UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA

FACULTAD DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

PROYECTO EXAMEN GENERAL PRIVADO

ÁREA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

0907-16-10278

Josué Isael Bonilla Matías

GUATEMALA OCTUBRE 2021

INDICE

INTRODUCCIÓN

Es innegable que en la actualidad hasta la empresa más pequeña necesita de la implementación de una red que le permita trabajar de forma que pueda mejorar sus procedimientos, atenciones con los clientes, entre otras cosas más, aunque las razones de hacer este tipo de implementaciones no sólo se quedan en eso, puesto que al seguir ciertas normas y buenas prácticas, podemos lograr formar una estructura que sea capaz de implementar ciertos planes de seguridad que protejan la integridad de la información, agilizar procesos, permitir alta disponibilidad de los sistemas, estableces conexiones con áreas geográficamente distantes, entre muchas otras cosas más.

Estas Razones hacen que el enfoque de este proyecto esté orientado a ofrecer soluciones que puedan soportar un crecimiento de la Compañía Alimentos Buena Vida, siguiendo ciertas normativas que van a permitirles mantener seguridad, disponibilidad, planes de recuperación y administración de las redes.

Esta investigación tiene el objetivo de que dicha compañía sea capaz de crecer sin que sus procesos se vean afectados y sin que la seguridad de la información se vea comprometida ante las amenazas que se puedan presentar.

OBJETIVOS

GENERAL

Proveer de una estructura de red que permita el crecimiento de la compañía sin problemas, que provea de seguridad en la red ante las amenazas y permita hacer una recuperación total o parcial de pérdidas que se puedan dar ante una amenaza que pueda dañar o penetrar la seguridad de la red.

ESPECÍFICOS

1. Crear un diseño de red.
2. Implementar medidas de seguridad como planes de contingencia, de seguridad y de recuperación.
3. Permitir que las sucursales estén conectadas con la central de la compañía sin importar la distancia geográfica.

CAPITULO I - PROPUESTA COMERCIAL

DISEÑO DE RED

El diseño de la red se realizará por medio de la topología árbol, la cual combina características de la topología de estrella con la de bus, pero la principal razón de escoger esta topología es gracias a que permite un fácil crecimiento de la red en la medida de lo necesario.

CONEXIÓN CON ÁREAS GEOGRÁFICAMENTE DISTANTES

Para ofrecer una comunicación tanto con la central (matriz), las sucursales y los vendedores ruteros, se recomienda utilizar una red LAN por medio de una VPN, para que, en el caso de los vendedores ruteros, puedan acceder a la red de la empresa sin necesidad de estar conectados a la misma red física.

Antes de todo, es necesario implementar políticas de seguridad para regular la manera en que se realizarán y utilizarán las conexiones a través de la VPN, por ejemplo, la codificación de datos, para que estos no sean visibles por clientes no autorizados en la red. Otros puntos que también son necesarios o deseable para implementar de mejor manera una VPN son los siguientes:

- Un servidor de acceso y autenticación, para que se tenga un control de los usuarios que ingresan, verificar su identidad y tener un registro sobre sus accesos.
- Un servicio de VPN, en este caso tomaremos ZeroTier, mismo que de forma gratuita ofrece un servicio básico con una conexión de hasta 50 usuarios y un servicio profesional con un costo de $49/mes que soporta hasta 500 conexiones.

- El sistema operativo que se usará en las computadoras será un poco indiferente, siempre y cuando sea compatible con la VPN, en este caso los deseables serían: Windows, MacOS, Linux y Android e IOS (En caso de móviles).
- Las conexiones que se deben realizar en cuanto a la red LAN local, se realizarán por medio de conexiones ethernet, para tener una mejor conexión sobre la red y así un mejor tiempo de respuesta con la VPN.

ASIGNACIÓN DE DIRECCIONES IP PARA EL DISEÑO

Debido a que el problema no especifica la cantidad de sedes que posee la empresa, tomaremos como ejemplo tres, donde una será la sede matriz, y las otras dos serán las sucursales. La ubicación de estas tres sedes será la siguiente: La sede matriz se encontrará en el departamento de Guatemala, otra se ubicará en el departamento de Jalapa y la última en el departamento de Petén.

Actualmente tanto la sede matriz como las sucursales distribuidas por Guatemala se encuentran distribuidas de la siguiente manera:

Sede matriz			
Oficinas	Equipos		Tipo de comunicación
	Tipo	Cantidad	
Data center	Switch	3	RED LAN
	Router	1	
Gerencia	Computadoras	10	
Ventas	Computadoras/Vendedores Ruteros	9	
RRHH	Computadoras	8	

Sucursales			
Oficinas	Equipos		Tipo de comunicación
	Tipo	Cantidad	
Data center	Switch	3	RED LAN
	Router	1	
Gerencia	Computadoras	10	
Ventas	Computadoras/Vendedores Ruteros	9	
RRHH	Computadoras	8	

Cada una de las redes de cada sucursal se dividirá en 4 subredes (VLAN), una se utilizará para el cuarto de servidores de cada sede y los routers que transmitirán la información a las demás sedes. Al dividir la red en 4 estamos evitando al máximo que se pueda desperdiciar la red y a la vez que nos permita implementar más equipos en cada oficina a largo plazo, así mismo, al utilizar 4 VLAN evitamos que la información de cada oficina se cruce de forma innecesaria. También se opta por la conexión entre un router principal y uno de respaldo, mismos que se manejarán con un subneting diferente para que cada una de las redes pueda conocer una conexión alterna en caso de que una de las dos falle.

Para realizar el subneteo de la red se utiliza la fórmula 2^n-2 para mayor amplitud de equipos en la red de cada sede en este caso la formula quedaría (2^3-2 > 4) y nuestra mascara quedaría /27 debido a que nuestra mascara en un principio era (24+3(Numero de bits utilizados para obtener nuestras 4 subredes=27), el rango asignable para cada subred quedaría de 30 equipos, los hosts necesarios para en un futuro poder implementar equipos en cada área.

Guatemala					
Subred	Rango de Host Validos	Broadcast	Máscara de Subred	Número de Host Por cada VLAN	VLAN
192.168.2.0	192.168.2.1 - 192.168.2.30	192.168.2.31	255.255.255.224	30	Cuarto de Servidores
192.168.2.32	192.168.2.33 - 192.168.2.62	192.168.2.63			10 Gerencia
192.168.2.64	192.168.2.65 - 192.168.2.94	192.168.2.95			20 Ventas
192.168.2.96	192.168.2.97 - 192.168.2.126	192.168.2.127			30 RRHH
Jalapa					
Subred	Rango de Host Validos	Broadcast	Máscara de Subred	Número de Host Por cada VLAN	VLAN
192.168.3.0	192.168.3.1 - 192.168.3.30	192.168.3.31	255.255.255.224	30	Cuarto de Servidores
192.168.3.32	192.168.3.33 - 192.168.3.62	192.168.3.63			10 Gerencia
192.168.3.64	192.168.3.65 - 192.168.3.94	192.168.3.95			20 Ventas
192.168.3.96	192.168.3.66 - 192.168.3.126	192.168.3.127			30 RRHH
Petén					
Subred	Rango de Host Validos	Broadcast	Máscara de Subred	Número de Host Por cada VLAN	VLAN
192.168.8.0	192.168.8.1 - 192.168.8.30	192.168.8.31	255.255.255.224	30	Cuarto de Servidores
192.168.8.32	192.168.8.33 - 192.168.8.62	192.168.8.63			10 Gerencia
192.168.8.64	192.168.8.65 - 192.168.8.94	192.168.8.95			20 Ventas
192.168.8.96	192.168.8.66 - 192.168.8.126	192.168.8.127			30 RRHH

Para evitar la asignación manual de IPs dentro de la red de cada una de las sucursales se implementará un servidor DHCP el cual brindará el direccionamiento IP de las 3 oficinas de cada sucursal.

PROTOCOLOS A UTILIZAR EN EL DISEÑO DE RED QUE HA DECIDIDO IMPLEMENTAR

Para la red que se implementará, se decidió incluir los siguientes protocolos, mismos que proveerán de los servicios necesarios para la empresa. El primero de ellos es el HTTP que se utiliza para acceder a las páginas web, ARP para la resolución de direcciones, FTP para proveer la transferencia de archivos, SMTP y

POP que son muy importantes en este caso para el manejo de correos electrónicos. Sin duda alguna también estará incluido el protocolo TCP/IP, ya que este es la base de todo el internet.

MATRIZ DE RIESGOS

Categoría	Riesgos	Descripción
Administrativo	Perdida de personal clave.	Salida de personas necesarias para operar y mantener los equipos.
	Perdidas en facturación por equipo clave que no esté operando.	Si los servidores no están funcionando, la empresa no puede cobrar las horas no trabajadas
	Crecimiento del personal de la empresa	Necesidad de comprar más servidores por aumento en el uso, con más personal
Técnicos	Desperfecto de equipo por manejo inadecuado.	A la hora de operar los equipos, se pueden utilizar de forma inadecuada, provocando un daño.
	Falta de mantenimiento preventivo de equipos	Falla por falta de ajustes y limpieza de filtros.
	Riesgos de falla por fallas mecánicas	Los equipos ya llegaron a su vida útil y sus partes pueden fallar.
	Fallas por falta de fluido eléctrico	No hay plantas de emergencia ni UPS.
	Perdida de información de los clientes.	Fallas en el almacenamiento causada por componente dañado.
Operativos	Obsolencia del equipo	Equipos que ya cumplieron su vida útil.
	Accesos no autorizados a los servidores	Vulnerabilidad en el sistema.
	Ausencia de gestión experta (inexperiencia en la tecnología)	Falta de capacitación y experiencia de las personas que operan los equipos.
	Falta de documentación necesaria del proceso	Falta de documentación de los equipos y de los procesos necesarios de gestión, operación e instalación de los equipos.

	Mal dimensionamiento de las capacidades técnicas del equipo	Compra de equipo no acorde a las necesidades del negocio.

Frecuencia de Riesgo	Valores	Descripción
Bajo	1	Más de 1 año
Medio	2	Entre 2 meses y 1 año
Alto	3	Menor a 2 meses

Categoría	Riesgos	Alto	Medio	Bajo
Administrativo	Perdida de personal clave.			1
	Perdidas en facturación por equipo clave que no esté operando.			1
	Crecimiento del personal de la empresa		2	
Técnicos	Desperfecto de equipo por manejo inadecuado.		2	
	Falta de mantenimiento preventivo de equipos			1
	Riesgos de falla por fallas mecánicas		2	
	Fallas por falta de fluido eléctrico			1
	Perdida de información de los clientes.		2	
Operativos	Obsolencia del equipo		2	
	Accesos no autorizados a los servidores			1
	Ausencia de gestión experta (inexperiencia en la tecnología)			1
	Falta de documentación necesaria del proceso			1
	Mal dimensionamiento de las capacidades técnicas del equipo			1

Impacto del Riesgo	Valores	Descripción
Bajo	1	Impacto mínimo sobre costo, tiempo o técnico
Medio	2	Algún impacto sobre costo, tiempo o técnico
Alto	3	Impacto sustancial sobre costo, tiempo o técnico

Categoría	Riesgos	Alto	Medio	Bajo
Administrativo	Perdida de personal clave.			1
	Perdidas en facturación por equipo clave que no esté operando.			1
	Crecimiento del personal de la empresa		2	
Técnicos	Desperfecto de equipo por manejo inadecuado.	3		
	Falta de mantenimiento preventivo de equipos			1
	Riesgos de falla por fallas mecánicas	3		
	Fallas por falta de fluido eléctrico			1
	Perdida de información de los clientes.	3		
Operativos	Obsolencia del equipo	3		
	Accesos no autorizados a los servidores		2	
	Ausencia de gestión experta (inexperiencia en la tecnología)			1
	Falta de documentación necesaria del proceso			1
	Mal dimensionamiento de las capacidades técnicas del equipo			1

Nivel de Riesgo	Valores
Bajo	1-2
Medio	3-4
Alto	5-6

Análisis de Riesgos				
Categoría	**Riesgos**	**Alto**	**Medio**	**Bajo**
Administrativo	Perdida de personal clave.			2
	Perdidas en facturación por equipo clave que no esté operando.			2
	Crecimiento del personal de la empresa			2
Técnicos	Desperfecto de equipo por manejo inadecuado.	5		
	Falta de mantenimiento preventivo de equipos			2
	Riesgos de falla por fallas mecánicas	5		
	Fallas por falta de fluido eléctrico		3	
	Perdida de información de los clientes.	5		
Operativos	Obsolencia del equipo	5		
	Accesos no autorizados a los servidores		3	
	Ausencia de gestión experta (inexperiencia en la tecnología)			1
	Falta de documentación necesaria del proceso			1
	Mal dimensionamiento de las capacidades técnicas del equipo			1

PLAN DE CONTINGENCIA

OBJETIVO:

Mantener la continuidad de los sistemas de información frente a los eventos críticos, de su entidad y minimizar el impacto negativo sobre la misma.

ACCIONES A REALIZAR

SEGURIDAD FÍSICA:

La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de un sistema de información de datos, en este caso, la implementación de UPS para evitar daños en los equipos al momento de ocurrir una baja de energía eléctrica e implementación de un sistema contra incendios para evitar la pérdida de los activos.

SEGURIDAD LÓGICA:

La seguridad lógica permite proteger la integridad de los datos almacenados en un sistema informáticos. En este caso se recomienda mantener los antivirus actualizados, poseer un firewall para protegerse de los accesos no deseados que puedan ocurrir para el robo de información.

SEGURIDAD DEL EDIFICIO:

Preparar extinguidores, organizar las señales de evacuación, preparar bombas de extracción de agua, generadores eléctricos, etc.

TOPOLOGÍA DE RED:

Preparar planos de la topología, tener equipos de repuestos de la red, herramientas necesarias todo esto en lugar de fácil acceso.

COPIAS DE SEGURIDAD:

De forma periódica la información, es decir la base de datos de la empresa, es copia en un disco extraíble o en la nube. Esto permite salvar la información, en caso de ruptura parcial o total, de uno o ambos servidores, o de la propia base de datos. La restauración de la información, disminuye los tiempos de inactividad, en caso de rupturas parciales o totales de uno o ambos servidores o de las bases de datos.

RECOMENDACIONES

- Se recomienda brindar un mantenimiento de forma periódica a este plan.
- Se recomiendan capacitaciones al personal de informática en relación a seguridad informática y a la utilización de los sistemas y equipo físico, con el fin de implementar nuevas estrategias en dicho plan.
- Se recomienda la evaluación de otro tipo de tecnologías para realizar respaldos de forma eficiente y eficaz.
- Contar con una planta de emergencia que suministre energía regulada a todos los equipos.
- Implementar un plan de mantenimiento periódico con supervisiones.
- Contar con equipo de emergencia contra incendios como extintores.
- Contar con un procedimiento de operación y uno en caso de un mal funcionamiento.
- Contar con tierras físicas independientes a los servicios de telecomunicaciones.

- Contar con un UPS con capacidades necesarias (40% superiores)en todos los equipos.
- Determinar semestralmente el tiempo efectivo y real de respaldo del UPS con respecto a las diferentes cargas.
- Contar con procedimiento de ejecución de respaldos de emergencia a la información del servidor Web, DNS, configuraciones de Equipo Activo principales y centrales.
- Solicitar revisión periódica (semestral) del estado y óptimo funcionamiento de los bancos de respaldo eléctrico en los equipos del proveedor de medios.

PLAN DE SEGURIDAD

POLÍTICAS PARA LA SEGURIDAD FÍSICA

- No se deben mover los equipos físicos sin autorización previa.
- No comer alimentos ni ingerir bebidas mientras se utiliza el equipo.
- Se deberán reportar daños físicos o de softwares al departamento de TI.

POLÍTICAS PARA EL USO DE LAS COMPUTADORAS CORPORATIVAS

- Será únicamente para uso exclusivo de la empresa.
- Personas ajenas a la empresa no tendrán accesos al uso de las computadoras.
- No compartir ningún tipo de información sin autorización previa.

POLÍTICAS PARA EL USO CORRECTO DE LAS CONTRASEÑAS CORPORATIVAS

- No se deben escribir de manera física.
- No compartirlas con personas ajenas a la empresa ni compañeros de trabajo.
- Al ingresar por primera vez deberá cambiar la contraseña cumpliendo con los siguientes requisitos:
    - ✓ utilizar mayúsculas y minúsculas
    - ✓ símbolos
    - ✓ letras y números
    - ✓ mínimo 8 caracteres.

CONTROLES CRITICOS DE SEGURIDAD EN LA RED

Se pretende aplicar ciertos controles críticos de seguridad en la red para proteger los activos críticos, la infraestructura y la organización mediante una protección continua y automatizada.

PROTECCIÓN ANTI-MALWARE

Esta es necesario aplicarla debido a que es muy fácil que hoy en día los equipos puedan infectarse por malwares que puedan poner en riesgo la integridad de la información y los sistemas empresariales de nuestra empresa, debido a esto es necesario que cada uno de los equipos activos de la organización posea una protección anti-malware por medio de un software dedicado.

CAPACIDAD DE RECUPERACIÓN DE DATOS

Para protección de los datos y no perderlos, serán necesarias ciertas acciones de suma importancia, tales como:

IMPLEMENTACIÓN DE COPIAS DE SEGURIDAD EN LA BASE DE DATOS

Dentro de esta medida es necesario configurar el gestor de bases de datos a manera que realice copias de seguridad automáticas cada cierto tiempo. Para esto se recomienda la configuración de copias de seguridad diferenciales diarias cada final de jornada y una copia de seguridad completa los días miércoles y viernes al final de la jornada.

IMPLEMENTACIÓN DE BASES DE DATOS EN LA NUBE

Contar con un servicio de bases de datos en la nube ayuda mucho a la recuperación de datos en una organización, debido a que si un sistema o un equipo falla dentro de la empresa, no se sufrirá perdida de información debido a que esta estará almacenada en la nube y podremos acceder a ella en cualquier momento. Además dependiendo del servicio contratado, se puede proteger la información teniendo la misma en más de un servidor que esté en diferentes ubicaciones geográficas.

PROTECCIÓN DE DATOS

Junto con el punto anterior, la protección de los datos es un punto de mucha importancia, aunque este no depende de las mismas recomendaciones, debido a que existen distintas formas para la protección de datos, desde la implementación de políticas dentro de la organización que permitan regular el manejo de la información, controlar los accesos a los sistemas y designar niveles de jerarquía

para que no todos los usuarios tengan acceso a toda la información o la implementación de RAID's.

IMPLEMENTACIÓN DE UNA RAID

Una RAID es una matriz de redundante de discos independientes, mismos que ayudan a distribuir la información en cada disco o a realizar réplicas de la misma para que siempre exista un respaldo en caso de que una de las unidades de almacenamiento sufra desperfectos. Dependiendo de las necesidades de la empresa, existen diferentes tipos de RAID que ofrecen diferentes formas de almacenar la información. Para obtener una buena tolerancia a fallos, se recomiendo la aplicación de una RAID 1, que nos permite duplicar la información en dos discos duros o dos conjuntos de discos duros, permitiendo que al momento de almacenar un dato, este se replica inmediatamente en la unidad espejo para así tener dos veces el mismo dato. Esto no quiere decir que dentro de los sistemas la información se vaya a ver afectada o que nos aparecerá duplicada, sino que esto lo que hace es que al momento en que falle una de las unidades, el sistema no dejará de mostrarnos la información, simplemente la buscará en la unidad espejo de la que falló, previniendo así la pérdida total o parcial de la información.

CONTROL DE ACCESO INALÁMBRICO

Implementar medidas de control para los accesos inalámbricos es muy importante, debido a que los accesos desde fuera de la organización puede ser un problema muy preocupante, porque pueden modificar los datos o alterar los sistemas. Pero para evitar este tipo de problemas se pueden generar usuarios dentro de la red, para que únicamente se pueda acceder tanto a la red como a los sistemas por medio

de un ingreso de usuario y contraseña previamente autorizados por los administradores.

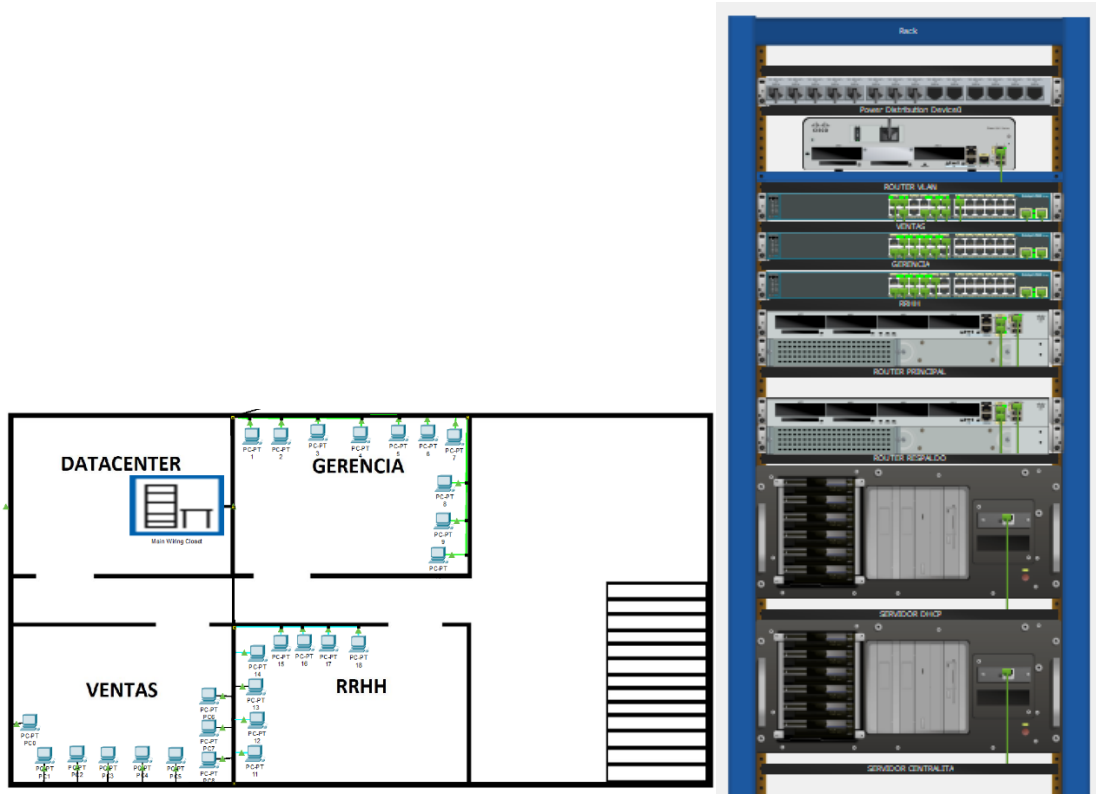
MONITOREO Y CONTROL DE CUENTAS

El monitoreo y control de cuentas nos permite tener un control de los usuarios que acceden a las redes y sistemas empresariales, conociendo los días en que accedieron, el tiempo de sesión y las acciones que realizaron, logrando de esta forma mantener los controles necesarios para evitar el filtrado de información por ejemplo.

PLAN DE RECUPERACIÓN DE DESASTRES

- Brindar un tiempo de gracia (dependiendo de la magnitud de la contingencia) para restablecer los equipos activos y servicios.
- Validar el correcto funcionamiento de los equipos activos y servicios.
- Identificar los posibles daños de los equipos activos.
- Evaluar los daños de los equipos activos, planta de emergencia, UPS y canalizarlos a las áreas involucradas.
- Realizar una evaluación de todos los sistemas de la organización y listar las perdidas.
- Realizar una evaluación de las bases de datos y listar las posibles pérdidas.
- Ejecutar los procesos de recuperación de datos en base a los respaldos creados.

CUARTO DE SERVIDORES



PLATAFORMA DE COMUNICACIONES

Por medio de operadores VoIP se pueden adquirir diferentes características y tarifas. Todas las funciones que se pueden obtener son fácilmente personalizables por medio de configuraciones para que las opciones de los clientes se vuelvan más sencillas de alcanzar. Tenemos además una ventaja en cuanto a la conexión con el cliente y los costes de la instalación, cosas que convierten la centralita virtual en una opción mucho más atractiva.

Issabel es una de las opciones más factibles al ser gratuita y además ofrecer una amplia gama de funcionalidades, por esta razón se convierte en el software elegido para la instalación de una centralita virtual en la organización.

CARACTERÍSTICAS DEL SERVIDOR A UTILIZAR

Para iniciar con la centralita virtual necesitaremos de las siguientes características:

- 2GB de RAM.
- 32GB de espacio de disco.
- Una tasa de transferencia de 640 E/S por segundo como mínimo.

TIPO DE SERVIDOR RECOMENDADO

Se recomienda un servidor virtual, para que se pueda tener acceso en cualquier momento y lugar a la centralita. Esto también permite una alta disponibilidad del servicio en la nube.

La plataforma que se recomienda para levantar el servidor, será por medio de una máquina virtual montada sobre Azure, ya que este servicio nos ofrece la posibilidad de ir creciendo conforme se vaya requiriendo, entonces podemos ir aumentando memoria RAM, tamaño de disco y velocidad de transferencia conforme sea necesario.

SOFTWARE DE CENTRALITA RECOMENDADO

Se trata de un software de código abierto de telefonía IP y comunicaciones unificadas basado en Asterisk, y que se utiliza para montar servidores incluyendo correo electrónico, fax, PBX IP, mensajería instantánea, video conferencia, centro de llamadas y funciones colaborativas.

Las numerosas aplicaciones de Issabel hacen de este software una de las más completas herramientas de comunicaciones. Así, no solamente provee de telefonía a la compañía, sino que, además, integra de un modo rápido y eficaz otros canales de comunicación que son imprescindibles hoy en día para el correcto desarrollo de la actividad empresarial.

VoIP PBX: la central telefónica de Issabel cuenta con un amplio número de utilidades entre las que podemos destacar:

- Grabación de llamada
- Identificación de llamadas
- Configuración de callback
- Llamada en espera
- Soporte para videoconferencias
- Sintetización de voz
- Colas de llamadas
- Herramientas para crear lotes de extensiones.
- IVR flexible y configurable
- Identificación de llamadas

- Soporte para configuración de la central de llamadas dependiendo del horario.

LAS PRINCIPALES VENTAJAS DE ISSABEL

El software Issabel es una de las plataformas de comunicaciones más completas existentes en la actualidad, y aporta una serie de importantes beneficios a la empresa. A continuación, destacamos algunos de ellos:

Software gratuito: Issabel es un software de código abierto, que permite su descarga y utilización gratuita. Esto ya de por sí supone una ventaja, pero además, podemos realizar las modificaciones que consideremos oportuno, si tenemos los conocimientos necesarios para ello. Así, el nivel de personalización es muy flexible, dependiendo de las necesidades concretas de la empresa en cada momento.

PLAN PARA AGREGAR TELÉFONOS ADICIONALES

Por la forma en cómo funciona Issabel, el mejor plan para agregar los teléfonos en base a lo requerido, que es iniciar con 25 teléfonos e ir agregando 25 más cada cuatrimestre hasta llegar a 100 teléfonos, se recomienda agregar los 100 perfiles de inicio en Issabel e ir activándolos conforme sea necesario cada cuatrimestre. De esta forma logramos ir integrando los teléfonos sin que suceda ningún retraso en este proceso.

COMO UTILIZAR CELULARES EN LA CENTRALITA

La forma de utilizar Issabel en los celulares para que formen parte de la centralita, es por medo de software de Zoiper, mismo que se ejecuta en una multitud

de plataformas diferentes. No importa si está utilizando macOS, Linux o Windows. iOS, Android o un navegador.

Zoiper dispone de una versión gratuita y varias de pago. La versión gratuita de Zoiper para smartphone permite llamar y recibir llamadas.

- **Conferencia**
- **Transferencia de llamada**
- **Encriptación de llamadas**
- **Presencia**
- **Grabación de llamadas**

SOFTWARE RECOMENDADO

SISTEMA OPERATIVO RECOMENDADO PARA CENTRALITA VIRTUAL

CentOS (Community ENTerprise Operating System) es una bifurcación a nivel binario de la distribución GNU/Linux Red Hat Enterprise Linux RHEL, compilado por voluntarios a partir del código fuente publicado por Red Hat, siendo la principal diferencia con este la eliminación de todas las referencias a las marcas y logos propiedad de Red Hat.

Es un sistema operativo de código abierto, basado en la distribución Red Hat Enterprise Linux, operándose de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar. Desde la versión 5, cada lanzamiento recibe soporte

durante diez años, por lo que la actual versión 7 recibirá actualizaciones de seguridad hasta el 30 de junio de 2024.

CentOS en su versión 7.8 es el sistema operativo necesario para poder montar la centralita de virtual, ya que este es el que posee las características necesarias para implementar el software de centralita que se mencionará más adelante en este documento. Necesariamente utilizaremos la versión 7.8 antes mencionada ya que versiones más actuales de este sistema no serán compatibles.

MAPA DE RED

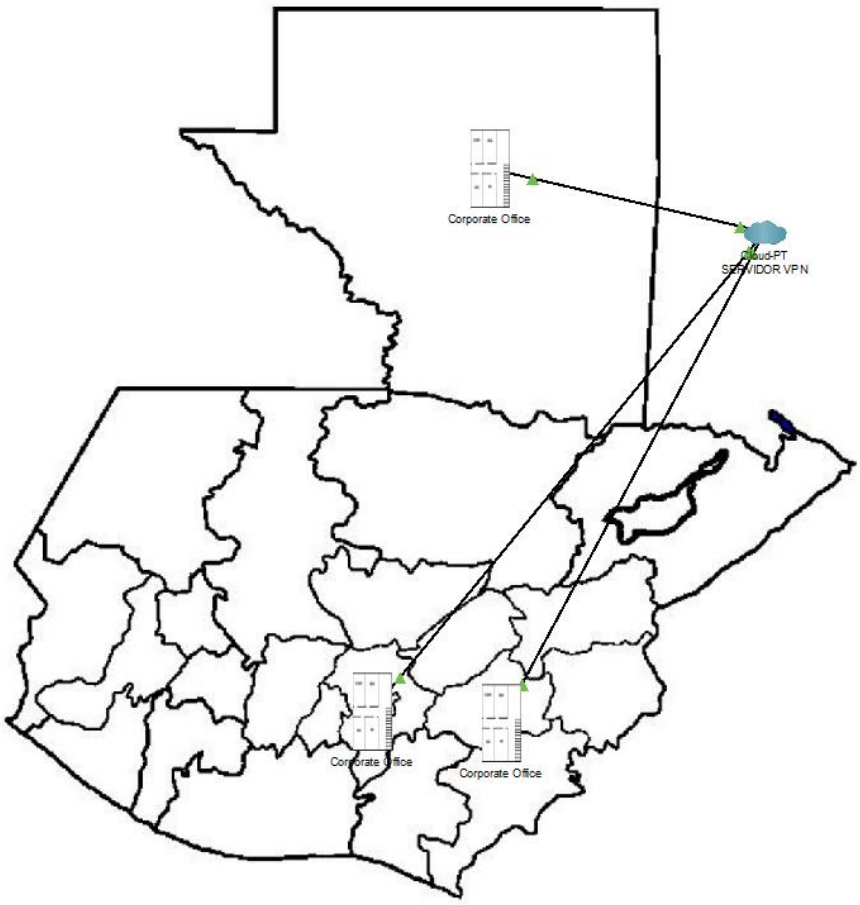
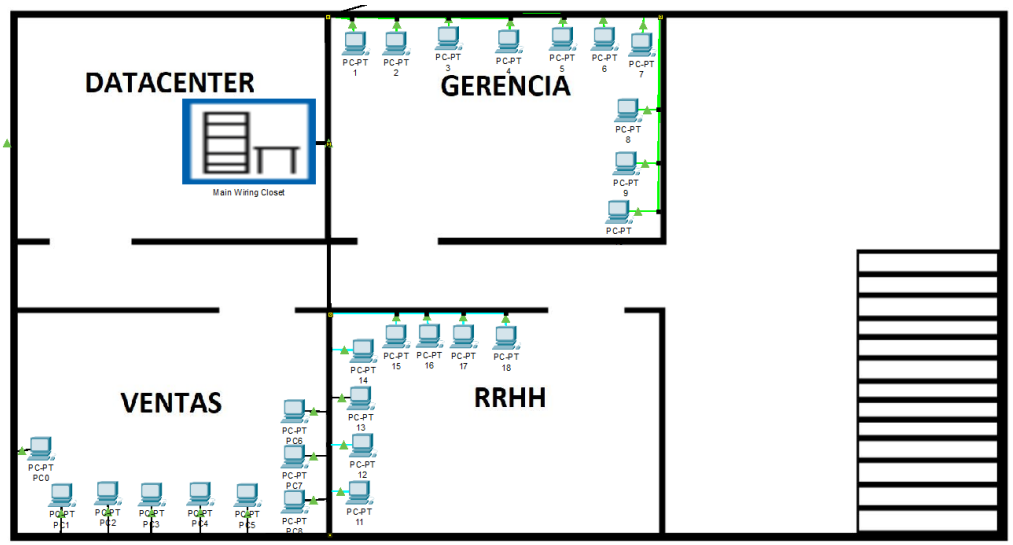
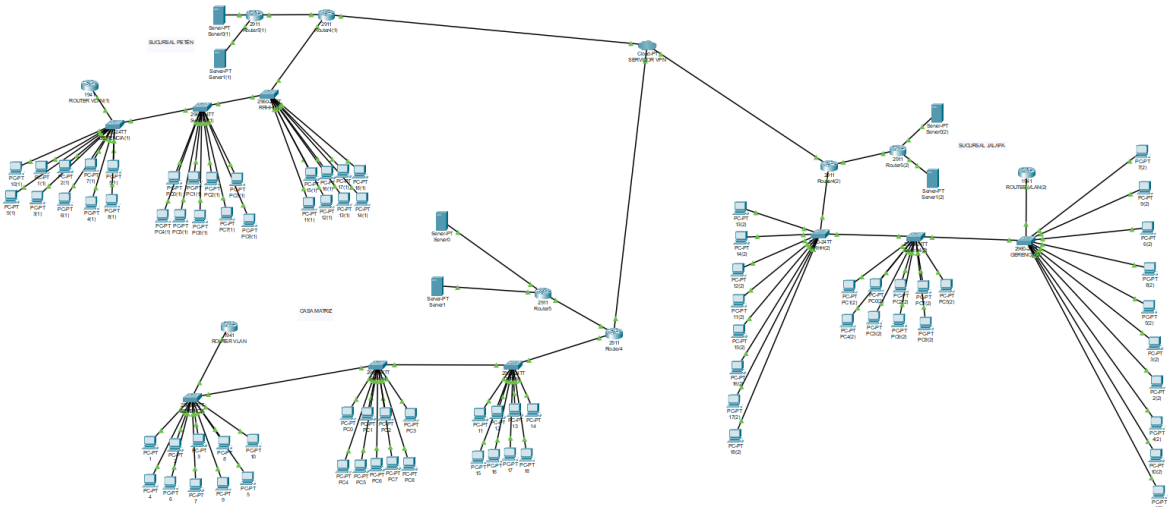


DIAGRAMA DE RED





CAPITULO II - MARCO TEÓRICO

METODOLOGÍA PARA EL DISEÑO DE REDES

Para iniciar con el diseño de una red, es necesario seguir con ciertos pasos que nos ayudarán a identificar de mejor manera la implementación que se necesita, unos de los pasos que debemos seguir son:

a. Recopilar todos los datos y expectativas del usuario.
b. Análisis de requerimientos.
c. Diseño de la capa 1, 2 y 3.
d. Documentación de la implementación física y lógica de la red.

RECOPILAR TODOS LOS DATOS Y EXPECTATIVAS DEL USUARIO.

Una de las cosas más importantes a tomar en cuenta al momento de recopilar datos es sobre las políticas empresariales, procesos críticos y protocolos empresariales para logar un diseño más acertado del requerimiento empresarial. Hay que entender que los 3 grandes factores que afectan directamente la implementación de una red están directamente relacionada con Hardware, Software y Recurso Humano, ya que la interrelación que existe entre estos es la que direcciona el objetivo de la red. También hay que identificar cuáles son las necesidades de hardware, software actual y futuro y si los implementos de red propios cumplen con este objetivo. (PRIETO, 2012)

ANÁLISIS DE REQUERIMIENTOS

Para esta parte la persona que se encarga del diseño de la red debe analizar los requerimientos del usuario para luego acoplarlos con la disponibilidad física de la

red y así encontrar un diseño que esté dentro del alcance de la empresa, tanto económico como tecnológico.

Para tener un control se debe enumerar y asignar prioridades a cada uno de los requerimientos.

DISEÑO DE CAPAS

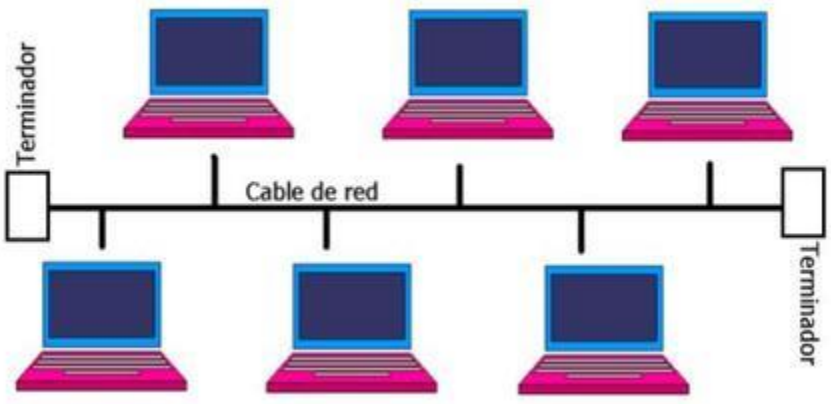
DISEÑO DE LA CAPA 1

En esta capa se realiza el control de como la información es transmitida entre los nodos, por esto el tipo de topología que se utilice definirá la cantidad de información que navegará en la red y la velocidad con la que esta será transmitida.

“La topología física de una red es la disposición geométrica real de las estaciones de trabajo”. (Rouse, 2021) Debemos elegir la topología que consideremos más óptima para nuestra red, para esto tenemos las siguientes:

TOPOLOGÍA DE BUS

En esta topología cada estación está conectada por medio de un cable principal al cual llamamos bus, por tanto, todas las estaciones de trabajo están interconectadas entre sí.

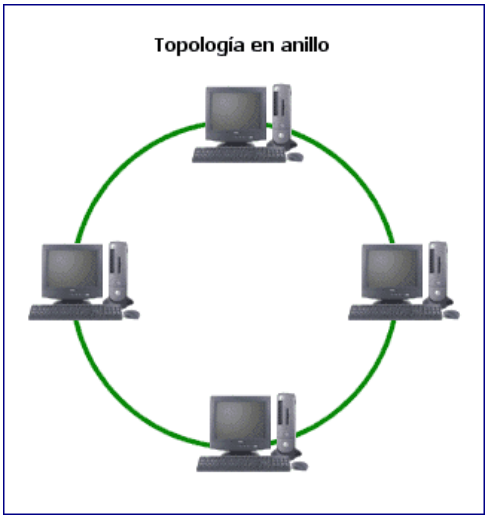


TOPOLOGÍA DE ESTRELLA

En esta existe un servidor central al que todas las máquinas están conectadas directamente y por lo tanto están conectadas entre sí de forma indirecta a través de esta estación central.

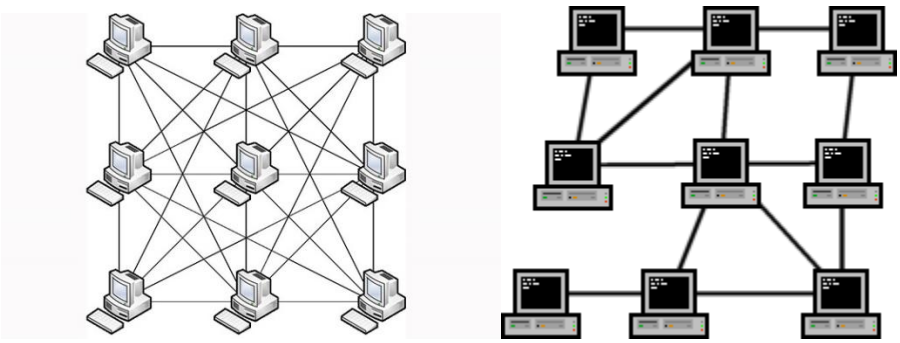
TOPOLOGÍA DE RED EN ANILLO

Esta topología presenta una conexión entre las estaciones de trabajo en forma de bucle, ya que los pares de equipos adyacentes están conectados directamente.



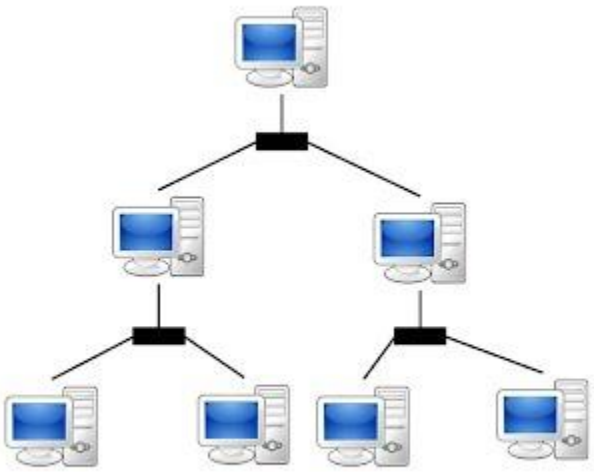
TOPOLOGÍA DE RED DE MALLA

Esta tiene dos esquemas: Malla completa y Malla parcial. Con malla completa cada estación de trabajo está conectada a cada uno de los otros. Con malla parcial, no todas las estaciones de trabajo están conectadas con todas las demás.



TOPOLOGÍA DE RED EN ÁRBOL

Consta de dos o más redes en estrella conectadas entre sí. Los servidores u ordenadores centrales están conectados a un bus principal.



SELECCIÓN DEL CABLEADO

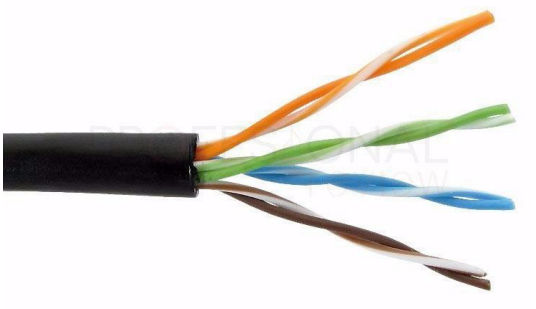
Al seleccionar cuál es el mejor cable para un lugar hay que considerar varios factores:

- Carga de tráfico en la red
- Nivel de seguridad requerida en la red.
- Distancia que debe cubrir el cable
- Opciones disponibles del cable
- Presupuesto para el cable

TIPOS DE CABLES:

CABLE PAR TRENZADO:

Es un tipo de cable en el que hay de 2 a 4 grupos de dos cables de cobre aislados, que tienen 1mm de grosor. En estos cables el trenzado que hay entre los pares sirve para cancelar las ondas de diferentes vueltas, provocando que la radiación del cable sea menos efectiva.



Este cable puede ser utilizado para la transmisión analógica o digital. Además existen diferentes tipos de cable de par trenzado, que puede ir por categorías, en donde la diferencia se marca en el grosor de los cables, blindaje y protección de los mismos, por lo que dependiendo del lugar donde se valla a utilizar, es necesario

escoger una categoría u otra. Las categorías que podemos encontrar son las siguientes:

Categoría	Velocidad	Frecuencia
Ethernet Cat 5e	1.000 Mbps	100 MHz
Ethernet Cat 6	1.000 Mbps	250 MHz
Ethernet Cat 6a	10.000 Mbps	500 MHz
Ethernet Cat 7	10.000 Mbps	600 MHz

CABLE COAXIAL:

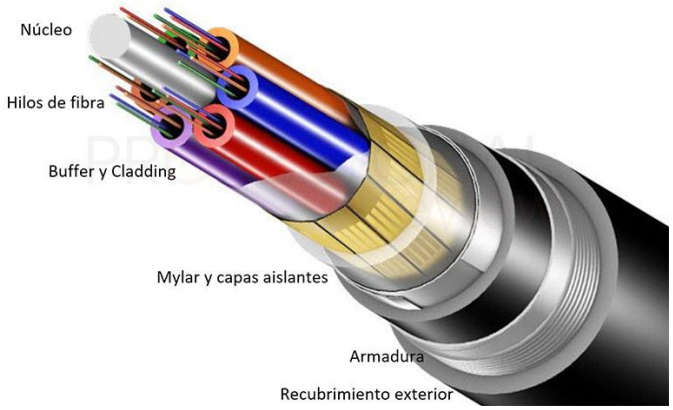
Este cable es capaz de transmitir la señal de manera más rápida debido a que tiene un mejor blindaje que el de par trenzado, lo que también permite que se pueda utilizar en distancias más largas. Se compone de un alambre de cobre rígido como núcleo, que está rodeado en un material aislante, una malla de hilo trenzado y una cubierta exterior.

La forma de instalar estos cables es más complicada que con el cable de par trenzado o UTP, pero se puede realizar conexiones con mayores distancias que con el antes mencionado.

FIBRA ÓPTICA

Con el sistema de transmisión óptica tiene tres componentes: una fuente de luz, el medio de transmisión y un detector. El medio de transmisión consiste en una fibra de vidrio ultra delgada, por medio de la cual al agregar una fuente de luz en un extremo y un detector en el otro, se convierte en un sistema de transmisión unidireccional que acepta una señal eléctrica y se transmite mediante pulsos de luz.

El cable de fibra óptica tiene una similitud con el coaxial, aunque sin la malla de hilo trenzado y permite cubrir distancias mucho más grandes sin tener una pérdida de señal. (GAMEZ, METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES, 2012)



DISEÑO DE LA CAPA 2

En esta se pretende proveer de un control sobre la información, detección de errores y corrección de los mismos, así también, mejorar la gestión de la red mediante dispositivos como routers y switches.

La importancia de esto es por ejemplo con los switches que nos ayudan a la distribución de un correcto ancho de banda por puerto, lo cual permite así un ancho de banda optimizado para el cableado. (GAMEZ, METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES , 2012)

DISEÑO DE LA CAPA 3

A través de este podemos crear segmentos únicos de la red físicos y/o lógicos y permiten la comunicación en los segmentos a través de un direccionamiento IP. Todo esto lo podemos conseguir mediante routers que se encargarán de realizar el enrutamiento de la información por medio de las direcciones IP.

IMPLEMENTACIÓN DE VLAN'S

> Las VLAN pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real en segmentos de redes lógicas. Esta implementación proporciona soporte al estándar de identificación IEEE 802.1Q. (IBM, 2020)

Al implementar las VLAN permitimos que las diferentes áreas de una organización puedan tener su propio segmento de red en una misma red LAN, para así evitar que la información que se traslada por medio de esta se cruce entre distintas dependencias y además mejora la seguridad de la red al crear grupos de usuarios según su función específica.

SEGURIDAD EN LA RED

La seguridad en la red es uno de los aspectos más importantes dentro de la administración de red de una empresa, puesto que de esta dependen puntos muy importantes como la integridad de la información que se maneja, es por esto que hay muchas formas en las cuales podemos proteger nuestras redes y hacerlas más seguras y así evitar algún problema que se pueda dar.

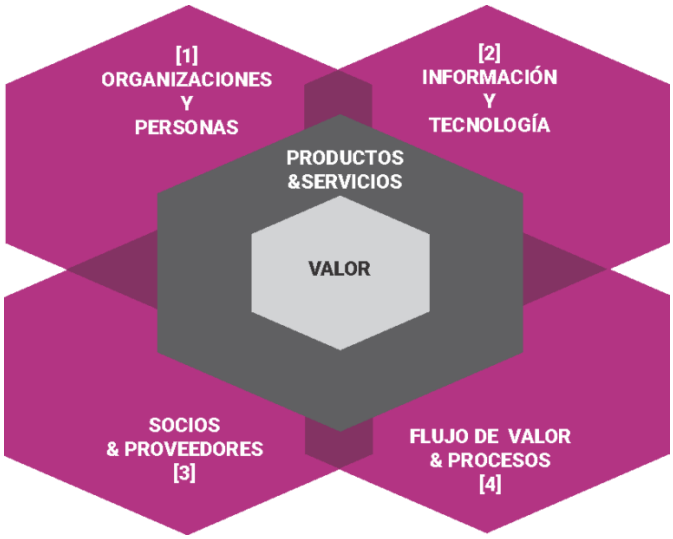
Dentro de la seguridad de la red hay 2 partes que debemos tomar en cuenta:

La primera es cuanto a la documentación de la red, en donde por medio de esta se pretende hacer lo más segura posible la red, a través de detalles como estableces contraseñas de acceso con un número mínimo de caracteres, un periodo de tiempo específico de acceso a la red y no permitir contraseñas duplicadas. La segunda es implementar políticas de seguridad en la red como no permitir que se usen contraseñas como nombres de mascotas o familiares. También es indispensable instalar software para analizar tráfico de datos, para un seguimiento estadístico o para solucionar problemas. (GAMEZ, METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES , 2012)

METODOLOGÍAS DE ADMINISTRACIÓN Y GESTIÓN DE TI

ITIL

ITIL es un conjunto de mejores prácticas y recomendaciones para la administración de servicios de tecnologías de información, enfocándose en administración de procesos. Su versión más actual es la 4 y se lanzó en febrero de 2019. Esta última versión está centrada principalmente en crear valor para los usuarios finales. Existen en este un modelo donde se presentan cuatro dimensiones que son esenciales para la creación de valor para los clientes y otras partes interesadas. Los elementos que conforman estas cuatro dimensiones tienen un impacto directo en la gestión de servicios de la empresa. Las dimensiones de este diagrama se representan de la siguiente manera:



COBIT

El Control Objectives for Information and Related Technologies en español significa Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas. Es un marco de gobierno de TI que ayuda a las empresas a desarrollar, organizar e implementar estrategias entorno a la gobernanza y la gestión de procesos de TI y de los recursos de la organización.(Lara, 2020)

COBIT es un marco de gestión que nos ayuda a sincronizar los objetivos del negocio con los de TI, para que se cree un vínculo entre las dos cosas y así definir procesos que ayuden al área de TI y a otros departamentos.

DIFERENCIAS ENTRE COBIT E ITIL

Existen muchas diferencias entre COBIT e ITIL en cuanto a objetivos y metodología. A continuación se enumeran las más importantes:

1. ITIL se basa en brindar un marco de trabajo de buenas prácticas para gestionar los servicios de IT, mientras que el objetivo de COBIT es facilitar el monitoreo y la evaluación de la seguridad de dichos servicios.
2. ITIL es una guía para las empresas para gestionar y ejecutar servicios de IT, mientras que COBIT se usa para la gestión de IT y procesos de gobernanza.
3. ITIL es una solución para mejorar claramente el flujo de trabajo, especialmente para las pequeñas organizaciones en las que los procesos de IT están todavía en sus inicios. COBIT, al estar más enfocado en la auditoría, es más importante para las empresas y organizaciones más grandes, ya que tienen más requisitos de cumplimiento.
4. ITIL es particularmente importante al establecer los procesos y estrategias de IT, mientras que COBIT asegura que esta estructura

esté en línea con las normas y en consonancia con los objetivos de una empresa u organización.

Por ejemplo, la información sobre la forma en que se establecen los procesos de IT individuales y las interfaces que pueden utilizarse mejor es algo que suele describirse en el marco de ITIL. Estos son pasos menos relevantes para el marco de COBIT. Lo que se describe en detalle en COBIT es la forma en que tal proceso puede ser auditado, cómo se hace “medible” y se mantiene en conformidad con la legislación. (Esp, Editorial, 2020)

A pesar de que COBIT e ITIL sean metodologías diferentes, estos dos pueden utilizarse en conjunto, puesto que se pueden complementar si se aplican correctamente.

CODD

Es una serie de reglas creadas por Edgar Frank Codd, quien fue el creador también del modelo relacional, que es el modelo más reconocido a nivel mundial al momento de trabajar con bases de datos, incluso para algunos, es el único que conocen.

Edgar postuló una serie de reglas que debe cumplir una base de datos para que se pueda considerar como una base de datos relacional, ya que en el mercado existían bases de datos que decían ser relacionales pero en realidad estas no estaban ni siquiera normalizadas. (Valenzuela, 2013)

Las mencionadas reglas fueron numeradas del 0 al 12 y son las siguientes:

REGLA 0

El sistema debe ser relacional, base de datos y administrador de sistema. Ese sistema debe utilizar sus facilidades relacionales (exclusivamente) para manejar la base de datos.

REGLA 1

La regla de la información, toda la información en la base de datos es representada unidireccionalmente, por los valores en posiciones de las columnas dentro de filas de tablas. Toda la información en una base de datos relacional se representa explícitamente en el nivel lógico exactamente de una manera: con valores en tablas.

REGLA 2

La regla del acceso garantizado, todos los datos deben ser accesibles sin ambigüedad. Esta regla es esencialmente una nueva exposición del requisito fundamental para las llaves primarias. Dice que cada valor escalar individual en la base de datos debe ser lógicamente direccionable especificando el nombre de la tabla, la columna que lo contiene y la llave primaria.

REGLA 3

Tratamiento sistemático de valores nulos, el sistema de gestión de base de datos debe permitir que haya campos nulos. Debe tener una representación de la "información que falta y de la información inaplicable" que es sistemática, distinto de todos los valores regulares.

REGLA 4

Catálogo dinámico en línea basado en el modelo relacional, el sistema debe soportar un catálogo en línea, el catálogo relacional debe ser accesible a los

usuarios autorizados. Es decir, los usuarios deben poder tener acceso a la estructura de la base de datos (catálogo).

REGLA 5

La regla comprensiva del sublenguaje de los datos, el sistema debe soportar por lo menos un lenguaje relacional que:

- Tenga una sintaxis lineal.
- Puede ser utilizado de manera interactiva.
- Soporte operaciones de definición de datos, operaciones de manipulación de datos (actualización así como la recuperación), seguridad e integridad y operaciones de administración de transacciones.

REGLA 6

Regla de actualización, todas las vistas que son teóricamente actualizables deben ser actualizables por el sistema.

REGLA 7

Alto nivel de inserción, actualización, y cancelación, el sistema debe soportar suministrar datos en el mismo tiempo que se inserte, actualiza o esté borrando. Esto significa que los datos se pueden recuperar de una base de datos relacional en los sistemas construidos de datos de filas múltiples y/o de tablas múltiples.

REGLA 8

Independencia física de los datos, los programas de aplicación y actividades del terminal permanecen inalterados a nivel lógico cuandoquiera que se realicen cambios en las representaciones de almacenamiento o métodos de acceso.

REGLA 9

Independencia lógica de los datos, los cambios al nivel lógico (tablas, columnas, filas, etc.) no deben requerir un cambio a una solicitud basada en la estructura. La independencia de datos lógica es más difícil de lograr que la independencia física de datos.

REGLA 10

Independencia de la integridad, las limitaciones de la integridad se deben especificar por separado de los programas de la aplicación y se almacenan en la base de datos. Debe ser posible cambiar esas limitaciones sin afectar innecesariamente las aplicaciones existentes.

REGLA 11

Independencia de la distribución, la distribución de las porciones de la base de datos a las varias localizaciones debe ser invisible a los usuarios de la base de datos. Los usos existentes deben continuar funcionando con éxito:

- Cuando una versión distribuida del SGBD se introdujo por primera vez
- cuando se distribuyen los datos existentes se redistribuyen en todo el sistema.

REGLA 12

La regla de la no subversión, si el sistema proporciona una interfaz de bajo nivel de registro, a parte de una interfaz relacional, que esa interfaz de bajo nivel no se pueda utilizar para subvertir el sistema, por ejemplo: sin pasar por seguridad relacional o limitación de integridad. Esto es debido a que existen sistemas anteriormente no relacionales que añadieron una interfaz relacional, pero con la interfaz nativa existe la posibilidad de trabajar no relacionalmente.

ISO 27000

Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la Organización Internacional para la Estandarización *(ISO) y* la Comisión Electrónica Internacional *(IEC).* Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.

Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos. (ISO Tools, 2015)

¿Qué es la ISO 27001?

- **ISO 27001:** Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Esta norma es certificable.

- **ISO 27002:** define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.
- **ISO 27003**: proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
- **ISO 27004:** proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI
- **ISO 27005:** define como se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información orientado en cómo establecer la metodología a emplear.
- **ISO 27006:** establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001
- **ISO 27007:**es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo d verificar y certificar implementaciones de la ISO/IEC-27001
- **ISO 27008:** define como se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.

- **ISO 27009:** complementa la norma 27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivos de hacer más eficaz su implantación.
- **ISO 27010:** indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas.
- **ISO 27011:** establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando como implantar los controles de manera eficiente.
- **ISO 27013:** establece una guía para la integración de las normas 27001 (SGSI) y 20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
- **ISO 27014:** establece principios para el gobierno de la seguridad de la información, para que las organizaciones puedan evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información.
- **ISO 27015:** facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros, tales como servicios bancarios o banca electrónica.
- **ISO 27016:** proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones.

- **ISO 27017:** proporciona una guía de 37 controles específicos para los servicios cloud, estos controles están basados en la norma 27002.
- **ISO 27018:** complementa a las normas 27001 y 27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en cloud para terceros.
- **ISO 27019:** facilita una guía basada en la norma 27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.

PROTOCOLOS DE RED

Son un conjunto de reglas, normas o políticas formales mediante procedimientos y formatos que definen la comunicación entre varios dispositivos dentro de una red. Incorporan todos los requisitos y restricciones necesarios para entablar una comunicación entre computadoras, routers, servidores y demás dispositivos que puedan conectarse a una red. Dichos protocolos deben de instalarse tanto por el remitente como por el receptor para que la comunicación entre la red y los datos puedan realizarse sin inconvenientes. (Jithin, 2016) Es importante tomar en cuenta que así como hay protocolos que son esenciales para la transmisión de datos y la comunicación a través de una red, existen otros que simplemente los podemos obviar, dependiendo de la situación y el lugar de aplicabilidad, es por esto que debemos conocer como mínimo aquellos que son considerados como más importantes y entender cuál es la función de cada uno de estos, por esto mencionamos los siguientes:

PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

Es el protocolo central de un conjunto de protocolos de internet. Este protocolo complementa al protocolo de internet (IP) donde juntos se conocen como TCP/IP. Pero el protocolo TCP por sí sólo lo que hace es garantizar una entrega confiable de un flujo de octetos a través de una red. Casi todas las aplicaciones que podemos encontrar en internet actualmente, se basan en TCP, tale como: World Wide Web, correo electrónico y la transferencia de archivos.

PROTOCOLO DE INTERNET

Es el protocolo principal para transmitir datos a través de las redes. Su función es proporcionar un enrutamiento que hace fácil conocer las direcciones a la cuales un flujo de datos se transfiere.

PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO (HTTP)

Se considera como la base de la comunicación para la World Wide Web. Este se basa en una estructura de datos a través de nodos que contienen textos.

El puerto que utiliza este protocolo es el 80 y 443 como puerto seguro.

PROTOCOLO DE TRANSFERENCIA DE ARCHIVOS (FTP)

Es el protocolo que más se utiliza en cuanto a la comunicación, ya que este se encarga de la transferencia de archivos a través de equipos o estaciones que están conectados en una red TCP. Básicamente se encarga de permitirnos tanto la descarga de archivos como el envío de los mismos, sin importar el sistema operativo que se utilice en cada uno de estos equipos.

El puerto predeterminado de este protocolo es el 20/21

SECURE SHELL (SSH)

Es un protocolo que nos permite conectarnos a un servidor desde lejos a través de una conexión segura con datos cifrados. También puede copiar datos de forma segura con él. Esto a veces se usa como reemplazo del protocolo telnet, que tiene varios inconvenientes notables, uno de los cuales es que no admite conexiones seguras.

El puerto predeterminado para este protocolo es el 22.

TELNET

Es un protocolo que, como SSH, nos permite acceder y gestionar de forma remota otro sistema. Aunque, a diferencia de las otras formas enumeradas anteriormente, esto no proporciona una conexión segura, es sin embargo una de las técnicas más comunes para administrar dispositivos de forma remota a través de la red.

El puerto utilizado por este protocolo es el 23.

PROTOCOLO SIMPLE DE TRANSFERENCIA DE CORREO (SMTP)

Se utiliza para dos funciones: 1) para transferir correos de un origen a un destino entre servidores de correo; y 2) para transferir correos de usuarios a un sistema de correo.

El puerto predeterminado para este protocolo es el 25 y seguro (SMTPS) es 465, aunque este no es estándar.

SISTEMA DE NOMBRES DE DOMINIO (DNS)

Es un protocolo que se encarga de convertir nombres de dominio en direcciones IP. Por ejemplo, cuando visitamos www.google.com, el DNS se encarga de convertir ese nombre de dominio en una dirección IP que nos dirige al sitio y nos permite

cargar recursos de Internet. Esto es posible gracias al hecho de que cada dispositivo conectado a Internet tiene una dirección IP única.

El puerto predeterminado de DNS es 53.

PROTOCOLO DE OFICINA POSTAL (POP)

Se utiliza para obtener los mensajes de correo electrónico que están almacenados en un servidor remoto.

El puerto predeterminado es el 110.

PROTOCOLO DE ACCESO A MENSAJES DE INTERNET (IMAP)

El funcionamiento de este protocolo puede parecer sencillo, pero es fundamental porque es responsable de conectar nuestra aplicación de correo electrónico a nuestras cuentas y así acceder a los mensajes guardados en esas cuentas.

El puerto de IMAP es el 143.

PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE REDES (SNMP)

Es un protocolo de administración de red que le permite monitorear, configurar y controlar dispositivos de red. Esto se puede configurar de modo que cuando se realiza una acción específica, los datos capturados se envían a un servidor central.

El puerto de SNMP es 161/162.

PROTOCOLO DE TRANSFERENCIA DE HIPERTEXTO SOBRE SSL/TLS (HTTPS)

Este protocolo es simplemente una forma de tecnología estándar que nos permite establecer una conexión a Internet estándar segura. Esto se logra mediante certificados que las páginas de Internet obtienen para establecer una conexión encriptada entre el navegador o computadora y un servidor o sitio web. Es posible

evitar que los datos confidenciales, como los datos de la tarjeta de crédito, sean interceptados por terceros no autorizados utilizando la seguridad proporcionada.

El puerto predeterminado de HTTPS es 443.

RAID

La tecnología RAID, que significa "Redundant Array of Independent Disks" en inglés y "Matriz redundante de discos independientes" en español, es un tipo de tecnología que nos permite tener un sistema de almacenamiento en el que empleamos numerosos HDD o SSD para distribuir o replicar nuestra información a través de ellos.

Existen numerosos tipos de niveles que se pueden utilizar para realizar este tipo de arreglos, cada uno con su propio propósito de almacenamiento de información.(Castillo, 2019)

VENTAJAS Y DESVENTAJAS DE UN RAID

VENTAJAS

- Permite una alta tolerancia a los fallos.
- Mejoras de rendimiento en la lectura y escritura.
- Posibilidad de combinar las dos propiedades anteriores.
- Buena escalabilidad y capacidad de almacenamiento.

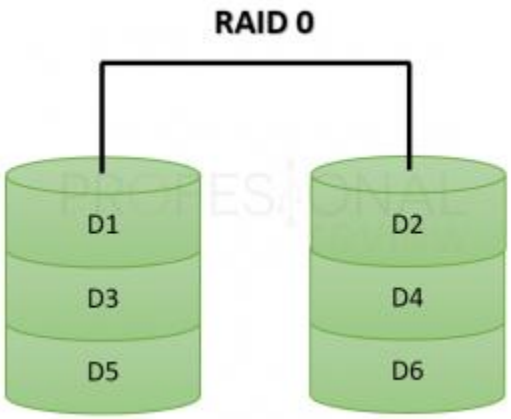
DESVENTAJAS

- La migración de datos es más complicada.
- Alto coste inicial.

NIVELES DE RAID QUE EXISTEN

RAID 0

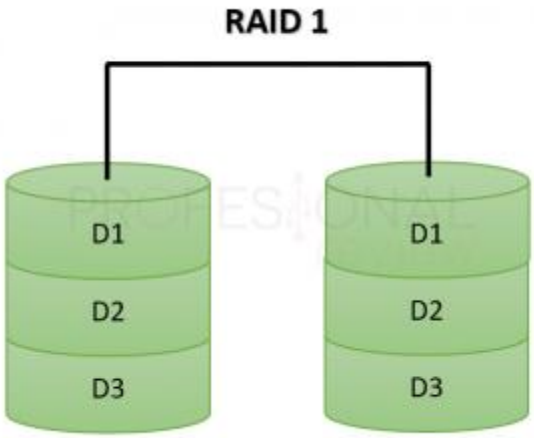
En este primer tipo denominado Nivel 0 o conjunto dividido, la función es la de distribuir los datos entre todos los discos que estén conectados al equipo.



Este tipo de RAID nos permite también manejar buenas velocidades de acceso a los datos que están guardados en las unidades de almacenamiento.

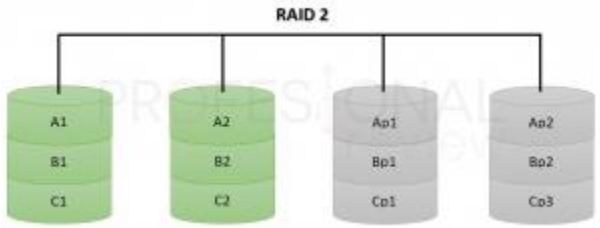
RAID 1

Esta configuración que también es llamada como configuración espejo, es una de las más utilizadas debido a que nos permite la redundancia de datos y tiene una buena tolerancia a fallos. Su funcionamiento es que la información que se almacena en las unidades, es duplicada en otra unidad llamada espejo.



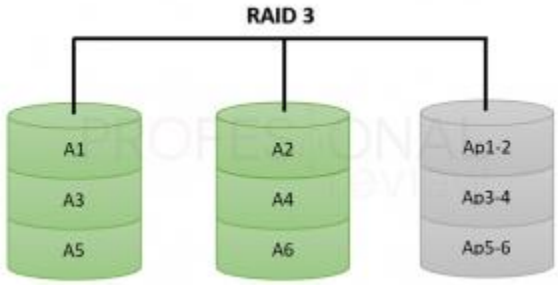
RAID 2

Este es uno de los niveles que se utilizan menos, porque realiza una distribución en todas las unidades de almacenamiento a nivel bit, pero este es el problema principal de este RAID, porque actualmente las unidades de almacenamiento ya poseen un sistema de detección de errores, por lo que esta configuración pierde un poco el sentido.



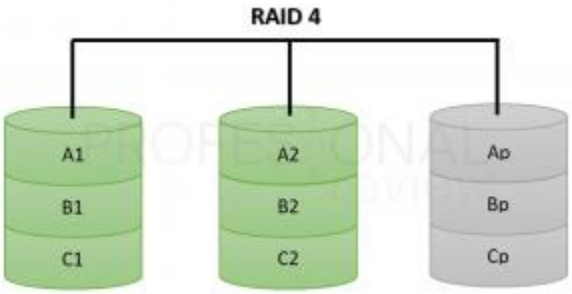
RAID 3

Tenemos una configuración en esto que no se usa actualmente, porque divide los datos a nivel de byte en múltiples unidades RAID, excepto una, que almacena información de paridad para que los datos se puedan unir cuando se lean.



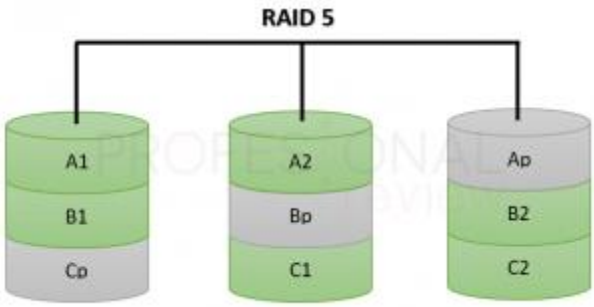
RAID 4

Esta es muy similar a al RAID 3, pero la diferencia radica en que si una de las unidades se daña, los datos pueden ser reconstruidos en tiempo real, gracias a que se almacenan bits de paridad calculados.



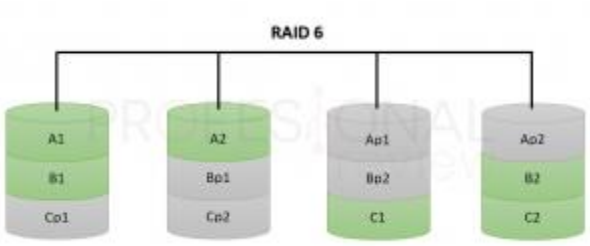
RAID 5

Esta es más utilizada que los niveles 2, 3 y 4, ya que esta configuración está incluida en los dispositivos NAS. La forma en como funciona esta configuración es almacenando la información de forma dividida en bloques que reparten entre discos duros que formen el RAID. Pero además se genera un bloque de parida para asegurar la redundancia y poder reconstruir la información en caso de que una de las unidades de almacenamiento se corrompa.



RAID 6

Este RAID es una ampliación del RAID 5, pero en este se agrega un bloque de paridad, para permitir que hasta dos unidades sean tolerantes a fallos.



REDES

Una red informática es solo una colección de equipos informáticos que se comunican entre sí mediante un conjunto de protocolos.

Las tecnologías de redes de telecomunicaciones se utilizan principalmente para permitir que las computadoras se comuniquen entre sí a través de una red). (Tokio School, 2021)

De uso individual para una comunidad más amplia, las redes se pueden clasificar según el área en la que operan o sus características. Los tipos de redes más populares que se utilizan en la actualidad se enumeran a continuación.

PAN (RED DE ÁREA PERSONAL)

Es el tipo de red informática más simple y básica. Un módem, una o más computadoras, teléfonos, impresoras, tabletas y otros dispositivos forman una red PAN.

Un PAN es una forma de red que se ve típicamente en pequeñas empresas y residencias residenciales. Son manejados por un solo individuo o una empresa desde un solo dispositivo.

UNA RED DE ÁREA LOCAL (LAN)

Es una especie de red que conecta un grupo de computadoras o dispositivos en la misma área para intercambiar datos y recursos.

RED INALÁMBRICA DE ÁREA LOCAL (WLAN)

Las WLAN actúan como una LAN utilizando tecnología de red inalámbrica como Wi-Fi.

La única diferencia entre una WLAN y una LAN es que la WLAN se conecta a la red sin utilizar cables físicos.

RED DEL ÁREA DEL CAMPUS (CAN)

Estas redes, que son más grandes que las LAN pero más pequeñas que las que veremos a continuación, se encuentran comúnmente en las universidades.

Los usuarios pueden compartir recursos distribuyéndolos entre varias estructuras vecinas.

RED DE ZONA METROPOLITANA (MAN)

Son redes mucho más grandes que LAN y CAN y cubren mucha más tierra. Este tipo de red se limita a un área geográfica específica, generalmente una ciudad o pueblo.

Su mantenimiento e instalación son realizados por empresas especializadas en este campo.

RED DE ÁREA AMPLIA (WAN)

Las redes WAN enlazan computadoras que están físicamente separadas por una distancia considerable.

Permiten que los dispositivos se comuniquen a través de una gran red, incluso si están a miles de kilómetros de distancia.

Internet es la WAN más básica, que conecta todos los dispositivos con conexión a Internet en cualquier parte del planeta.

SAN (RED DE ÁREA DE ALMACENAMIENTO)

Las SAN son redes de computadoras de alta velocidad que conectan varios servidores a grupos de almacenamiento compartido.

En este tipo de redes, no es necesaria una LAN o WAN. En estas redes, los recursos de almacenamiento se transfieren de la red a su propia red de alto rendimiento.

RED ÓPTICA PASIVA DEL ÁREA LOCAL (POLAN)

Como alternativa a las LAN tradicionales basadas en conmutadores, la tecnología POLAN está integrada en el cableado, lo que elimina las preocupaciones sobre la compatibilidad con los protocolos Ethernet típicos.

POLAN es una LAN de punto a multipunto que utiliza divisores ópticos para dispersar la señal de un hilo de fibra óptica monomodo a usuarios y dispositivos.

RED PRIVADA EMPRESARIAL (EPN)

Estas redes son creadas y son propiedad de empresas que desean conectar de forma segura sus numerosos sitios de uso compartido de recursos informáticos.

Una VPN permite que sus dispositivos envíen y reciban datos como si estuvieran vinculados a una red privada, a pesar de que no lo están.

Los usuarios pueden utilizar una conexión virtual para conectarse a una red privada desde lejos.

COSTOS

Cantidad	Descripción	Precio Unitario	Costo Total
6	DELL SERVIDOR POWEREDGE T40 XEON E-2224G 3.5GH 8GB1 TB DVD	**Q.5909.00**	**Q.35454.00**
9	NEXXT AXIS 2400R SWITCH DE 24 PUERTOS 10/100/1000 RACK METAL	**Q.974.00**	**Q.5844.00**
9	LINKSYS EA8300 MAX STREAM AC2200 MU-MIMO GIGABIT ROUTER INALAMBRICO	**Q.1510.00**	**Q.13590.00**
1	BOLSA DE CONECTORES (100 UNIDADES) RJ45 CAT6	**Q.200.00**	**Q.200.00**
6	BOBINA DE CABLE UTP CAT6/ INTERIOR 305MTS GRIS	**Q.543.03**	**Q.3258.18**
	KASPERSKY INTERNET SECURITY 1 USUARIO - WINDOWS MAC ANDROID iOS 1 AÑO	**Q.307.00**	
1	LICENCIA DE ZERO TIER 1 PROFESSIONAL PARA 500 USUARIOS		**Q.387.10 MENSUALES**
	MANO DE OBRA POR INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN DE LA RED		**Q.20,000.00**

CONCLUSIONES

- Con la implementación de este nuevo diseño de red, le permitimos a la Compañía Alimentos Buena Vida agregar tantos usuarios sean necesarios dentro de las redes que se conformaron tanto en la casa matriz, como en las sucursales, ya que con la distribución de las IP, creación de las VLANS, implementación de VPN y asignaciones de IP por medio de servidores DHCP, se facilita el crecimiento.
- Permitimos una mayor seguridad en la información que se maneja en la compañía al realizar los diferentes planes de seguridad, de recuperación de datos y medidas de contingencia, puesto que esto nos permite tener una guía específica de las acciones a tomar al momento de presentarse un problema lógico o físico en la organización.

GLOSARIO

Ancho de Banda: Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado.

Backbone (Red Troncal): Conexión de alta velocidad dentro una red que interconecta los principales sitios de la Internet. Las redes de grandes empresas pueden estar compuestas por múltiples LAN (segmentos) y se conectan entre sí a través del backbone, que es el principal conducto que permite comunicar segmentos entre sí.

BGP: Es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos.

Calidad de Servicio (QoS): Es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.

IP: Se puede considerar el más importante de los protocolos sobre los cuales se basa la Internet.

IPv4: Es la cuarta versión del protocolo Internet Protocol (IP), y la primera en ser implementada a gran escala.

IPv6: Es una versión del protocolo Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet

ISP: Es la empresa que brinda conexión a Internet a sus clientes.

LAN: Un tipo de arreglo para comunicación de datos a alta velocidad. Red limitada en el espacio, concebida para abastecer a sub- unidades organizativas.

SWICH: Es un aparato que canaliza los datos provenientes de múltiples puertos a un puerto en específico que llevara los datos a su destino.

TCP: Es uno de los protocolos fundamentales en Internet. Crea conexiones entre sí a través de las cuales puede enviarse un flujo de datos.

WAN: Es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes.

BIBLIOGRAFÍA/EGRAFÍA

Bibliografía

Castillo, J. (24 de Enero de 2019). *profesionalreview.com*. Obtenido de https://www.profesionalreview.com/2019/01/24/tecnologia-raid/

Esp, Editorial. (2 de Diciembre de 2020). *freshservice.com*. Obtenido de https://freshservice.com/es/itil/itil-vs-cobit-que-marco-es-mas-recomendable-blog/

GAMEZ, D. (2012). METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES. En D. GAMEZ, *METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES* (págs. 30-32). Bogotá.

GAMEZ, D. (2012). METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES . En D. GAMEZ, *METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES* (pág. 32). Bogotá.

GAMEZ, D. (2012). METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES . En D. GAMEZ, *METODOLOGÍA PARA EL ANÁLISIS Y DISEÑO DE REDES* (pág. 36). Bogotá.

IBM. (2020). *ibm.com*. Obtenido de https://www.ibm.com/docs/es/aix/7.1?topic=cards-virtual-local-area-networks

ISO Tools. (21 de Enero de 2015). *www.isotools.org*. Obtenido de https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

Jithin. (4 de Agosto de 2016). *interserver.net*. Obtenido de https://www.interserver.net/tips/kb/common-network-protocols-ports/

Lara, C. (10 de Noviembre de 2020). *icorp.com.mx*. Obtenido de http://www.icorp.com.mx/blog/que-es-cobit-y-para-que-sirve/

PRIETO, D. A. (2012). *repository.unilibre.edu.co.*

Rouse, M. (Abril de 2021). *www.computerweekly.com*. Obtenido de https://www.computerweekly.com/es/definicion/Topologia-de-red

Tokio School. (21 de Mayo de 2021). *tokioschool.com*. Obtenido de https://www.tokioschool.com/noticias/tipos-redes-informaticas/

Valenzuela, G. (18 de Julio de 2013). *medievalstrucos.com*. Obtenido de https://medievalstrucos.com/2013/07/18/12-reglas-de-codd-para-bases-de-datos-relacionadas/

ANEXOS

Link Repositorio de este documento: https://github.com/MasterJB2127/ATI-EGP-UMG

CODIGO PARA CREAR VLAN'S EN LA RED

SWITCH GERENCIA

vlan 10

name GERENCIA

VLAN 20

NAME VENTAS

VLAN 30

NAME RRHH

VLAN 100

NAME NATIVA

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 10,20,30,100

switchport trunk native vlan 100

int g0/1

switchport mode access

switchport access vlan 10

int g0/2

switchport mode access

switchport access vlan 20

int g0/3

switchport mode access

switchport access vlan 30

int g0/2

switchport mode access

switchport access vlan 10

int g0/3

switchport mode access

switchport access vlan 20

int g1/0

switchport mode access

switchport access vlan 30

VTP MODE CLIENT

VTP DOMAIN PROYECTO

VTP PASSWORD RD

VTP VERSION 2

SWITCH VENTAS

vlan 10

name GERENCIA

VLAN 20

NAME VENTAS

VLAN 30

NAME RRHH

VLAN 100

NAME NATIVA

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 10,20,30,100

switchport trunk native vlan 100

int g0/1

switchport mode access

switchport access vlan 10

int g0/2

switchport mode access

switchport access vlan 20

int g0/3

switchport mode access

switchport access vlan 30

int g0/2

switchport mode access

switchport access vlan 10

int g0/3

switchport mode access

switchport access vlan 20

int g1/0

switchport mode access

switchport access vlan 30

VTP MODE CLIENT

VTP DOMAIN PROYECTO

VTP PASSWORD RD

VTP VERSION 2

SWITCH RRHH

vlan 10

name GERENCIA

VLAN 20

NAME VENTAS

VLAN 30

NAME RRHH

VLAN 100

NAME NATIVA

switchport trunk encapsulation dot1q

switchport mode trunk

switchport trunk allowed vlan 10,20,30,100

switchport trunk native vlan 100

int g0/1

switchport mode access

switchport access vlan 10

int g0/2

switchport mode access

switchport access vlan 20

int g0/3

switchport mode access

switchport access vlan 30

int g0/2

switchport mode access

switchport access vlan 10

int g0/3

switchport mode access

switchport access vlan 20

int g1/0

switchport mode access

switchport access vlan 30

VTP MODE SERVER

VTP DOMAIN PROYECTO

VTP PASSWORD RD

VTP VERSION 2

CONFIGURACIÓN DE DHCP PARA ASIGNACIÓN DE IP

CONFIGURACION DE DHCP ROUTER VLAN

int g1/0.10

encapsulation dot1q 10

ip add 192.168.2.32 255.255.255.224

int g1/0.20

encapsulation dot1q 20

ip add 192.168.2.64 255.255.255.224

int g1/0.30

encapsulation dot1q 30

ip add 192.168.2.96 255.255.255.224

ip dhcp pool GERENCIA

network 192.168.2.32 255.255.255.224

default-router 192.168.2.33

ip dhcp pool VENTAS

network 192.168.2.64 255.255.255.224

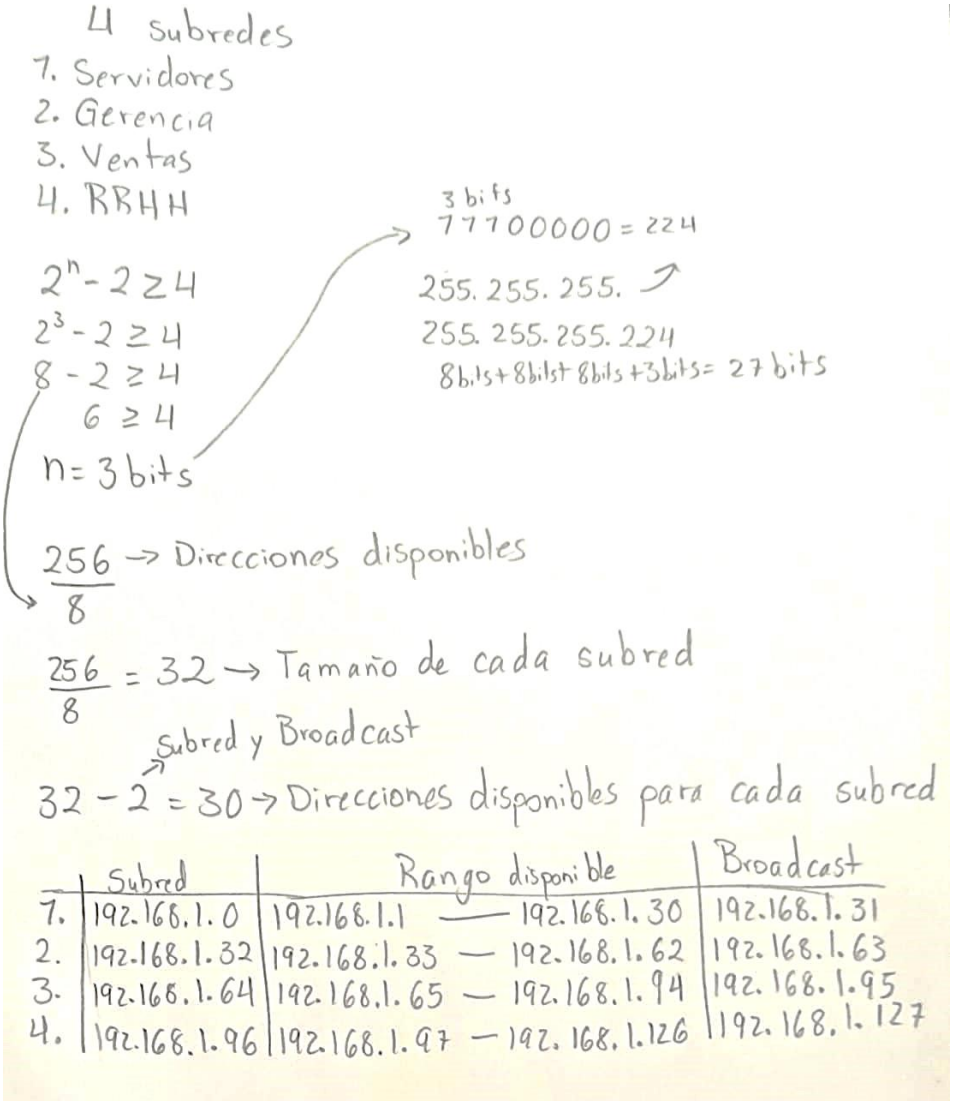
default-router 192.168.2.65

ip dhcp pool RRHH

network 192.168.2.96 255.255.255.224

default-router 192.168.2.97

PROCEDIMIENTO PARA EL CÁLCULO DE LAS SUBREDES



	Subred	Rango disponible	Broadcast
1.	192.168.1.0	192.168.1.1 — 192.168.1.30	192.168.1.31
2.	192.168.1.32	192.168.1.33 — 192.168.1.62	192.168.1.63
3.	192.168.1.64	192.168.1.65 — 192.168.1.94	192.168.1.95
4.	192.168.1.96	192.168.1.97 — 192.168.1.126	192.168.1.127