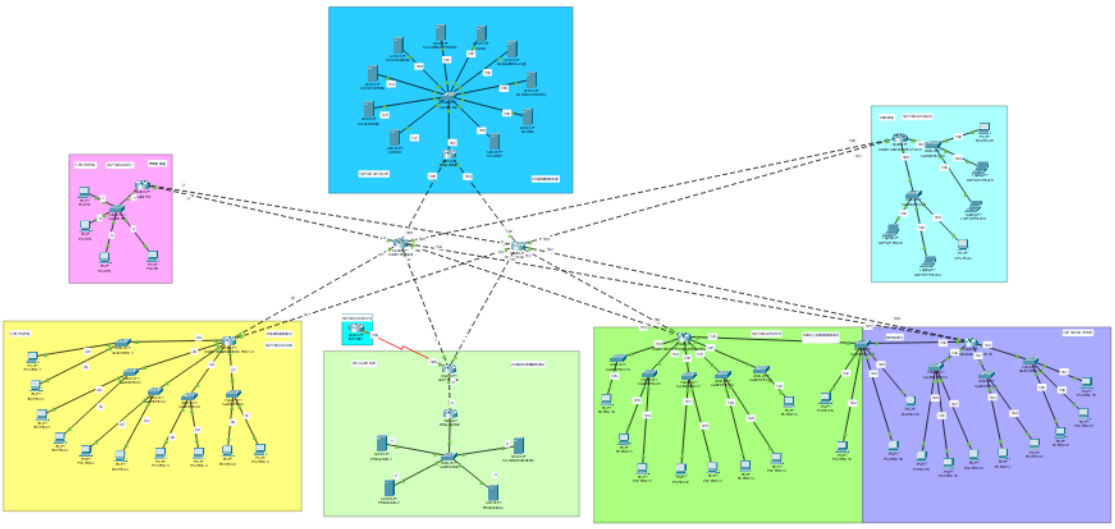
El acceso a los servidores está controlado según el rol de cada equipo: los desarrolladores tienen permisos exclusivos para los servidores de desarrollo, mientras que el equipo de control de cambios tiene acceso tanto a los servidores de desarrollo como a los de producción y QA. Las aplicaciones de Recursos Humanos, Administración y Mercadeo están restringidas exclusivamente al personal autorizado de estas áreas. Por su parte, la gerencia tiene acceso únicamente a las aplicaciones de finanzas, ventas e indicadores de gestión.

La seguridad de la red se gestiona con Windows Server, aprovechando el contrato existente con Microsoft, lo cual garantiza un control riguroso sobre los usuarios y las políticas de acceso. Este enfoque permite que cada departamento acceda solo a los recursos y aplicaciones necesarias para sus funciones, manteniendo la integridad y seguridad de la infraestructura de red.

Topología de la Red

En el edificio de 20 pisos, se ha implementado una topología de red tipo estrella en cada uno de los pisos, así como también en el enrutador central. Este enfoque facilita la interconexión de los dispositivos y la gestión eficiente del tráfico de red. Para cada subred,

se utiliza un router que se conecta a un switch principal, encargado de distribuir la conexión a los equipos dentro de esa subred.



Topologia

El switch seleccionado para este proyecto es el Cisco 2960-24TT, que ha sido elegido por su capacidad de manejar 24 conexiones y, además, por contar con dos puertos adicionales dedicados a la conexión con otros switches o al router.

Esta característica permite una mayor flexibilidad y escalabilidad, ya que se pueden agregar switches adicionales sin consumir las conexiones estándar destinadas a los dispositivos finales. Esto es especialmente útil en áreas donde se requiere conectar más de 24 dispositivos, como el área de Desarrolladores y Control de Cambios, evitando la necesidad de ocupar múltiples interfaces del router.

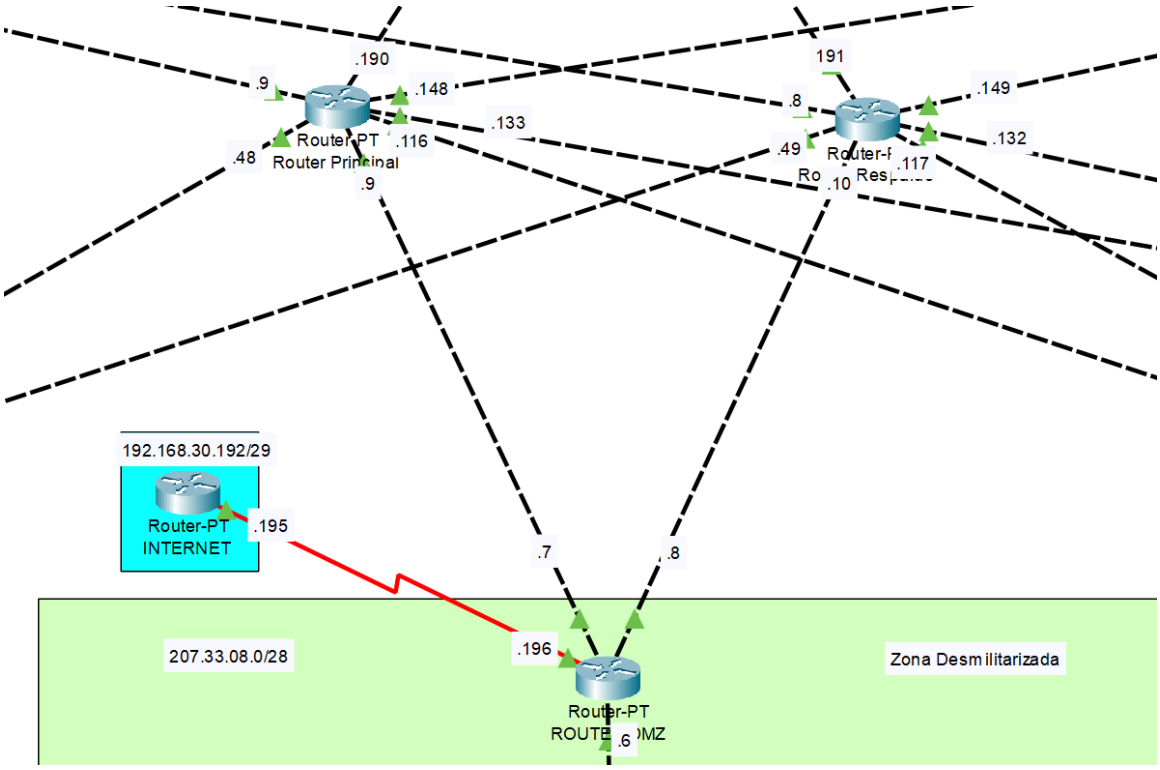
Esta elección de hardware y topología permite que, en subredes con alta densidad de dispositivos, se puedan implementar varios switches en cascada, garantizando una expansión de red fluida y sin comprometer la disponibilidad de puertos del router. De esta manera, se asegura una configuración que favorece la escalabilidad y la posibilidad de futuros cambios en la infraestructura de red.

El enrutador central también adopta una topología en estrella para conectar los distintos enrutadores de cada subred y el switch que maneja los servidores de producción. Esta disposición centralizada facilita la administración y el control de la red, asegurando

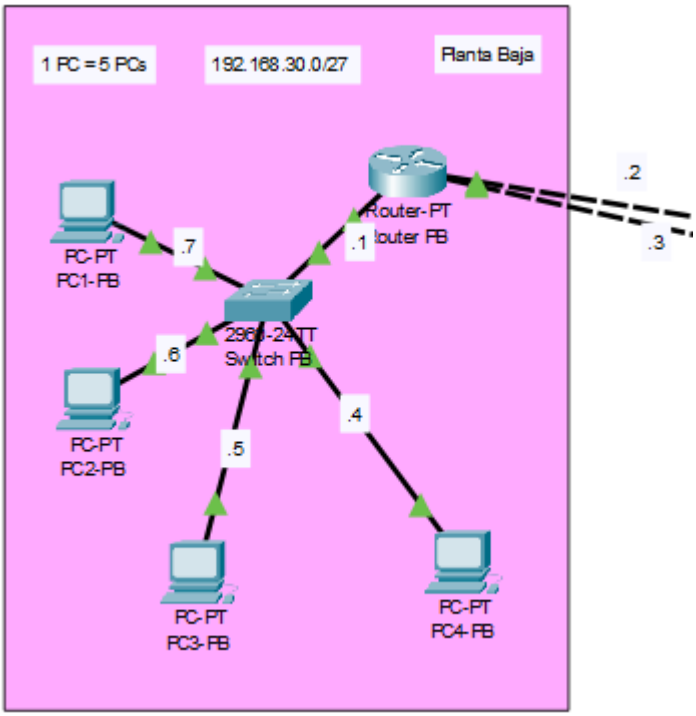
que cada departamento pueda comunicarse eficientemente a través de una infraestructura robusta.

Sin embargo, en caso de que el enrutador central falle, se ha implementado un plan de contingencia con un enrutador de respaldo que está conectado a los demás enrutadores de la red. Este enrutador alternativo se activará automáticamente si el enrutador principal sufre una avería, manteniendo así la conectividad y el acceso a los servidores críticos. Esta configuración proporciona un alto nivel de redundancia, minimizando el tiempo de inactividad y asegurando que las operaciones de la red no se vean interrumpidas.

Esta estrategia de diseño permite que la red mantenga su estabilidad incluso ante fallos en el hardware central, lo cual es esencial para la continuidad operativa en un entorno que maneja aplicaciones críticas y un gran volumen de usuarios.

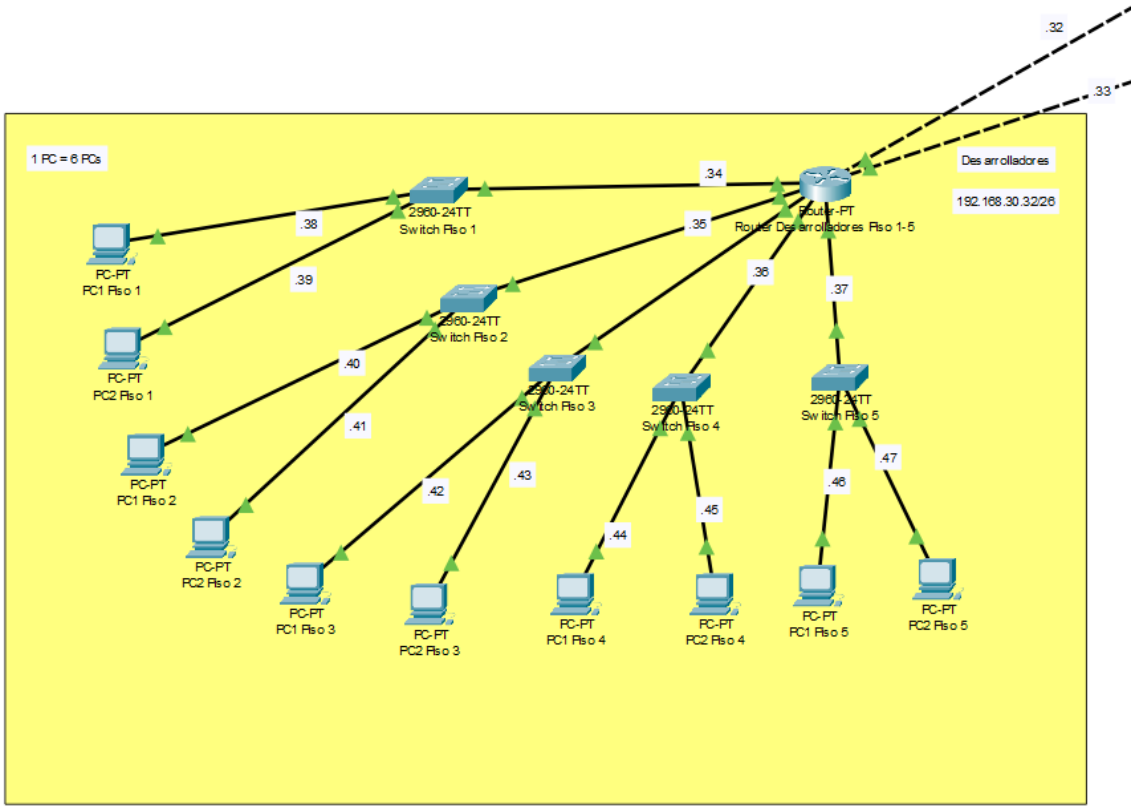


Routers Principales



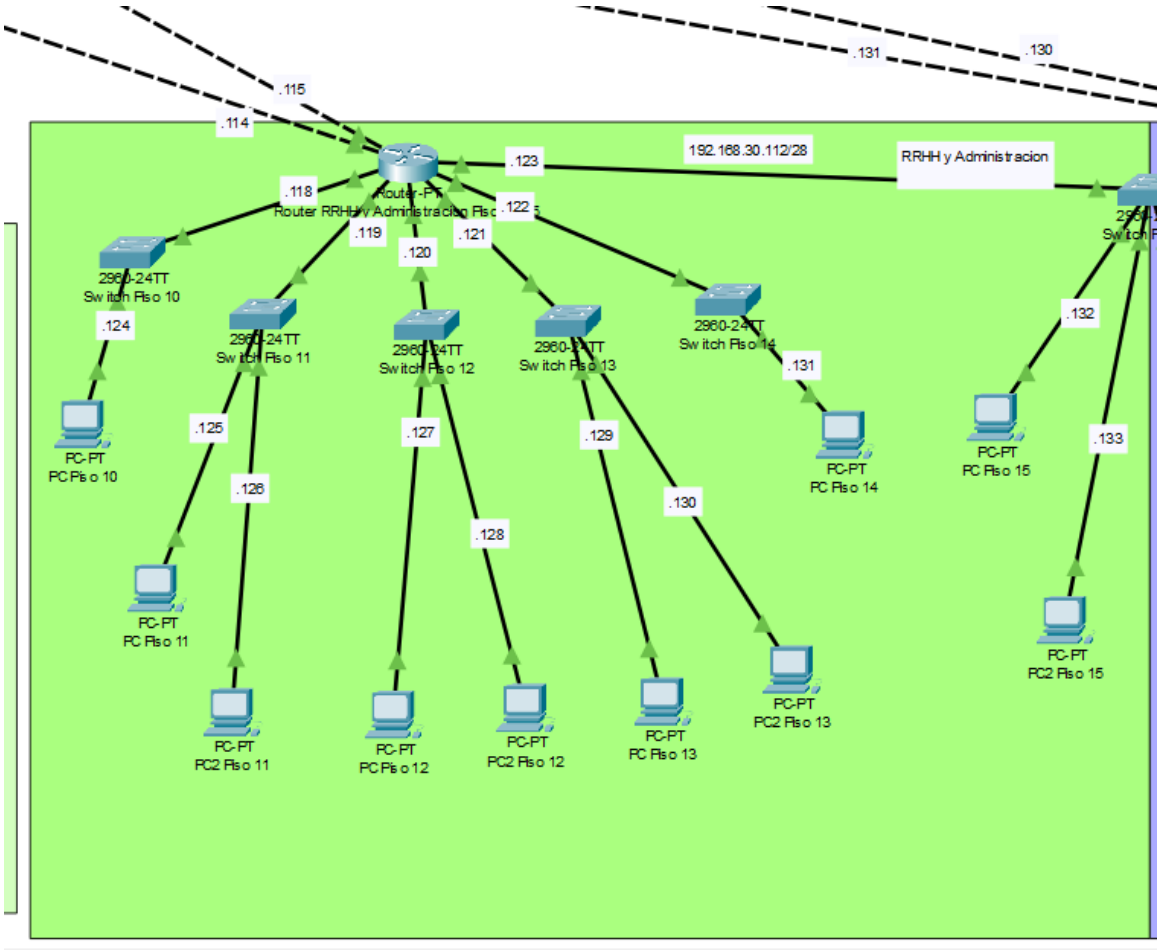
Planta Baja

(20 PC, 1 PC equivale a 5 PCs)



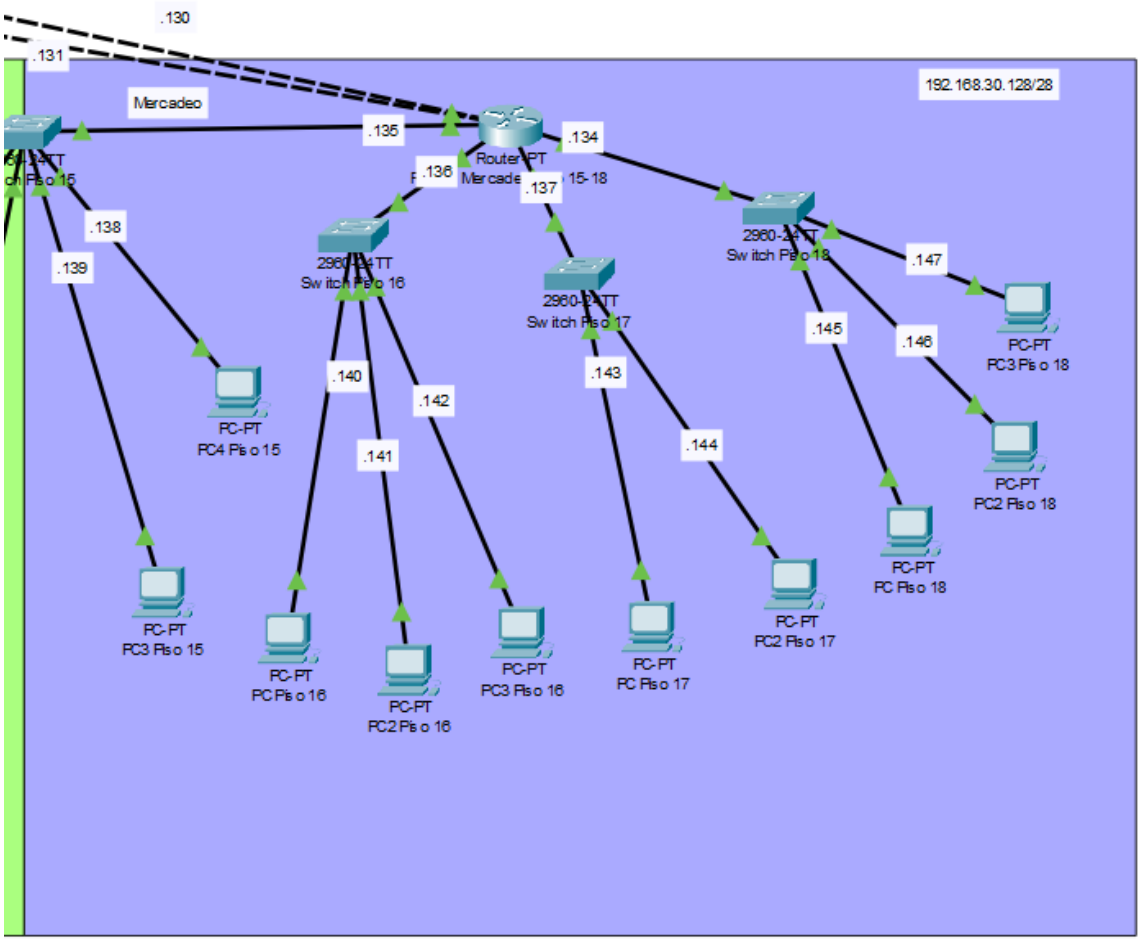
Pisos 1-5

(60 PC, 1 PC equivale a 6 PCs)



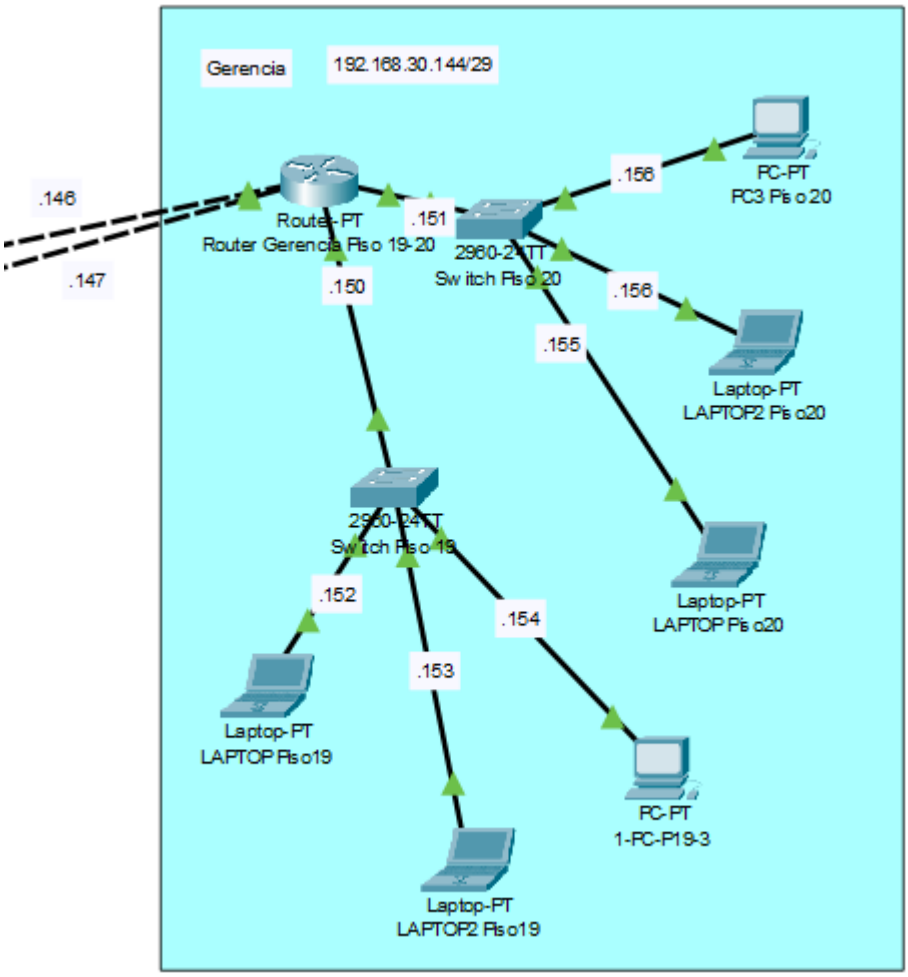
Pisos 10-15 RRHH y Administracion

(10 PC)



Pisos 15-18 Mercadeo

(10 PC)



Pisos 19-20 Gerencia

(6 PC)

Direccionamiento y subredes

Se utilizaron subredes generadas mediante VLSM (Variable Length Subnet Masking), permitiendo crear subredes de diferentes tamaños según las necesidades específicas de cada departamento y área del edificio. Para la red interna, se usó la dirección IP 192.168.30.0/24, que proporciona un rango amplio y flexible, ideal para acomodar un total de 30, 62, 14, 6, y 14 hosts en las diferentes subredes requeridas para cada departamento, desde Atención al Cliente hasta Gerencia. Se optó por una dirección de Clase C porque la cantidad total de hosts necesarios es considerable, pero también se necesitan múltiples subredes para segmentar correctamente el tráfico y garantizar la seguridad de la red.

Es importante destacar que los servidores de producción se encuentran en una subred separada con direccionamiento público, específicamente usando la red 207.33.08.0/28. Esto se realiza para asegurar que los servidores estén accesibles desde el exterior de manera controlada, mientras que los otros servidores se ubican en la subred 192.168.30.176/28, manteniéndolos dentro de la red interna pero separados del tráfico regular de los usuarios. Además, los routers que gestionan las conexiones de Internet utilizan la subred 192.168.30.192/29, asegurando una gestión eficaz de las conexiones externas.

Nombre	Subred	Mascara de Subred	IP de Gateway/ Router	Rango de IPs	Broadcast	IPs
Atencion al Cliente	192.168.30.0/27	255.255.255.224	192.168.30.1	192.168.30.2 - 192.168.30.30	192.168.30.31	30
Desarrolladores y Control de Cambios	192.168.30.32/26	255.255.255.192	192.168.30.33	192.168.30.34 - 192.168.30.94	192.168.30.95	62
Salas de Computo	192.168.30.96/28	255.255.255.240	192.168.30.97	192.168.30.98 - 192.168.30.110	192.168.30.111	14
RRHH y Administracion	192.168.30.112/28	255.255.255.240	192.168.30.113	192.168.30.114 - 192.168.30.126	192.168.30.127	14
Mercadeo	192.168.30.128/28	255.255.255.240	192.168.30.129	192.168.30.130 - 192.168.30.142	192.168.30.143	14

Gerencia	192.168.30.144/29	255.255.255.248	192.168.30.145	192.168.30.146 - 192.168.30.150	192.168.30.151	6
Servidores de Produccion (DMZ)	207.33.08.0/28	255.255.255.240	207.33.08.1	207.33.08.2 - 207.33.08.14	207.33.08.15	16
Otros Servidores (MZ)	192.168.30.176/28	255.255.255.240	192.168.30.177	192.168.30.178 - 192.168.30.190	192.168.30.191	14
Internet y Routers	192.168.30.192/29	255.255.255.248	192.168.30.193	192.168.30.194 - 192.168.30.198	192.168.30.199	6

Enrutamiento

La asignación de direcciones IP para los diferentes dispositivos terminales en el centro de cómputo se ha aplicado de acuerdo con los requerimientos específicos de cada uno. Para los ordenadores de usuarios en áreas como Atención al Cliente, Administración, Mercadeo, y RRHH, se utiliza el protocolo DHCP, el cual está configurado en uno de los servidores de la infraestructura. Los enrutadores, a través del comando ip helper-address [Dirección del Servidor DHCP], son capaces de detectar las peticiones DHCP Discover de los dispositivos terminales y redirigirlas a dicho servidor.

Sin embargo, para ciertos dispositivos críticos como servidores y dispositivos de infraestructura que requieren acceso constante y confiabilidad en sus conexiones, no es conveniente que su dirección IP cambie de manera dinámica, ya que esto podría causar interrupciones en los servicios, afectando su disponibilidad y rendimiento. Por lo tanto, para estos dispositivos, como los servidores de producción se asignaron IPs fijas, respetando el pool de direcciones IP creado anteriormente.

Para los servidores de producción, dado que están expuestos al tráfico externo y deben interactuar con más de 10 millones de clientes concurrentes, se han asignado direcciones IP públicas. Este direccionamiento asegura que los servicios sean accesibles de manera continua y segura desde el exterior.

Además, en los diferentes pools DHCP de la red, se reservaron ciertas direcciones IP para garantizar que ciertos dispositivos críticos mantengan direcciones IP estáticas. A continuación, se presentan las direcciones IP reservadas por subred:

POOL DHCP	**CANTIDAD RESERVADA**	**RANGOS**
Gerencia	1	192.168.30.146 - 192.168.30.150
Administración y RRHH	4	192.168.30.114 - 192.168.30.126
Mercadeo	4	192.168.30.130 - 192.168.30.142
Desarrolladores	4	192.168.30.34 - 192.168.30.94
Recepcion	2	192.168.30.2 - 192.168.30.30
Servidores de Produccion (DMZ - Publico)	14	207.33.08.2 - 207.33.08.14

Para el enrutamiento interno, se implementó el protocolo EIGRP (Enhanced Interior Gateway Routing Protocol) en el área 1. EIGRP fue seleccionado por su capacidad de optimizar las rutas, tomando en cuenta la velocidad y otros factores para el cálculo de la ruta más eficiente. Esto permite la transferencia eficiente de datos entre los diferentes dispositivos y servidores, lo que es crítico dado el alto volumen de tráfico que manejan las aplicaciones con más de 10,000,000 de clientes concurrentes.

VLAN	**Departamento/Área**	**Subred**	**Rango de IPs**	**Gateway**	**Máscara**
VLAN 1	Atención al Cliente (PB)	192.168.30.0/27	192.168.30.1 - 192.168.30.30	192.168.30.1	255.255.255.224
VLAN 2	Desarrolladores y Control de Cambio	192.168.30.32/26	192.168.30.33 - 192.168.30.94	192.168.30.33	255.255.255.192
VLAN 3	Salas de Cómputo	192.168.30.96/28	192.168.30.97 - 192.168.30.110	192.168.30.97	255.255.255.240
VLAN 4	RRHH y Administración	192.168.30.112/28	192.168.30.113 - 192.168.30.126	192.168.30.113	255.255.255.240
VLAN 5	Mercadeo	192.168.30.128/28	192.168.30.129 - 192.168.30.142	192.168.30.129	255.255.255.240
VLAN 6	Gerencia	192.168.30.144/29	192.168.30.145 - 192.168.30.150	192.168.30.145	255.255.255.248
VLAN 7	Servidores de Producción (DMZ)	207.33.8.0/28	207.33.8.1 - 207.33.8.14	207.33.8.1	255.255.255.240
VLAN 8	Otros Servidores (MZ)	192.168.30.176/28	192.168.30.177 - 192.168.30.190	192.168.30.177	255.255.255.240
VLAN 9	Internet y Routers	192.168.30.192/29	192.168.30.193 - 192.168.30.198	192.168.30.193	255.255.255.248

Segmentación de Red mediante VLANs

El uso de VLANs (Virtual Local Area Networks) permite la segmentación lógica de una red física, optimizando tanto la seguridad como la administración de los recursos dentro de un centro de cómputo. Al asignar VLANs específicas a diferentes departamentos y funciones, se garantiza el aislamiento del tráfico de red, evitando interferencias y mejorando la seguridad.

Cada VLAN se configura de acuerdo con los requerimientos operativos de los equipos y usuarios. De esta manera, el tráfico de datos entre distintos departamentos permanece segregado, limitando el acceso a los recursos según las necesidades. Esto es

particularmente importante en entornos con requisitos estrictos de seguridad y acceso, como las áreas de desarrollo, producción y administración.

- VLAN 1 (Atención al Cliente): Segmentada para evitar que el tráfico de este departamento interfiera con otras áreas críticas, lo que mejora la eficiencia y la seguridad.
- VLAN 2 (Desarrolladores y Control de Cambio): Los desarrolladores tienen acceso controlado a los servidores de desarrollo y QA, sin interferir con los servidores de producción, lo que garantiza la estabilidad y seguridad del entorno de producción.
- VLAN 7 (Servidores de Producción - DMZ): Aislada del resto de la red interna, utiliza direcciones IP públicas para facilitar la accesibilidad desde el exterior bajo un estricto control de seguridad.

La segmentación mediante VLANs también facilita la aplicación de políticas de control de acceso mediante Access Lists (ACL) y Firewalls, que permiten definir qué dispositivos y usuarios pueden interactuar con ciertos recursos dentro de la red. Esta arquitectura reduce significativamente los riesgos de acceso no autorizado, al tiempo que optimiza el flujo de trabajo entre los distintos departamentos.

SEGURIDAD

Seguridad Lógica

La seguridad lógica juega un papel fundamental para proteger la información digital y los sistemas informáticos de cada departamento. Esta seguridad se enfoca en salvaguardar todos los activos tecnológicos a nivel electrónico y digital, diferenciándose de la seguridad física que se ocupa de proteger los equipos y las instalaciones.

Dado que el proyecto cuenta con un contrato con Microsoft, se implementará Active Directory (AD) como la plataforma principal para gestionar el acceso y la autenticación de los usuarios. Active Directory permite una administración centralizada de usuarios, dispositivos y recursos, lo que facilita el control sobre quién accede a qué sistemas y en qué condiciones. Además, se utilizarán políticas de grupo (Group Policy) para establecer contraseñas seguras, reglas de autenticación multifactorial (MFA) y directrices para la gestión de contraseñas.

Los controles de acceso basados en roles (RBAC) se integrarán directamente con Active Directory para definir permisos específicos según el nivel de responsabilidad de cada usuario, garantizando que departamentos como Desarrollo, RRHH, Mercadeo y Gerencia accedan únicamente a las aplicaciones y datos necesarios para sus funciones.

Para proteger la transmisión de datos tanto internos como externos, se implementarán soluciones de encriptación proporcionadas por tecnologías de Microsoft, como BitLocker para el cifrado de discos y TLS/SSL para asegurar las comunicaciones. Además, se utilizarán herramientas avanzadas para la prevención de intrusiones, incluyendo Microsoft Defender for Endpoint para proteger contra amenazas y firewalls configurados para monitorizar continuamente el tráfico de la red y bloquear intentos no autorizados de acceso.

Se desplegarán soluciones antimalware basadas en Microsoft Defender en todas las estaciones de trabajo y servidores, con actualizaciones automáticas para detectar y neutralizar las últimas amenazas conocidas. La plataforma Azure Sentinel se utilizará para la auditoría y monitoreo continuo del sistema, permitiendo detectar actividades sospechosas y responder rápidamente a cualquier intento de vulneración de la seguridad.

Este enfoque integral de seguridad lógica, basado en tecnologías de Microsoft, permite proteger no solo los datos críticos de la organización sino también las aplicaciones web que manejan más de 10 millones de clientes, garantizando la continuidad operativa y la integridad de la información en un entorno seguro y bien administrado.

Intranet

Siendo una intranet una red privada que opera de manera similar a Internet, pero a la que solo tienen acceso los miembros de una organización o entidad. Su propósito principal es facilitar la comunicación, colaboración y el acceso seguro a los recursos internos sin exponer la red a Internet. Dado que el proyecto incluye un centro de cómputo en un edificio de varios pisos, la intranet permitirá gestionar la distribución de servicios y aplicaciones entre los departamentos, controlando el acceso y optimizando el flujo de información. Una intranet ofrece diversas ventajas para el proyecto, entre las cuales se destacan:

- Acceso Controlado y Seguro: Cada usuario accede solo a los recursos que necesita según su rol, mejorando la seguridad y eficiencia.
- Mejora de la Comunicación y Colaboración: Los departamentos pueden comunicarse y colaborar internamente mediante aplicaciones y servicios específicos.
- Centralización de Servicios y Datos: Todos los recursos importantes se encuentran en el centro de cómputo, facilitando su administración, monitoreo y protección.
- Optimización de Recursos de Red: Segmentar la red con VLANs reduce el uso de ancho de banda y mejora la gestión del tráfico.
- Reducción de Riesgos de Exposición Externa: Al estar aislada de Internet, la intranet minimiza el riesgo de ataques externos.

Para este tipo de instalación, una intranet proporciona:

- Centralización de servicios críticos: Como autenticación, aplicaciones de gestión (ERP), bases de datos, y más.
- Aislamiento y seguridad: Limitando el acceso externo y permitiendo una mayor supervisión y control sobre la información y los dispositivos conectados.
- Gestión eficiente de recursos: Proporciona a cada usuario y departamento el acceso a los servicios necesarios, según sus roles y autorizaciones.

Dado el tamaño del edificio y la cantidad de departamentos y pisos, la topología de red de la intranet debe diseñarse de manera estructurada, considerando aspectos como conectividad, rendimiento y seguridad.

- Centro de Cómputo (Zona Militarizada): Este será el núcleo de la red y contendrá los servidores críticos de la intranet, como los servidores de aplicaciones, bases de datos, controladores de dominio, almacenamiento de backup, y servicios de autenticación como Active Directory. Estos servidores estarán ubicados en una zona militarizada (DMZ) para agregar una capa de seguridad, controlando y limitando el acceso.
- Uso de Zona Desmilitarizada (DMZ): La DMZ es una zona intermedia entre la intranet y cualquier posible acceso externo. En este caso, la DMZ se configurará para alojar servicios que puedan requerir accesos externos controlados, como un servidor web o un sistema de correo electrónico corporativo. Esta zona es fundamental para proteger el centro de cómputo del acceso externo directo, lo que también mitiga riesgos de ataques cibernéticos.
- Switches de Distribución en Cada Piso: En cada piso del edificio se instalarán switches de distribución que conectarán los dispositivos de los usuarios con el centro de cómputo. Cada uno de estos switches estará conectado mediante fibra óptica para garantizar una transmisión de datos rápida y eficiente.
- Segmentación mediante VLANs: La red se segmentará en VLANs específicas para cada departamento y grupo funcional, lo que facilita el control y aislamiento del tráfico entre diferentes áreas del edificio. Esto asegura que el tráfico de un departamento no interfiera ni acceda a la información de otro, aumentando la seguridad.

Estrategia de seguridad de la Intranet

Para proteger la intranet y los datos que se almacenarán en ella, es vital implementar una estrategia de seguridad sólida que aborde los siguientes aspectos:

- **Firewall**

Aquí se definieron distintas reglas para evitar la conexión y acceso no permitido a zonas sensibles, a continuación, se representa en una tabla como se definieron los accesos a la zona militarizada.

Equipo	Red permitida	Descripción
Servidores de Desarrollo	192.168.30.32/26	Solo se permitió acceso desde el departamento de Desarrolladores y Control de Cambio.
Servidores QA	192.168.30.32/26 192.168.30.128/28	Los departamentos de Desarrollo y Control de Cambio tienen acceso, además del equipo de Mercadeo que prueba aplicaciones antes de producción.
Servidores de Producción	207.33.08.0/28	Accesibles únicamente desde los servidores de Desarrollo y QA autorizados, además de los clientes externos mediante IP pública.

- **Access-list**
    - **Reglas de Servidores de Desarrollo:**
        - Solo los dispositivos de la subred de Desarrolladores (192.168.30.32/26) tienen permiso para acceder a los servidores de desarrollo. Cualquier otro tráfico hacia estos servidores será denegado.

```
access-list 101 permit ip 192.168.30.32 0.0.0.63 any
access-list 101 deny ip any any
```

    - **Reglas de Servidores de QA:**
        - Se permite el acceso desde las subredes de Desarrolladores y QA (192.168.30.32/26 y 192.168.30.128/28) para realizar pruebas de software. Tráfico no autorizado será denegado.

```
access-list 102 permit ip 192.168.30.32 0.0.0.63 any
access-list 102 permit ip 192.168.30.128 0.0.0.15 any
access-list 102 deny ip any any
```

    - **Reglas de Servidores de Producción (DMZ):**
        - Solo los servidores de desarrollo, QA, y el tráfico proveniente del exterior (clientes) pueden acceder a los servidores de producción,

con una IP pública asignada (207.33.08.0/28).

```
access-list 103 permit ip 192.168.30.32 0.0.0.63 207.33.08.0 0.0.0.15
access-list 103 permit ip 192.168.30.128 0.0.0.15 207.33.08.0 0.0.0.15
access-list 103 permit ip 207.33.08.0 0.0.0.15 any
access-list 103 deny ip any any
```

- **Reglas de Bases de Datos (BD):**
  - Solo los servidores de Producción y los desarrolladores autorizados pueden acceder a los servidores de base de datos.

```
access-list 104 permit ip 192.168.30.32 0.0.0.63 207.33.08.0 0.0.0.15
access-list 104 permit ip 207.33.08.0 0.0.0.15 any
access-list 104 deny ip any any
```

- **Reglas para Impresoras:**
  - Las impresoras solo están disponibles para los departamentos de Administración, RRHH y Gerencia (192.168.30.112/28 y 192.168.30.144/29). Ningún otro departamento puede acceder a ellas.

```
access-list 105 permit ip 192.168.30.112 0.0.0.15 192.168.30.176 0.0.0.7
access-list 105 permit ip 192.168.30.144 0.0.0.7 192.168.30.176 0.0.0.7
access-list 105 deny ip any any
```

- **Actualización de Parches de Seguridad**: Todo el software, desde el sistema operativo de los servidores hasta las aplicaciones, debe mantenerse actualizado.
- **Pruebas de Penetración y Evaluación de Vulnerabilidades:** Evaluaciones periódicas ayudan a detectar vulnerabilidades antes de que puedan ser explotadas, asegurando que el sistema siempre esté preparado ante nuevas amenazas.
- **Active Directory**

El Directorio Activo juega un papel esencial en la infraestructura de red de esta organización, permitiendo una gestión centralizada de usuarios y recursos. Garantiza que solo los usuarios autorizados accedan a la información sensible, y facilita la administración segura de contraseñas y el acceso a recursos compartidos. Este sistema almacena de manera eficiente la información sobre usuarios, grupos, dispositivos y otros componentes de la red.

En esta estructura, el Directorio Activo está dividido por dominios específicos para cada departamento, lo que permite aplicar políticas de seguridad personalizadas según las necesidades de cada área. Además, se han establecido relaciones de confianza entre los

administradores de cada dominio, lo que permite compartir recursos de manera segura entre las áreas sin comprometer la seguridad general de la red.

A continuación, se presentan los usuarios y administradores asignados a cada departamento clave en el Directorio Activo:

Departamento	**Rol**	**Usuario**	**ID de usuario**	**Correo electrónico**	**Fecha de creación**
Desarrolladores	Controlador de dominio	Juan Perez	juan.perez	juan.perez@empresa.com	01/01/2023
	Administrador de dominio	Manuel Flores	manuel.flores	manuel.flores@empresa.com	01/01/2023
		Patricia Reyes	patricia.reyes	patricia.reyes@empresa.com	05/03/2023
		Ricardo Cruz	ricardo.cruz	ricardo.cruz@empresa.com	10/03/2023
	Usuario	Isabel Silva	isabel.silva	isabel.silva@empresa.com	01/04/2023
		Fernando Rojas	fernando.rojas	fernando.rojas@empresa.com	01/01/2023 05/01/2023
Administración y RRHH	Controlador de dominio	Paula Mendoza	paula.mendoza	paula.mendoza@empresa.com	10/04/2023
	Administrador de dominio	Maria Lopez	maria.lopez	maria.lopez@empresa.com	12/04/2023
	Usuario	Carlos Gomez	carlos.gomez	carlos.gomez@empresa.com	01/01/2023
		Ana Martinez	ana.martinez	ana.martinez@empresa.com	05/01/2023

Mercadeo	Controlador de dominio	Luis Hernandez	luis.hernandez	luis.hernandez@empresa.com	10/01/2023
	Administrador de dominio	Jose Garcia	jose.garcia	jose.garcia@empresa.com	01/01/2023
	Usuario	Laura Rodriguez	laura.rodriguez	laura.rodriguez@empresa.com	05/01/2023
		Pedro Sanchez	amartin.pedro	pedro.sanchez@empresa.com	10/01/2023
		Sofia Ramirez	mgarcia.sofia	sofia.ramirez@empresa.com	01/01/2023
Gerencia	Controlador de dominio	Miguel Torres	miguel.torres	miguel.torres@empresa.com	10/04/2023
	Administrador de dominio	Lucia Fernandez	ksmith.lucia	lucia.fernandez@empresa.com	01/04/2023
	Usuario	Diego Morales	wparker.diego	diego.morales@empresa.com	05/01/2023
		Elena Vargas	cbrown.elena	elena.vargas@empresa.com	05/01/2023
Atención al cliente	Controlador de dominio	Andres Castro	andres.castro	andres.castro@empresa.com	01/01/2023
	Administrador de dominio	Javier Diaz	gturner.javier	javier.diaz@empresa.com	05/01/2023
	Usuario	Carmen Ortiz	mroberts.carmen	carmen.ortiz@empresa.com	10/04/2023

Estado de cuenta	**Ultimo acceso**	**Nivel de Acceso**
Activa	20/10/2024	Total (Controlador)

Activa	21/10/2024	Alto (Administración)
Activa	22/10/2024	Alto (Administración)
Activa	20/10/2024	Alto (Administración)
Activa	24/10/2024	Medio (Desarrollo y Prueba)
Activa	25/10/2024	Medio (Desarrollo y Prueba)
Activa	25/10/2024	Total (Controlador)
Activa	20/10/2024	Alto (Finanzas y RRHH)
Activa	23/10/2024	Medio (Nómina)
Activa	22/10/2024	Medio (Nómina)
Activa	22/10/2024	Total (Controlador)
Activa	25/10/2024	Alto (Campañas)
Activa	25/10/2024	Alto (Campañas)
Activa	23/10/2024	Medio (CRM)
Activa	22/10/2024	Medio (CRM)
Activa	21/10/2024	Total (Controlador)
Activa	23/10/2024	Alto (Reportes)
Activa	22/10/2024	Medio (Reportes)
Activa	23/10/2024	Medio (Reportes)
Activa	23/10/2024	Total (Controlador)
Activa	21/10/2024	Alto (Soporte al Cliente)
Activa	20/10/2024	Medio (Soporte al Cliente)

- Departamento: Define la unidad organizativa (departamento) a la que pertenece cada usuario, como Desarrolladores, Administración y RRHH, Mercadeo, Gerencia, o Atención al Cliente. Este campo es esencial para segmentar el acceso y asignar políticas de seguridad específicas según las funciones del área.
- Rol: Especifica el nivel de privilegio del usuario dentro de Active Directory para su departamento. Los roles incluyen:
- Controlador de Dominio: Encargado de la administración central de seguridad, autenticación y configuración en el dominio.
- Administrador de Dominio: Gestiona usuarios y permisos en el dominio, configurando políticas de acceso.

- Usuario: Cuenta operativa con acceso limitado a los recursos específicos de su área, según sus funciones.
- Nombre de Usuario: Nombre completo del usuario, útil para identificarlo en la organización. Este campo facilita la revisión de roles y permisos asignados, y permite la generación de informes claros en auditorías.
- ID de Usuario: Nombre de usuario único en el sistema de Active Directory, usado para la autenticación y para el acceso a recursos. Este ID es clave para el inicio de sesión en la red y para rastrear actividades individuales de cada usuario en el sistema.
- Correo Electrónico: Dirección de correo asociada a la cuenta de usuario en AD. Este campo es vital para la comunicación interna, recuperación de contraseñas y para la configuración de sistemas de autenticación de múltiples factores (MFA) en aplicaciones de seguridad.
- Fecha de Creación: Indica el día en que se creó la cuenta en Active Directory. Este dato es importante para monitorear la antigüedad de las cuentas, verificar su creación dentro de procedimientos de alta de personal y realizar auditorías de control.
- Estado de Cuenta: Define si la cuenta está Activa, Desactivada, o En Espera. Mantener actualizado el estado de cada cuenta es esencial para controlar el acceso a la red, especialmente en casos de rotación de personal, permisos temporales o usuarios inactivos.
- Último Acceso: Fecha del último inicio de sesión del usuario en el sistema. Este campo es útil para identificar cuentas inactivas, revisar el uso efectivo de las cuentas y tomar decisiones de limpieza o actualización de usuarios en el sistema, además de ayudar a detectar accesos no autorizados.
- Nivel de Acceso: Describe el nivel de permisos asignados al usuario dentro de su dominio, indicando el alcance de sus capacidades. Los niveles de acceso incluyen:
    - Total: Acceso completo a todas las configuraciones y recursos en el dominio (usualmente reservado para los Controladores de Dominio).
    - Alto: Permisos avanzados para la administración de aplicaciones y recursos críticos (para Administradores de Dominio).

- Medio: Permisos operativos que limitan al usuario a funciones específicas de su trabajo, asegurando que acceda solo a los recursos necesarios para sus tareas.

Los campos de perfil en Active Directory brindan una visión integral del usuario, clave para el control de accesos, ya que permiten a los administradores asignar y revisar permisos según el rol y las necesidades de cada usuario; seguridad y auditoría, facilitando la detección de accesos indebidos, auditorías de cuentas activas e inactivas, y asegurando el cumplimiento de políticas de seguridad; y gestión de usuarios, optimizando la administración del ciclo de vida de las cuentas desde su creación hasta la desactivación, mejorando la seguridad y eficiencia de la red. Cada departamento tiene su propio dominio, lo que refuerza la seguridad y garantiza que las políticas se apliquen de acuerdo con las funciones de cada área. Además, se ha implementado un servicio de backup en cada dominio para asegurar la continuidad operativa en caso de fallas, permitiendo que los usuarios mantengan acceso a los recursos esenciales.

Seguridad Física

La seguridad física se refiere a las medidas y controles implementados para proteger la infraestructura física del centro de cómputo, incluyendo sistemas, servidores, centros de datos, equipos de red y otros recursos críticos. Estas medidas están diseñadas para evitar el acceso no autorizado y proteger los activos tecnológicos mediante el uso de barreras físicas, como controles de acceso, cámaras de seguridad y cerraduras electrónicas.

Enrutadores

Se ha implementado una arquitectura de subredes independientes para cada departamento o área. Cada subred cuenta con su propio enrutador para garantizar la comunicación controlada entre las diferentes áreas del edificio. Estos enrutadores no solo facilitan la interconexión de equipos de diferentes departamentos, sino que también permiten aislar ciertas subredes, limitando el acceso a usuarios no autorizados.

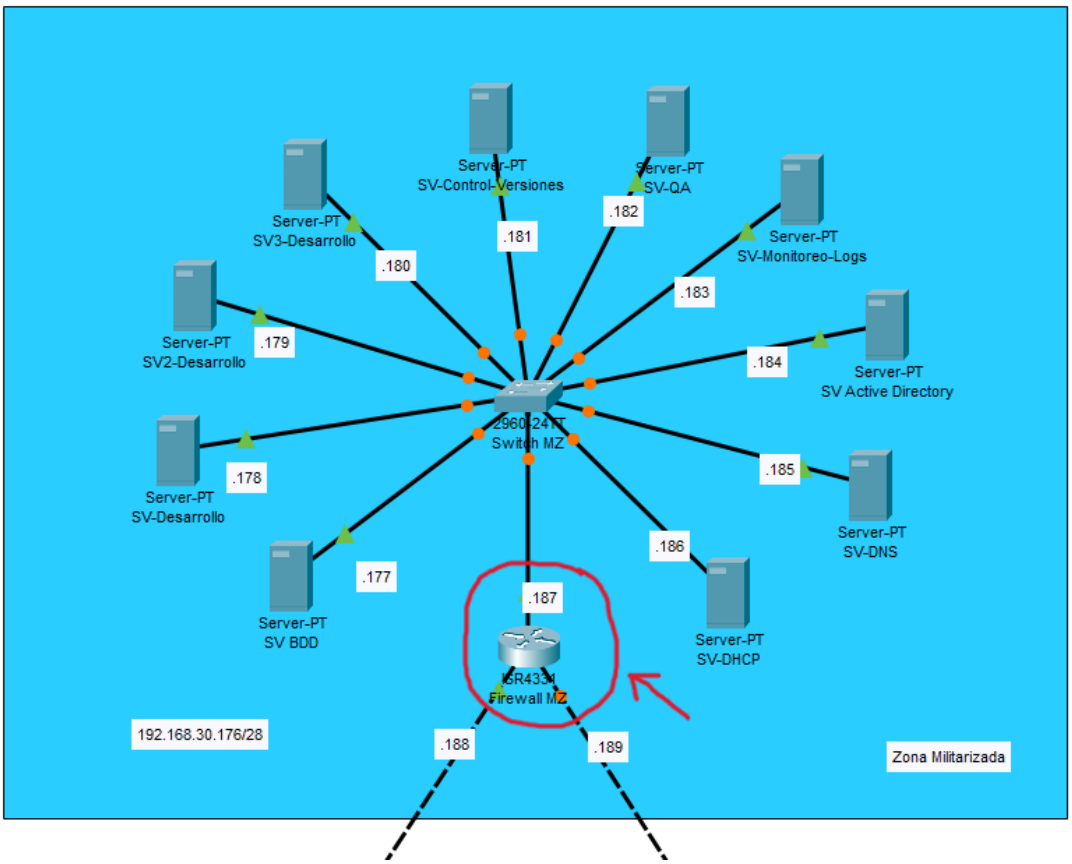
Para asegurar una mayor segmentación y seguridad, se utilizarán Listas de Control de Acceso (ACLs) configuradas en los enrutadores, lo que nos permitirá restringir el tráfico hacia y desde las áreas sensibles del centro de cómputo. Esta configuración asegura que solo los usuarios y dispositivos autorizados puedan acceder a recursos específicos, protegiendo áreas como los servidores de producción y los sistemas administrativos.

Firewalls

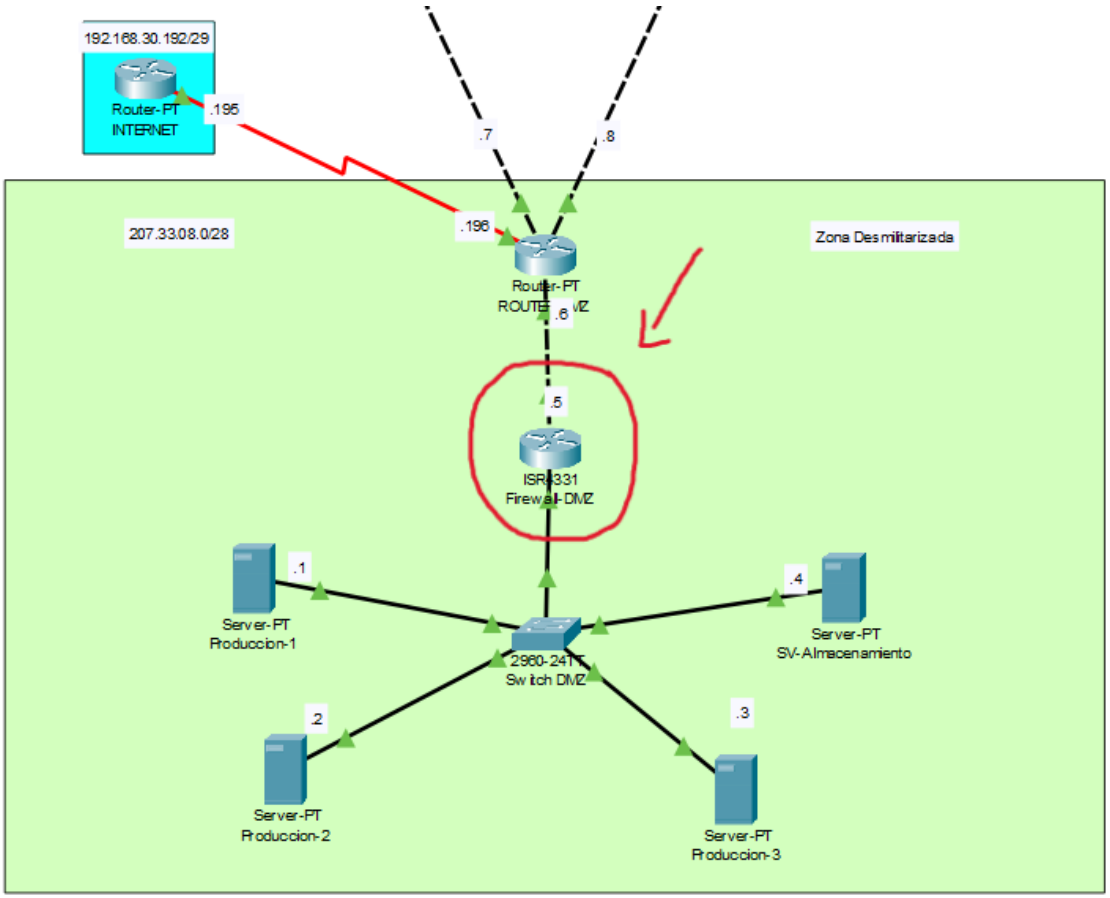
Los firewalls son componentes cruciales para proteger las subredes y servidores contra ataques externos y accesos no autorizados. Se han implementado firewalls estratégicamente en las áreas más críticas del centro de cómputo, como la zona de servidores de producción y la zona militarizada.

La ventaja de utilizar tecnologías Microsoft y Windows Server es que se integran perfectamente con el Active Directory y otros sistemas de gestión ya implementados en la red, lo que permite una administración centralizada y eficiente de la seguridad.

Con esta estrategia de seguridad física, que combina controles de acceso, firewalls avanzados y una segmentación efectiva de las redes, garantizamos una protección sólida y adaptable para el centro de cómputo, facilitando al mismo tiempo la escalabilidad y la operación continua del edificio.



Firewall zona MZ



Firewall zona DMZ

Zona Desmilitarizada y Zona Militarizada

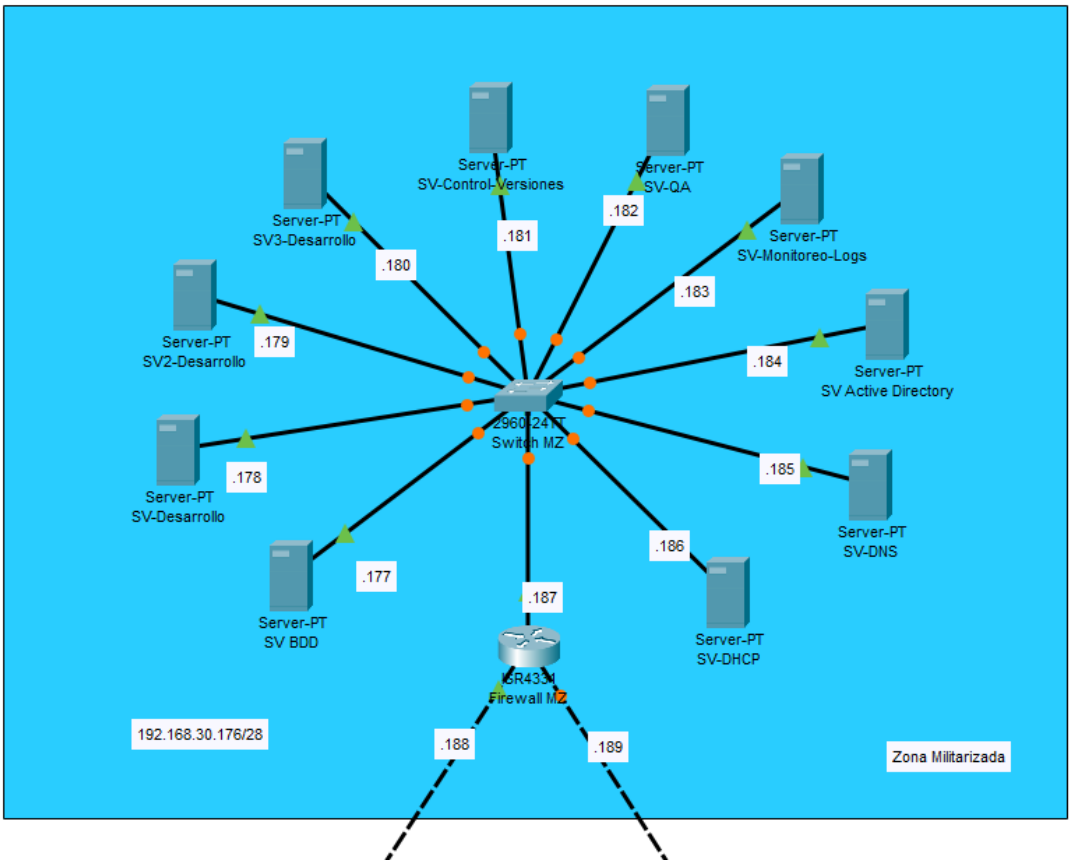
Se han implementado dos áreas críticas para la seguridad y gestión de los servidores: la Zona Militarizada (MZ) y la Zona Desmilitarizada (DMZ).

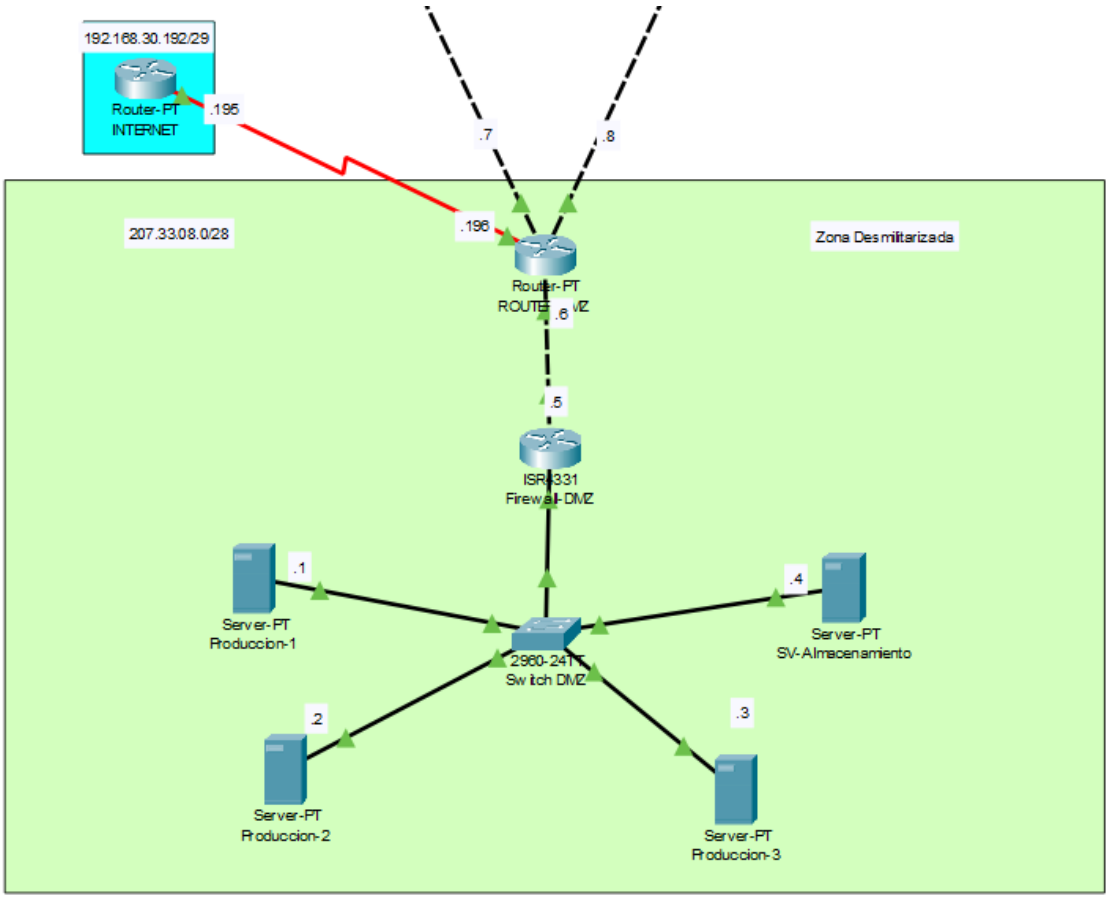
La Zona Militarizada (MZ) es la región de la red donde se encuentran los servidores internos más críticos y sensibles, que manejan la información confidencial y los procesos de gestión de la organización. Esta área está protegida por múltiples capas de seguridad, incluyendo firewalls basados en tecnologías de Windows Server y configuraciones de Active Directory para controlar y monitorear el acceso a los recursos.

La MZ se encuentra segmentada de las demás áreas del centro de cómputo para asegurar que el tráfico interno sea cuidadosamente regulado, permitiendo únicamente el acceso a usuarios y sistemas autenticados. Esto garantiza que los datos internos y las aplicaciones sensibles estén resguardados de amenazas potenciales y accesos no autorizados.

Por otro lado, la Zona Desmilitarizada (DMZ) es donde se alojan los servidores de producción que necesitan estar accesibles desde el exterior, como servicios web y otros recursos públicos. Estos servidores están conectados directamente a un switch que a su vez se enlaza con el enrutador principal facilitando el acceso controlado desde redes externas y permitiendo una rápida respuesta a las solicitudes entrantes.

Para optimizar el rendimiento y la disponibilidad de estos servidores de producción, se ha considerado la implementación de un balanceador de carga. Este balanceador distribuirá el tráfico de manera eficiente entre los servidores de la DMZ, evitando sobrecargas y asegurando que los servicios permanezcan operativos incluso durante picos de demanda. Este enfoque minimiza las barreras al acceso externo, pero mantiene un nivel adecuado de protección mediante las reglas de seguridad establecidas en los firewalls de la red.





Zona militarizada y desmilitarizada (Parte superior zona militarizada, parte inferior zona desmilitarizada)

Instalaciones

El acceso a las instalaciones del centro de cómputo y las áreas asignadas a cada departamento en el edificio de 20 pisos es un aspecto crítico para proteger los recursos informáticos y la infraestructura. El acceso a las áreas de servidores y redes debe estar estrictamente controlado y limitado únicamente al personal autorizado, como administradores de sistemas y gerentes responsables de la gestión y mantenimiento de la infraestructura. El monitoreo continuo de estas áreas es esencial para prevenir actividades no autorizadas o manipulaciones indebidas.

Para garantizar la máxima seguridad, se implementarán sistemas de control de acceso en red que permitirán una gestión detallada y precisa del ingreso a las diferentes áreas del edificio. Este control se complementará con tecnologías avanzadas como el reconocimiento de huellas dactilares o tarjetas de identificación electrónicas, asegurando que solo los usuarios previamente autorizados puedan acceder a los pisos o departamentos

correspondientes. Adicionalmente, se mantendrán registros detallados de acceso para un monitoreo efectivo y trazabilidad.

El edificio también contará con un sistema de cámaras de vigilancia ubicadas estratégicamente en cada piso, enfocadas en las áreas críticas, para identificar a cualquier persona que intente ingresar sin el debido permiso, reforzando la seguridad del centro de cómputo.

Consideraciones a tomar en cuenta:

- **Ubicación adecuada:** Los servidores y equipos electrónicos estarán colocados estratégicamente para minimizar la exposición a fuentes de calor y garantizar una distribución eficiente del flujo de aire. Esta disposición ayudará a reducir el riesgo de sobrecalentamiento y a maximizar la eficiencia de los sistemas de climatización.
- **Sistema de detección de incendios:** Se instalarán sistemas avanzados de detección de incendios en el área de servidores y otras áreas críticas del edificio. Estos incluirán detectores de humo, calor y llama, todos conectados a una alarma central y al sistema de monitoreo de seguridad para una respuesta rápida en caso de incidentes. Para la supresión de incendios, se utilizarán sistemas de extinción por gas como el dióxido de carbono (CO_2), que son ideales para proteger los equipos electrónicos del centro de cómputo, evitando daños que pudieran ser causados por métodos de extinción más convencionales como agua o espuma.
- **Ventilación Adecuada:** El área de servidores estará equipada con sistemas de aire acondicionado de precisión y refrigeración eficiente para mantener una temperatura óptima y evitar el sobrecalentamiento. Los deshumidificadores serán utilizados para controlar la humedad relativa y prevenir la acumulación de humedad que podría dañar los equipos. Se implementarán también barreras físicas y un sellado adecuado de las áreas críticas para prevenir la entrada de humedad del entorno circundante, utilizando elementos como cortinas de aire y burletes para minimizar las filtraciones.
- **Cableado Seguro:** Todo el cableado eléctrico del edificio será instalado de acuerdo con los más altos estándares de seguridad, utilizando cables ignífugos para reducir la propagación del fuego en caso de una emergencia. Se evitará la sobrecarga de los circuitos eléctricos para minimizar los riesgos.

- **Mantenimiento Regular:** Se realizarán inspecciones y mantenimiento regular de todos los sistemas de detección y supresión de incendios, así como de los sistemas de ventilación, para asegurar su correcto funcionamiento. Además, se garantizará que todos los extintores estén accesibles y en óptimas condiciones.
- **Control de la temperatura y la Humedad:** Es importante mantener un control preciso de la temperatura y la humedad relativa en el centro de cómputo mediante sistemas de climatización adecuados, para ello se pensó en el uso de:
- **Aire Acondicionado de precisión:** Los sistemas de aire acondicionado de precisión son fundamentales para mantener una temperatura estable y controlada en el centro de cómputo. Estos equipos están diseñados específicamente para entornos críticos como centros de datos y ofrecen características avanzadas, como:
- **Control de Temperatura Constante:** Permite una regulación precisa de la temperatura, lo que es crucial para el rendimiento y la durabilidad de los servidores y otros equipos críticos.
- **Distribución Uniforme del Aire:** Garantiza que el flujo de aire se distribuya equitativamente en todas las áreas del centro de cómputo, evitando puntos calientes que puedan dañar los equipos.
- **Filtración de Partículas y Control de Humedad:** Muchos de estos sistemas incluyen filtros de alta eficiencia y deshumidificadores integrados, eliminando la necesidad de adquirir equipos adicionales para controlar la humedad relativa en el entorno.
- **Deshumificadores:** Para los entornos donde la humedad pueda ser un problema crítico, se utilizan deshumidificadores que pueden ser unidades independientes o integradas en los sistemas de aire acondicionado de precisión. Estos dispositivos eliminan la humedad del aire, protegiendo los equipos de posibles daños por condensación y asegurando un ambiente estable.
- **Barreras Fisicas y Sellado:** Es crucial garantizar que las áreas de servidores estén adecuadamente selladas para evitar la entrada de humedad y polvo. Esto incluye:
    - Sellado de Puertas y Ventanas: Uso de burletes y cortinas de aire para minimizar filtraciones y mantener el entorno controlado.
    - Diseño de Barreras Físicas: Implementación de divisiones y barreras para separar las zonas críticas de posibles fuentes de humedad.

- **Control de Fugas de Agua:** El agua puede ser una amenaza significativa para un centro de cómputo. Para evitar problemas:
    - Inspecciones Regulares: Revisión periódica de las instalaciones hidráulicas y del techo para detectar posibles fugas.
    - Sistemas de Detección de Fugas: Instalación de sensores de agua y sistemas de alerta para identificar cualquier infiltración y responder rápidamente.
- **Sistema de Respaldo de Energia:** Los sistemas de respaldo son vitales para asegurar que el centro de cómputo continúe operando sin interrupciones:
    - Sistemas de Alimentación Ininterrumpida (UPS): Estos sistemas se encargarán de mantener la energía a los equipos críticos durante los cortes de energía momentáneos, protegiendo a los servidores y otros dispositivos de daños.
    - Generadores Eléctricos: Instalación de generadores que entren en funcionamiento automáticamente en caso de fallos prolongados en el suministro eléctrico.
- **Proteccion Contra Sobretensiones y Bajas de Tension:**
    - Dispositivos de Protección contra Sobretensiones (SPD): Instalados tanto en el panel principal como en los paneles de distribución de cada piso, estos dispositivos desvían el exceso de corriente hacia la tierra, protegiendo los equipos conectados.
    - Reguladores de Voltaje: Uso de reguladores para estabilizar el suministro eléctrico, asegurando que cualquier fluctuación de voltaje no afecte a los servidores ni a otros dispositivos sensibles.
- **Mantenimiento y Pruebas Continuas:** Implementar un plan de mantenimiento riguroso para realizar pruebas frecuentes a todos los sistemas eléctricos y de respaldo, asegurando su operatividad continua.
- **Alternativas de Generación Eléctrica:**
    - **Sistemas de Energía Renovable:**
        - Paneles Solares: Instalación de paneles solares para generar energía limpia y reducir la dependencia de la red eléctrica, diseñados para proporcionar energía suficiente durante cortes prolongados.

        - Baterías de Alta Capacidad: Uso de baterías para almacenar la energía generada y garantizar que el suministro eléctrico sea constante y estable para todos los equipos del centro de cómputo.
    - **Dispositivos de Bajo Consumo:**
        - Conectar equipos de bajo consumo (como enrutadores, switches, y puntos de acceso) a sistemas UPS para que puedan operar sin interrupciones sin requerir grandes demandas eléctricas.
    - **Transformadores y Reguladores de Energía:**
        - Equipar el sistema con transformadores que conviertan adecuadamente la energía generada por paneles solares o baterías, asegurando que sea adecuada para alimentar los servidores y demás dispositivos de alto consumo.
- **Protección Integral:**
    - **Programa de Mantenimiento y Monitoreo:** Establecer un protocolo de mantenimiento y pruebas continuas para todos los sistemas eléctricos y de climatización, garantizando que estén siempre en perfecto estado y listos para operar en situaciones críticas.
    - **Alternativas de internet y fallas de servidores:**
        - Para mantener la conectividad en caso de una falla del servidor o de la conexión a Internet principal, se considerarán varias alternativas:
            1. **Conexión de respaldo:** Se configurará una conexión secundaria a Internet de un proveedor alternativo, utilizando enrutadores con capacidad de conmutación automática para cambiar al proveedor de respaldo en caso de una interrupción.
            2. **Puntos de acceso móviles:** Se dispondrá de dispositivos móviles o puntos de acceso como respaldo temporal para asegurar la continuidad del servicio en áreas críticas del edificio.
            3. **Redes WiFi públicas seguras:** Cuando sea posible, se evaluará la posibilidad de utilizar redes WiFi públicas con medidas adicionales de seguridad, como el uso de VPN, para proteger las conexiones.

4. **Conectividad de respaldo vecinal**: Se establecerán acuerdos con empresas cercanas para compartir sus conexiones a Internet en caso de emergencias, utilizando enlaces seguros.

Administración de la Red

- **Monitoreo:** Para mantener la eficiencia y seguridad de la red en el edificio, se implementará un sistema de monitoreo continúo basado en herramientas como Azure Sentinel y Microsoft Defender, aprovechando el contrato con Microsoft. Estas herramientas permiten detectar intrusiones, analizar el tráfico de la red y monitorear el uso de ancho de banda en tiempo real. El monitoreo proactivo ayuda a identificar rápidamente problemas de rendimiento, intentos de acceso no autorizado y posibles amenazas, permitiendo una rápida respuesta para minimizar riesgos.

  El sistema de monitoreo incluirá alarmas y notificaciones para alertar al personal de TI en caso de anomalías, garantizando que cualquier actividad sospechosa sea revisada y gestionada de inmediato. Esto también ayudará a mantener el cumplimiento de las políticas de seguridad definidas, como la separación entre zonas DMZ y MZ.
- **Backup:** Para garantizar la continuidad operativa, se establecerá una política de respaldo de datos en cada dominio de Active Directory por departamento. Estos backups se programarán regularmente y almacenarán en servidores dedicados dentro de la Zona Militarizada (MZ) para proteger datos sensibles. Además, los backups se duplicarán en un almacenamiento secundario ubicado fuera del centro de datos para mayor seguridad. Las copias de seguridad incluirán tanto datos críticos de los servidores de producción como configuraciones de red y políticas de seguridad, facilitando una restauración completa y rápida en caso de fallas. El uso de Azure Backup permitirá la automatización de este proceso, asegurando que cada copia de seguridad sea actualizada periódicamente sin intervención manual.
- **Mantenimiento de Software y Hardware:** El mantenimiento preventivo y correctivo será un componente esencial para la estabilidad de la red. El equipo de TI programará revisiones mensuales de todos los sistemas,

incluyendo actualizaciones de firmware para routers y switches Cisco, así como revisiones de seguridad y actualizaciones de Windows Server y Microsoft Defender. Cada seis meses, se realizará una auditoría integral de la infraestructura física y lógica para evaluar el estado general y hacer ajustes según las necesidades de la organización. En cuanto al hardware, el plan de mantenimiento incluye limpieza regular de componentes críticos como routers y servidores, revisión de los sistemas de ventilación y enfriamiento, y pruebas de los sistemas de respaldo de energía. Esto garantiza que los dispositivos operen a su máxima capacidad y con una alta disponibilidad, minimizando el riesgo de fallas inesperadas.

- **Capacitación del Personal:** Para maximizar la efectividad y seguridad de la administración de la red, el personal de TI y los usuarios clave en cada departamento recibirán capacitación especializada y continua en áreas críticas de gestión y seguridad de redes. El programa de capacitación incluirá:
  - **Formación en Seguridad de Red y Respuesta ante Incidentes:** El personal recibirá entrenamiento detallado en la identificación de amenazas y en protocolos de respuesta ante incidentes de seguridad. Esta capacitación incluirá prácticas sobre el uso de herramientas de monitoreo, como Azure Sentinel, y sistemas de firewall para reconocer patrones de actividad sospechosa y responder rápidamente a intentos de acceso no autorizado. Simulacros periódicos de incidentes ayudarán al equipo a estar bien preparado y asegurarán una respuesta coordinada y eficaz en caso de emergencias.
  - **Certificación en Plataformas Microsoft y Cisco:** Dada la importancia de las herramientas de Microsoft (como Active Directory y Azure) y los equipos Cisco en la infraestructura de red, el personal técnico recibirá formación certificada en su instalación, configuración y administración avanzada. Esto incluirá cursos y talleres prácticos sobre gestión de VLANs, control de acceso, configuración de enrutadores y switches, y administración de usuarios mediante políticas de Active Directory. La certificación asegura que el equipo esté al tanto de las mejores prácticas de

administración y de las últimas actualizaciones de seguridad y funcionalidad.

- **Capacitación en Protocolos de Backup y Recuperación de Datos:** Dado el rol crítico del respaldo de datos en la continuidad operativa, el equipo de TI recibirá una formación exhaustiva en el uso de Azure Backup y en los protocolos internos de recuperación. Esto incluye procedimientos para programar, verificar y restaurar backups de manera eficiente, minimizando el tiempo de inactividad en caso de fallos. Simulacros de recuperación y restauración asegurarán que el personal esté preparado para ejecutar el proceso sin errores y con rapidez.
- **Actualización Continua y Entrenamiento en Nuevas Tecnologías y Ciberseguridad:** La capacitación del personal será continua, con actualizaciones semestrales que incluyan las últimas tendencias y amenazas en ciberseguridad, así como nuevas tecnologías y prácticas de administración de redes. Seminarios sobre inteligencia artificial aplicada a la seguridad de redes y sesiones sobre tecnologías emergentes fortalecerán el conocimiento del equipo para adaptarse a la evolución tecnológica y mejorar la protección de la infraestructura.
- **Capacitación en Comunicación y Colaboración Interdepartamental:** Como la administración de la red implica la colaboración entre distintas áreas del edificio, el personal recibirá formación en comunicación eficaz para trabajar de manera coordinada con otros departamentos. Esto facilitará la solución rápida de problemas y la implementación de políticas de seguridad específicas en cada departamento, asegurando que la red funcione de manera segura y sin interrupciones en todas las áreas.

ESTRUCTURA DE COSTOS

Estructura de Costos:

Se presenta la siguiente es una estimación detallada de los costos asociados a la implementación de la infraestructura de red y hardware necesario para un edificio de 20

pisos. Se han seleccionado equipos modernos y de última generación, adecuados para garantizar el rendimiento, la seguridad y la eficiencia operativa de la red. A continuación, se presenta la descripción del equipo utilizado, la cantidad requerida, el consumo de energía y su costo.

Unidad de Medida	Tipo	Descripción	Cantidad	Repuestos	Watts Requeridos	Precio Unitario ($)	Total ($)
und	Enrutador	Cisco ISR 4321 Router	9	2	45w	899.00	8,991.00
und	Servidor	HPE ProLiant DL380 Gen10	14	2	800w	8,999.00	125,986.00
und	Switch	Cisco Catalyst 2960X-48TS-L 48-Port PoE	7	1	15.5w	2,399.00	16,793.00
und	Switch	Cisco Catalyst 2960X-24PS-L 24-Port PoE	3	1	15.5w	1,799.00	5,397.00
und	Firewall	Cisco ASA 5525-X Firewall	2	1	50w	1,295.00	3,885.00

und	Impresora	Brother MFC-L8900CDW Todo en uno	3	1	640w	699.00	2,796.00
und	PC	Dell OptiPlex 5090 Tower	126	10	150w	749.99	104,998.74
und	Monitor	Dell P2722H 27" Full HD	136	10	25w	259.99	36,838.64
und	Teclado	Logitech K845 Mechanical Keyboard	136	10	2w	59.99	8,398.64
und	Mouse	Logitech M510 Wireless	136	10	1.5w	39.99	5,758.64
und	Rack	Tripp Lite SR42UB SmartRack 42U	7	1	—	1,299.99	9,099.93
und	Cámara	Ubiquiti UniFi Protect G4	40	5	—	129.99	5,199.60
und	Control de Acceso	ZKTeco F18 Biometric Access Control	9	1	5w	399.99	3,999.90

und	Panel de Alarma	Honeywell VISTA-128BPT Panel de Alarma	4	1	10w	249.99	999.96
und	Detector de Humo	Kidde i4618AC Smoke Detector	10	2	1w	19.99	199.90
und	Inversor	Wagan EL3748 ProLine 10000W	1	1	—	1,399.00	1,399.00
und	Extintor	Amerex B500 Multi-purpose Fire Extinguisher	10	1	—	149.99	1,499.90
Total estimado:							$342,139.95

1. **Enrutadores:** Se seleccionaron Cisco ISR 4321 por su capacidad de manejar tráfico de red de manera eficiente y por ofrecer una conexión segura y robusta. Estos enrutadores son ideales para el entorno de red de un edificio de gran tamaño, ya que permiten administrar grandes volúmenes de tráfico entre diferentes VLANs y ofrecen conectividad estable.
2. **Servidores:** Los servidores HPE ProLiant DL380 Gen10 fueron elegidos por su alto rendimiento y confiabilidad. Estos servidores están optimizados para manejar grandes cantidades de datos y procesos simultáneos, lo que es esencial para soportar la carga de trabajo de los desarrolladores y los servicios críticos, como los servidores de producción, QA y backup.

3. **Switches:** Los Cisco Catalyst 2960X soportan PoE (Power over Ethernet), lo que permite alimentar dispositivos como cámaras de vigilancia y puntos de acceso a través del cable de red, eliminando la necesidad de cables de alimentación separados. Además, estos switches están diseñados para manejar grandes volúmenes de tráfico de red, lo que es fundamental para garantizar la conectividad en todas las áreas del edificio.
4. **Firewalls:** Se ha optado por los Cisco ASA 5525-X, que brindan un nivel avanzado de seguridad para la red. Estos firewalls permiten establecer políticas de seguridad, gestionar accesos y proteger las áreas críticas del sistema de posibles amenazas, lo que es crucial para proteger la información sensible en la infraestructura.
5. **PCs y Monitores**: Los Dell OptiPlex 5090 Tower junto con los monitores Dell P2722H son ideales para proporcionar a los empleados equipos confiables y de alto rendimiento. Los PCs están equipados con suficiente capacidad de procesamiento para manejar las tareas diarias, mientras que los monitores proporcionan una resolución Full HD, optimizando la experiencia de usuario.
6. **Control de Acceso:** Se ha implementado un sistema biométrico con ZKTeco F18, que proporciona control de acceso seguro en las áreas críticas del edificio. Esto garantiza que solo el personal autorizado pueda acceder a ciertas zonas, fortaleciendo la seguridad física de la instalación.

Consideraciones Adicionales:

No se han incluido en la estimación los costos asociados con las licencias de software, como los sistemas operativos necesarios para servidores y estaciones de trabajo, aplicaciones empresariales o software de seguridad (antivirus, firewalls de software, entre otros). Además, los costos de instalación y configuración de los equipos, el cableado estructurado y la mano de obra no se consideran en este análisis.

Asimismo, es importante tener en cuenta los costos futuros de mantenimiento preventivo, actualizaciones de software y reemplazo de hardware. Esto incluye la contratación de personal técnico para el monitoreo continuo de la red, así como los gastos relacionados con la renovación de licencias y los planes de respaldo de datos.

Cálculo de ancho de banda para 10.000.000 clientes conectados a los servidores de producción

En base a los requerimientos del proyecto, hemos realizado un análisis detallado del ancho de banda necesario para soportar la carga de hasta 10 millones de usuarios conectados simultáneamente a los servidores de producción. Este cálculo tiene en cuenta la estructura de la red del edificio de 20 pisos, con áreas diferenciadas, y está diseñado para asegurar un rendimiento óptimo.

Para garantizar precisión en el cálculo del ancho de banda, hemos considerado la estructura de tres tablas clave en su base de datos PostgreSQL:

- Tabla Usuario: Contiene información personal de cada usuario, como nombre y correo.
- Tabla Cuenta: Registra los IDs de las cuentas asociadas a cada usuario.
- Tabla Transacción: Almacena las transacciones, incluyendo el ID, la fecha y el monto de cada operación.

Cada consulta que un usuario realiza a los servidores genera los siguientes datos:

- Datos del usuario: 716 bytes
- Datos de la cuenta: 4 bytes
- Datos de las transacciones (20 por consulta): 240 bytes
- Total, por usuario: 960 bytes

Cálculo para 10 Millones de Usuarios:

Para satisfacer las demandas de tráfico y asegurar la disponibilidad continua de la plataforma bancaria a hasta 10 millones de usuarios simultáneos, se realizó un análisis exhaustivo del ancho de banda requerido. A continuación, se presenta cada etapa del cálculo y la distribución estratégica del ancho de banda para cada área.

Tamaño Total de Datos Generado por los Usuarios

Cada usuario conectado genera un promedio de 960 bytes por consulta. Multiplicando esta cifra por los 10 millones de usuarios simultáneos, obtenemos el tamaño total de datos necesario para gestionar el tráfico:

$$\text{Total} = 10{,}000{,}000 \text{ usuarios} \times 960 \text{ bytes} = 9{,}600{,}000{,}000 \text{ bytes} \approx 9.6 \text{ GB}$$

Aplicación de Margen de Seguridad

Para manejar aumentos en el tráfico y picos en el uso, se aplica un margen de seguridad del 10%, que garantiza que la red soporte incrementos inesperados sin afectar el rendimiento:

$$\text{Tamaño con Holgura} = 9.6 \text{ GB} \times 1.1 = 10.56 \text{ GB}$$

Cálculo del Ancho de Banda Requerido

Convertimos el tamaño total de datos (incluyendo holgura) a bits para calcular el ancho de banda necesario para transmitir estos datos en tiempo real:

$$\text{Ancho de Banda} = 10.56 \text{ GB} \times 8 = 84.48 \text{ Gbps}$$

Este ancho de banda de 84.48 Gbps es necesario exclusivamente para los servidores de producción que gestionan las consultas simultáneas de los usuarios de la plataforma bancaria, garantizando una experiencia fluida y de alta disponibilidad.

Distribución Estratégica del Ancho de Banda en el Edificio

Para asegurar que cada departamento cuente con los recursos necesarios, se asignó ancho de banda en función de las actividades y requisitos específicos de cada área:

- **Desarrolladores: 1 Gbps**
  Los desarrolladores requieren un ancho de banda amplio para tareas intensivas de red como pruebas en tiempo real, sincronización de código y transferencia de archivos de gran tamaño. Esta asignación permite a los desarrolladores trabajar sin interrupciones, garantizando una conectividad rápida y estable para proyectos críticos y pruebas continuas en la red interna.
- **Administración y jefes de Área: 0.6 Gbps**
  Este equipo necesita un acceso fluido a sistemas de gestión de datos, reportes y documentos compartidos para la toma de decisiones. La asignación de 0.6 Gbps asegura que puedan trabajar de manera eficiente y sin interrupciones al acceder a bases de datos internas y aplicaciones de gestión administrativa.
- **Gerencia: 1 Gbps**
  La gerencia requiere un ancho de banda elevado para videoconferencias de alta

calidad, análisis de grandes volúmenes de datos y acceso a aplicaciones de planificación y evaluación. Esta asignación garantiza que puedan operar sin restricciones y mantener una comunicación clara y sin latencias durante reuniones y presentaciones estratégicas.

- **Desktop Services: 0.2 Gbps**

  Los servicios de soporte a equipos de escritorio necesitan un ancho de banda moderado para brindar mantenimiento remoto, actualizaciones de software y asistencia técnica en toda la red. 0.2 Gbps es suficiente para sus actividades, asegurando la conectividad necesaria para mantener operativos los equipos de los usuarios finales.

- **Asesores de Software: 0.3 Gbps**

  Los asesores de software requieren un ancho de banda dedicado para brindar soporte técnico avanzado, realizar diagnósticos en tiempo real y acceder a bases de datos de documentación y asistencia. Con 0.3 Gbps, pueden responder de manera ágil a las solicitudes de soporte y asistencia, asegurando una resolución rápida y eficiente.

- **Recepción y Áreas Comunes: 0.15 Gbps**

  En estas áreas se necesita un ancho de banda menor, adecuado para tareas de comunicación básicas, gestión de visitantes y sistemas de mensajería. 0.15 Gbps permite un funcionamiento suficiente para las actividades de soporte y servicio, sin afectar el rendimiento de las áreas críticas.

- **Servidores de Producción: 84.48 Gbps**

  Dado el tráfico generado por la plataforma bancaria, estos servidores requieren la mayor asignación de ancho de banda. Los 84.48 Gbps garantizan que las interacciones simultáneas de millones de usuarios se gestionen sin interrupciones y con una latencia mínima, asegurando la disponibilidad de los servicios en todo momento.

- **Otros Servidores (Backup, Almacenamiento, etc.): 2 Gbps**

  Otros servidores, como los de almacenamiento y respaldo, requieren un ancho de banda adecuado para realizar copias de seguridad automáticas y sincronizaciones de datos. Los 2 Gbps asignados permiten que estas tareas de respaldo se realicen de manera constante y sin afectar los servicios críticos, garantizando así la continuidad y seguridad de los datos.

Ancho de Banda Total

Sumando las necesidades de cada área, el ancho de banda total requerido para el edificio es:

$$\text{Ancho de Banda Total} = 1+0.6+1+0.2+0.3+0.15+84.48+2 = 89.73 \text{ Gbps}$$

Para asegurar el rendimiento óptimo y la estabilidad de la infraestructura de red, se recomienda que la infraestructura del edificio esté preparada para un ancho de banda total de 89.73 Gbps. Esto cubrirá las necesidades actuales y permitirá una operación fluida en todas las áreas y servicios del edificio.

Límite de Ancho de Banda por Área

Para una gestión eficaz y controlada de los recursos de red, se establece un límite de ancho de banda específico para cada área. Esto optimiza el rendimiento y permite la priorización de servicios críticos. La siguiente tabla detalla los límites de ancho de banda asignados a cada área:

Área	**Ancho de banda (Mbps)**
Desarrolladores	1000
Desktop Services	200
Asesores de software	300
Servidores	2000
Administradores	600
Gerencia	1000

CONCLUSION

El diseño de la infraestructura de red para el edificio de 20 pisos expuesto en este proyecto refleja una planificación meticulosa que tiene como objetivo no solo satisfacer las necesidades actuales, sino también proveer escalabilidad y flexibilidad para el futuro. La arquitectura implementada, que incluye la segmentación de la red mediante VLANs, el uso de firewalls y controles de acceso estrictos, y la integración con herramientas de Microsoft, asegura un entorno seguro, eficiente y adaptable a las demandas cambiantes de la organización.

El enfoque integral adoptado cubre tanto aspectos técnicos como de seguridad, lo cual es crucial en un entorno donde se manejan grandes volúmenes de datos confidenciales. La implementación de zonas desmilitarizadas y militarizadas (DMZ y MZ) para aislar los servidores más críticos, así como la distribución inteligente de la red con subredes específicas para cada departamento, aseguran que el acceso a los recursos esté controlado y supervisado de manera efectiva.

Uno de los puntos más destacados del proyecto es el cálculo del ancho de banda requerido para manejar hasta 10 millones de usuarios simultáneos, lo que asegura un rendimiento óptimo y prepara la infraestructura para soportar picos de tráfico sin comprometer la estabilidad del sistema. Además, la inclusión de mecanismos de respaldo de energía, ventilación adecuada, y sistemas de detección y extinción de incendios demuestran el compromiso con la continuidad operativa y la protección de los activos críticos.

El análisis detallado de los costos proporciona una visión clara de la inversión necesaria, tanto en hardware como en recursos adicionales, como personal de instalación y mantenimiento. Si bien el proyecto excluye ciertos costos, como licencias de software o gastos de mantenimiento a largo plazo, estas consideraciones están claramente especificadas, lo que permite una planificación financiera más precisa.