



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO®

Instituto Tecnológico de Apizaco

TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE APIZACO

**CONFIGURACIÓN Y MANTENIMIENTO DE DISPOSITIVOS DE
REDES PARA SERVICIOS DIGITALES CON SEGUIMIENTO Y
CONTROL USANDO BASE DE DATOS**

TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

**PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES**

**PRESENTA:
ANGEL RICARDO ALBURQUERQUE FLORES**

**NOMBRE DEL ASESOR:
LIC. LAURO CARLOS PAYÁN REYES**



APIZACO, TLAX., ENERO 2024



Instituto Tecnológico de Apizaco

Apizaco, Tlaxcala, **13/junio/2023**

OFICIO No: SC/OPV/148/23

ASUNTO: Liberación de proyecto
para titulación integral

MARTÍN ROJAS RAMÍREZ
JEFE DEL DEPTO. DE DIVISIÓN DE ESTUDIOS PROFESIONALES
P R E S E N T E.

POR ESTE MEDIO LE INFORMO QUE HA SIDO LIBERADO EL SIGUIENTE PROYECTO PARA LA TITULACIÓN INTEGRAL.

NOMBRE DEL EGRESADO:	ÁNGEL RICARDO ALBURQUERQUE FLORES
CARRERA:	INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
NO. DE CONTROL:	19370968
NOMBRE DEL PROYECTO:	CONFIGURACIÓN Y MANTENIMIENTO DE DISPOSITIVOS DE REDES PARA SERVICIOS DIGITALES CON SEGUIMIENTO Y CONTROL USANDO BASES DE DATOS.
PRODUCTO U OPCIÓN:	TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL

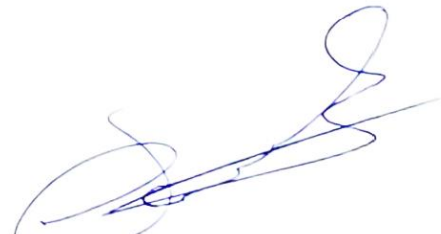
AGRADEZCO DE ANTEMANO SU VALIOSO APOYO EN ESTA IMPORTANTE ACTIVIDAD PARA LA FORMACIÓN PROFESIONAL DE NUESTROS EGRESADOS.

ATENTAMENTE

*Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®*


ALAN AUGUSTO CALLEGOS CUELLAR
JEFE DEL DEPTO. DE SISTEMAS Y COMPUTACIÓN

c.c.p. División de Estudios Profesionales
c.c.p. Depto. de Servicios Escolares
c.c.p. Archivo
AAGC/mrol*


LAURO CARLOS PAYAN REYES

ASESOR INTERNO



Carretera Apizaco-Tzompantepec, esquina con Av. Instituto Tecnológico S/N,
Conurbado Apizaco-Tzompantepec, Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010 Ext. 115,
e-mail: sistemas@apizaco.tecnm.mx | tecnm.mx | apizaco.tecnm.mx



2022 *Ricardo Flores*
Año de Magón



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO®

Instituto Tecnológico de Apizaco

Apizaco, Tlax., **11/diciembre/2023**
No. OFICIO: DEP-CT/870/2023

ASUNTO: AUTORIZACIÓN DE IMPRESIÓN

ANGEL RICARDO ALBURQUERQUE FLORES
EGRESADO DE LA CARRERA DE
INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
CON NÚMERO DE CONTROL: 19370968
P R E S E N T E

Por este medio, me permito informar a usted que por aprobación de la comisión revisora asignada para valorar el trabajo que mediante la opción **TITULACIÓN INTEGRAL INFORME DE RESIDENCIA PROFESIONAL** cuyo tema es: **"CONFIGURACIÓN Y MANTENIMIENTO DE DISPOSITIVOS DE REDES PARA SERVICIOS DIGITALES CON SEGUIMIENTO Y CONTROL USANDO BASE DE DATOS"**, conforme a lo establecido en el procedimiento para la obtención del Título Profesional en el Instituto Tecnológico, la División de Estudios Profesionales a mi cargo le otorga:

AUTORIZACIÓN DE IMPRESION

Debiendo entregar **3** empastados del mismo, apropiadamente encuadernados, a la brevedad, para presentar su acto de recepción profesional.

Sin otro particular por el momento, le envió un cordial saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®
Pensar para Servir, Servir para Triunfar®


MARTÍN ROJAS RAMÍREZ
JEFE DE LA DIVISIÓN DE ESTUDIOS PROFESIONALES



c.p. archivo



Av. Instituto Tecnológico No. 418, San Andrés Ahuashuatepec, Municipio de Tzompantepec,
Tlaxcala, Mex. C.P. 90491 Tel. (241) 4172010 Ext. 304,
e-mail: dep_titulacion@apizaco.tecnm.mx



Agradecimientos

Estimados lectores,

Me complace dedicar estas líneas para agradecer a todas las personas que de alguna manera contribuyeron a la realización de mi reporte de residencia profesional.

En primer lugar, deseo agradecer a mi asesor de residencia, quien me brindó su guía y conocimientos para desarrollar mi proyecto y me apoyó en todo momento para alcanzar mis objetivos.

También me gustaría expresar mi gratitud a todo el personal de la empresa donde realicé mi residencia, por abrirme las puertas y darme la oportunidad de aprender de su experiencia y conocimiento en el área. Fueron un gran equipo con el que pude trabajar y aprender de ellos, lo que me permitió crecer profesionalmente y adquirir habilidades valiosas.

Además, no puedo dejar de agradecer a mis compañeros de trabajo, quienes me recibieron con amabilidad y me brindaron su apoyo en todo momento, tanto en lo laboral como en lo personal. Me hicieron sentir parte del equipo y me ayudaron a desenvolverme en el ambiente laboral de manera más eficiente.

Por último, agradezco a mi familia y amigos, quienes me brindaron su apoyo y motivación para culminar esta etapa de mi formación profesional, siempre estuvieron alentándome y brindándome su apoyo y amor, lo que me permitió cumplir con éxito esta meta.

Gracias a todos por su contribución en esta experiencia, me siento afortunado de haber contado con su apoyo en mi formación profesional.

Resumen

La configuración y mantenimiento de dispositivos de redes para servicios digitales con seguimiento y control utilizando una base de datos es un proceso fundamental en la gestión de redes. En primer lugar, es necesario configurar los dispositivos de red para que puedan conectarse correctamente a la red y permitir el acceso a los servicios digitales que se ofrecen. Esto implica establecer configuraciones como direcciones IP, protocolos de enrutamiento y políticas de seguridad.

Una vez que se han configurado los dispositivos de red, es importante asegurarse de que estén funcionando correctamente y que la red esté operando de manera eficiente. Para ello, se debe realizar un mantenimiento periódico, que incluye actualizaciones de firmware y software, y la monitorización continua del estado de los dispositivos de red. La base de datos es un elemento clave en la gestión del mantenimiento, ya que permite el seguimiento y control de los dispositivos de red y su estado en tiempo real.

Además, la base de datos puede utilizarse para recopilar información y estadísticas sobre el tráfico de red, lo que permite identificar patrones de uso y detectar problemas en la red. Esta información también puede ser utilizada para mejorar la calidad del servicio ofrecido a los usuarios.

En resumen, la configuración y mantenimiento de dispositivos de redes para servicios digitales con seguimiento y control utilizando una base de datos es un proceso esencial en la gestión de redes, ya que garantiza el correcto funcionamiento de la red y el acceso a los servicios digitales. La base de datos es un elemento clave en este proceso, ya que permite el seguimiento y control de los dispositivos de red y su estado en tiempo real, así como la recopilación de información para mejorar la calidad del servicio ofrecido a los usuarios.

Índice

Agradecimientos.....	2
Resumen	3
Índice de figuras	9
Introducción.....	1
Descripción de la empresa u organización y del puesto o área del trabajo el estudiante	2
Ocean restoration & construction corp.....	2
Área de trabajo del residente	3
Problemas por resolver	4
Objetivos.....	5
Objetivo general	5
Objetivos específicos.....	5
Justificación.....	6
Marco teórico.....	7
Tipos de mantenimiento	7
Mantenimiento preventivo.....	7
Mantenimiento correctivo	7
Mantenimiento predictivo	7
Mantenimiento proactivo.....	8
Mantenimiento adaptativo	8

Estándares para mantenimiento de redes.....	8
LAN (Red de área local).....	10
Topología de red en bus.	10
Topología de red en estrella.	10
Topología de red anillo.....	11
Topología de red jerárquica.....	11
Topología de red malla.	12
Dirección IP.....	12
Clase A.	13
Clase B.....	13
Clase C.....	13
VLAN (Red de área local virtual).	13
Beneficios de las VLAN.....	14
DHCP.	14
Base de datos	15
Medidas de seguridad	16
Tipos de base de datos.....	17
Base de datos relacional	18
Base de datos jerárquica	18
Base de datos de red	18

Base de datos orientada a objetos	18
Base de datos NoSQL.....	18
Base de datos distribuida	19
Importancia de una base de datos en el seguimiento y control de una red de comunicaciones	19
Políticas y leyes en NY.....	20
Desarrollo	21
Reconocimiento de la red	21
Definición de dispositivos	22
Configurar puntos de red	23
Nuevo diseño de red	24
Selección de equipos de red	24
Configuración de los nuevos puntos de red.....	25
Pruebas y verificación	26
Documentación.....	26
Supervisar y mejorar el rendimiento de la red.....	27
Supervisión de la Red	27
Mejora del Rendimiento de la Red	27
Crear y mantener la documentación de la red	28
Creación de la Documentación de la Red.....	28

Mantenimiento de la Documentación de la Red.....	29
Revisión por parte del equipo de TI	29
Garantizar el Cumplimiento de las Políticas de la Red	30
Asegurar la red contra todo tipo de amenazas.....	31
Creación de base de datos para el control de la red.....	32
Definición de requisitos:.....	32
Selección del sistema de gestión de bases de datos (SGBD):	33
Diseño del modelo de datos:.....	34
Creación de las tablas y definición de los campos:	36
Establecimiento de relaciones entre las tablas:	38
Definición de restricciones y validaciones:	41
Creación de índices:	43
Establecimiento de seguridad:	44
Pruebas y optimizaciones:	46
Copias de seguridad y plan de recuperación:	48
Competencias desarrolladas	49
Conocimientos técnicos en redes.....	49
Solución de problemas	49
Documentación.....	49
Seguridad.....	49

Gestión de bases de datos	50
Trabajo en equipo	50
Conocimientos en virtualización	50
Planificación y organización	50
Monitoreo y análisis de la red	50
Soluciones innovadoras	51
Comunicación efectiva	51
Conocimientos de normativas y regulaciones	51
Análisis de riesgos	51
Conocimientos en sistemas operativos	51
Administración de bases de datos.....	51
Resolución de problemas.....	51
Conocimientos en seguridad informática	52
Actualización y capacitación continua	52
Fuentes de información	52

Índice de figuras

Figura 1. Protocolos soportados	9
Figura 2. Topología de red en bus.	10
Figura 3. Topología red en estrella.	11
Figura 4. Topología red en anillo.	11
Figura 5. Topología red jerárquica	12
Figura 6. Topología red en malla.	12
Figura 7. Escaneo de la red actual.	22
Figura 8. Estado actual de la red	23
Figura 9. Organización de la red futura.....	24
Figura 10. identificación de dispositivos.....	24
Figura 11. Configuración de puntos.	25
Figura 12. Conexión con el servidor DHCP.....	25
Figura 13. Creación de nuevos segmentos.	26
Figura 14. Definir rango de direcciones IP.	26
Figura 15. Primera pantalla del SGBD.....	33
Figura 16. Primer propuesta para la BD.	35
Figura 17. Propuesta final para la BD	37
Figura 18. Modelo relacional.	38
Figura 19. código de creación de tablas.	39
Figura 20. visualización de las filas de cada tabla.....	39
Figura 21. tablas creadas en la BD.	39
Figura 22. Asignación de llaves primarias.	40

Figura 23. asignación de llaves foráneas.....	40
Figura 24. llaves primarias y foráneas asignadas.	40
Figura 25. Código para insertar datos.....	40
Figura 26. inserción de datos genéricos en la BD.	41

Introducción

En la actualidad, la conectividad y el acceso a servicios digitales son elementos clave en la vida diaria de las personas y las empresas. Para garantizar la calidad del servicio y el correcto funcionamiento de la red, es necesario llevar a cabo la configuración y mantenimiento adecuados de los dispositivos de red utilizados en la conexión y prestación de estos servicios.

La configuración y mantenimiento de dispositivos de redes para servicios digitales con seguimiento y control utilizando una base de datos es una tarea crítica en la gestión de redes. La configuración adecuada de estos dispositivos permite el acceso a los servicios digitales de manera eficiente y segura, mientras que el mantenimiento periódico asegura el correcto funcionamiento de la red y la prevención de problemas técnicos.

El seguimiento y control de los dispositivos de red se realiza mediante el uso de una base de datos, lo que permite tener una visión completa del estado de la red y de los dispositivos conectados a ella. Esta información permite identificar patrones de uso, detectar problemas en la red y tomar decisiones informadas para mejorar la calidad del servicio.

En esta introducción, se aborda la importancia de la configuración y mantenimiento adecuado de dispositivos de red para servicios digitales y la utilización de una base de datos para llevar a cabo el seguimiento y control de estos dispositivos. Asimismo, se destacará la relevancia de una gestión adecuada de la red para garantizar la calidad del servicio ofrecido a los usuarios.

Descripción de la empresa u organización y del puesto o área del trabajo el estudiante

Ocean restoration & construction corp.

La empresa ofrece servicios, como la gestión de permisos y licencias de construcción, la coordinación de los diferentes trabajos de remodelación, y el seguimiento del progreso del proyecto para asegurarse de que se cumplan los plazos y presupuestos.

Se dedica a la renovación y mejora de edificios y espacios residenciales y comerciales. Proporciona servicios como la remodelación de cocinas y baños, la instalación de nuevos pisos y paredes, la reparación y reemplazo de techos y ventanas, y la ampliación de espacios habitables etc.

Cuenta con un equipo de profesionales calificados, como contratistas generales, arquitectos, diseñadores de interiores, especialistas en construcción y especialistas en comunicaciones. Estos profesionales trabajan en estrecha colaboración para entender sus necesidades y objetivos de remodelación, y luego crean un plan detallado para la remodelación.

La corporación ocean restoration & construction corp, es una corporacion comercial nacional, la corporación cuenta con una matrícula de 73 trabajadores distribuidos en 7 departamentos diferentes. La carrera de Tecnologías de la Información y Comunicaciones pertenece al departamento de TI y es el área donde se pretende llevar a cabo el proyecto de residencia profesional planteado y está ubicado en Brooklyn NY.

Giro o actividad y tipo de capital:

Corporación comercial nacional, institución privada.

Dirección, teléfono, correo electrónico de la empresa.

1209 Myrtle avenue Brooklyn NY 11221, (646)606-7470, luis.ocean.restoration@gmail.com

Mapa de localización.

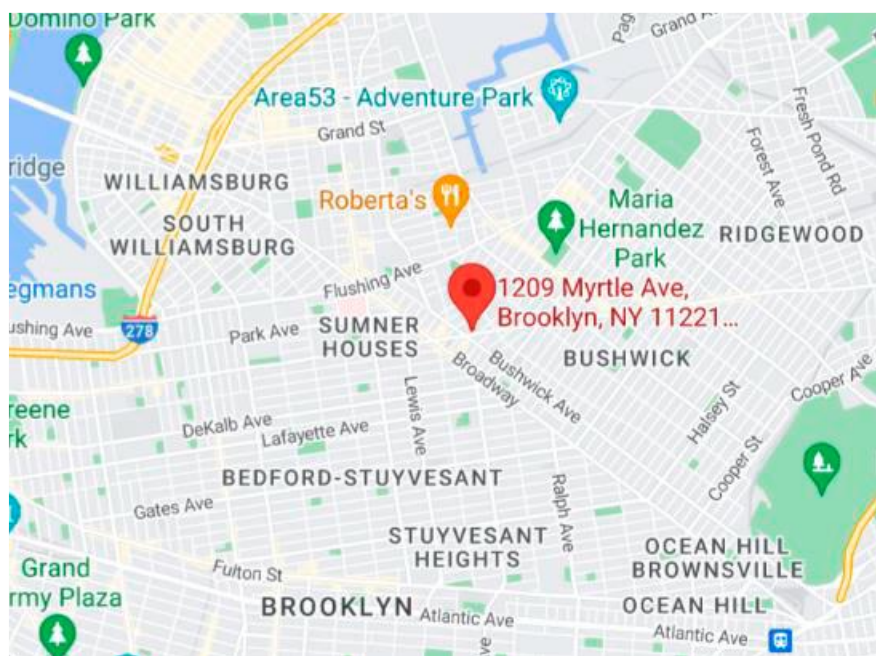


Figura 1. Localización de la corporación.

Área de trabajo del residente

El departamento de tecnologías de la información (TI) es responsable de la gestión y mantenimiento de los sistemas informáticos y de tecnología utilizados por la empresa. Este departamento es esencial para garantizar que la empresa tenga la capacidad de procesar, almacenar y acceder a la información crítica de manera segura y eficiente.

Los profesionales que trabajan en el departamento de TI son especialistas en redes, ingenieros de sistemas, analistas de seguridad, administradores de bases de datos, desarrolladores de software, entre otros. Estos profesionales trabajan juntos para garantizar que la infraestructura de

TI de la empresa sea sólida y segura, y que se mantenga actualizada con las últimas tendencias y avances tecnológicos.

- Entre las responsabilidades del departamento se encuentran:
- Mantenimiento y actualización de la infraestructura de TI, incluyendo servidores, redes, hardware y software
- Gestión y supervisión de la seguridad de la información y la protección de los sistemas contra amenazas externas e internas
- Desarrollo e implementación de políticas y procedimientos de seguridad y protección de datos
- Soporte técnico y capacitación para los usuarios de los sistemas informáticos y de tecnología
- Investigación y prueba de nuevas tecnologías para determinar su aplicabilidad en la empresa
- Planificación y coordinación de proyectos de TI

Problemas por resolver

Problemas de compatibilidad: Puede haber problemas para conectar diferentes tipos de dispositivos a la red, especialmente cuando se utilizan diferentes sistemas operativos o plataformas.

- Problemas de configuración: Los problemas de configuración pueden incluir problemas con la asignación de direcciones IP, problemas con la configuración de routers y problemas con la configuración de dispositivos de red.

- Problemas de conectividad: Esto puede incluir dificultades para conectar dispositivos a la red, problemas con la velocidad de la red y problemas con la estabilidad de la conexión.
- Problemas de rendimiento: Una red de comunicación puede ser lenta, especialmente cuando se está compartiendo una gran cantidad de datos o cuando hay muchos dispositivos conectados a la red.
- Problemas de seguridad: Una red de comunicación insegura puede estar expuesta a ataques de virus, malware, piratas informáticos, etc. Esto puede llevar a la pérdida o el robo de datos y puede causar graves problemas para la empresa.

Objetivos

Objetivo general

Diseñar y desarrollar un plan de gestión de configuración y mantenimiento de la infraestructura para el área de comunicación del departamento de TI de la corporación ocean restoration & construction corp, con seguimiento y control usando una base de datos.

Objetivos específicos

- Identificar los tipos de mantenimiento de redes disponibles en la actualidad.
- Realizar un estudio del estado del arte de los estándares para mantenimiento de redes.
- Diseñar un plan de mantenimiento para el área de comunicaciones de ocean restoration & construction corp.
- Evaluación de herramientas informáticas que automatice el mantenimiento.

Justificación

La creación de una nueva red de comunicación en una empresa puede justificarse por varias razones importantes. En primer lugar, una red actualizada puede mejorar significativamente la eficiencia de la empresa al permitir la transferencia rápida y segura de datos, lo que a su vez reduce el tiempo de respuesta y aumenta la productividad. Además, una red de comunicación moderna puede reducir los costos de la empresa al eliminar la necesidad de sistemas de comunicación más antiguos y obsoletos, como los sistemas de fax, correo postal y otros medios más lentos y costosos.

La mejora en la colaboración es otra razón importante para crear una nueva red de comunicación. Una nueva red puede fomentar la comunicación entre empleados y departamentos, lo que a su vez puede aumentar la creatividad y la innovación dentro de la empresa. La colaboración también puede ser más efectiva y eficiente, ya que se pueden compartir documentos y archivos en tiempo real.

La seguridad también es un factor clave en la justificación de la creación de una nueva red de comunicación. Las redes modernas están diseñadas con medidas de seguridad avanzadas para proteger la información confidencial y prevenir ataques externos. Una red segura puede ayudar a proteger la empresa contra amenazas cibernéticas, como virus, malware y piratería informática.

Por último, la creación de una nueva red de comunicación también puede ser justificada por su capacidad para soportar nuevas tecnologías emergentes. Una red moderna y actualizada puede soportar nuevas tecnologías y herramientas de comunicación que pueden ser críticas para mantenerse competitivo en un entorno empresarial en constante evolución.

En conclusión, la creación de una nueva red de comunicación en una empresa puede ser justificada por su capacidad para mejorar la eficiencia, reducir costos, fomentar la colaboración, mejorar la seguridad y soportar nuevas tecnologías emergentes. Es importante trabajar con profesionales calificados en la creación y configuración de la nueva red para asegurarse de que sea adecuada y segura para las necesidades específicas de la empresa.

Marco teórico

Tipos de mantenimiento

Existen varios tipos de mantenimiento de redes disponibles en la actualidad, entre los que destacan *((Los 4 tipos de mantenimiento de software: ¿qué es el mantenimiento de software?, s. f.))*:

Mantenimiento preventivo: Este tipo de mantenimiento se realiza de forma regular y programada, con el fin de evitar posibles fallas o problemas en la red. Incluye tareas como la limpieza de equipos, la actualización de software, la revisión de componentes y la evaluación del desempeño de la red.

Mantenimiento correctivo: Se realiza cuando se detecta una falla en la red, con el fin de identificar y solucionar el problema. Incluye tareas como la identificación de la causa de la falla, la reparación o reemplazo de componentes, la restauración de configuraciones y la realización de pruebas para verificar que el problema se ha resuelto.

Mantenimiento predictivo: Este tipo de mantenimiento se basa en el monitoreo constante de la red, con el fin de prever posibles fallas o problemas antes de que ocurran. Utiliza herramientas de monitoreo y análisis de datos para identificar patrones y tendencias que indiquen posibles problemas en la red.

Mantenimiento proactivo: Se realiza con el objetivo de mejorar el desempeño y la eficiencia de la red, antes de que surjan problemas. Incluye tareas como la identificación de cuellos de botella en la red, la optimización de configuraciones y la actualización de componentes para mejorar la capacidad y la velocidad de la red.

Mantenimiento adaptativo: Este tipo de mantenimiento se enfoca en la adaptación de la red a cambios en el entorno o en los requerimientos de la empresa. Incluye tareas como la configuración de nuevas políticas de seguridad, la implementación de nuevas tecnologías y la actualización de componentes para mantener la compatibilidad con los nuevos estándares de la industria (Calderon & Calderon, 2021).

Estándares para mantenimiento de redes

Existen varios estándares para el mantenimiento de redes que se utilizan en todo el mundo, incluyendo el ISO/IEC 14763-2, el ISO/IEC 20000-1, ITIL, IEEE 802.1AB y NIST SP 800-53. Cada uno de estos estándares proporciona una guía para la gestión del mantenimiento de redes y la seguridad de la información, lo que ayuda a las organizaciones a mantener sus redes seguras y eficientes.

- **ISO/IEC 14763-2:** Este estándar define las prácticas recomendadas para el mantenimiento de infraestructuras de telecomunicaciones en edificios y campus. Incluye una guía para la gestión del mantenimiento de redes, la documentación necesaria, los planes de mantenimiento y los procedimientos de prueba y verificación.
- **ISO/IEC 20000-1:** Este estándar define las mejores prácticas para la gestión de servicios de tecnologías de la información (TI). Incluye un marco para la gestión de servicios de TI, que abarca aspectos como la gestión de incidentes, la gestión de

cambios y la gestión de problemas, que son fundamentales para el mantenimiento de redes.

- ITIL (Information Technology Infrastructure Library): Este conjunto de mejores prácticas para la gestión de servicios de TI incluye un marco para la gestión de incidentes, la gestión de problemas, la gestión de cambios y la gestión de configuraciones, entre otros aspectos que son importantes para el mantenimiento de redes.
- IEEE 802.1AB (LLDP): Este estándar define el protocolo Link Layer Discovery Protocol (LLDP), que se utiliza para el descubrimiento de topología de redes. Ayuda a los administradores de red a identificar los dispositivos conectados a la red y su ubicación física, lo que es útil para el mantenimiento y la solución de problemas en la red.
- NIST SP 800-53: Este estándar define los controles de seguridad y los requisitos para los sistemas de información del gobierno de EE. UU. Incluye un conjunto de controles y prácticas recomendadas para la gestión de la seguridad de la información, que son fundamentales para el mantenimiento de redes seguras (*Estándares para la comunicación industrial - Comunicaciones Industriales - Logitek*, 2015).

Concepto	ANSI/TIA-568	ISO/IEC-11801	CENELEC EN-5017
Cable cat.3	Soportado	Soportado clase C	Soportado clase C
Cable cat.5e	Soportado	Soportado clase D	Soportado clase D
Cable cat.6	Soportado	Soportado clase E	Soportado clase E
Cable cat.6a	Soportado	Soportado clase EA	Soportado clase EA
Cable cat.7	No reconocido	Soportado clase F	Soportado clase F
Fibra MM 50/125-62.5/125	Soportado	Soportado	Soportado
Fibra OM	Soportado	Soportado	Soportado
Fibra OM al área de trabajo	No reconocido	Soportado	Soportado
Configuración de TO	T568A o T568B	T568A	T568A

Figura 2. Normas y estándares (recuperado de (Anmeran, 2017))

LAN (Red de área local).

Es por donde diferentes dispositivos como lo puede ser computadores, impresoras, cámaras, teléfono, etc., se pueden comunicar entre ellos pudiendo enviar diferente información o datos, también todos los dispositivos que estén conectados a ella podrán tener acceso a internet.

Dicha red se puede utilizar en diferentes lugares como lo es en casas, edificios, solo que esta red está limitada por espacio es decir es utilizada en lugares pequeños(School, 2023).

Este tipo de red es una de las más comunes, usadas en empresas y hogares, por lo tanto, tiene variedad de topologías.

Topología de red en bus.

Es cuando todos los equipos o dispositivos que se están utilizando en la red están conectados a un mismo cable, por lo tanto, la transmisión de datos o información es en línea recta, este tipo de red puede tener susceptibilidades como lo puede ser en el cable principal o interrupción de tráfico de los datos.

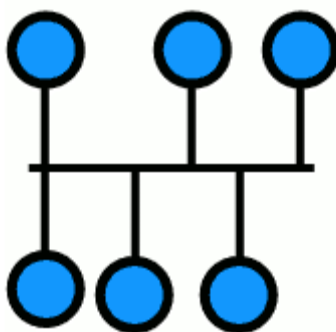


Figura 3. Topología de red en bus. recuperado de https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCZ_QJHY4i5bJrOzKKckCYOYUkEZWwrI8XxQ&usqp=CAU

Topología de red en estrella.

Es donde todos los equipos conectados en esta red se conectan a un servidor central que es el que administra los recursos y los asigna según los soliciten.

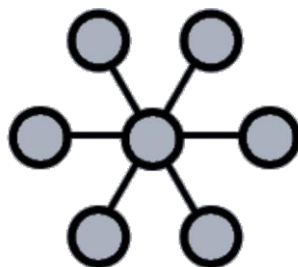


Figura 4. Topología red en estrella. recuperado de https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCZ_QJHY4i5bJrOzKKckCYOYUkEZWwrI8XxQ&usqp=CAU

Topología de red anillo.

Se entiende cuando los equipos están conectados a sus equipos vecinos con una transmisión o conexión unidireccional, esta red puede tener interrumpir las conexiones por medio de un fallo en algún nivel de esta.

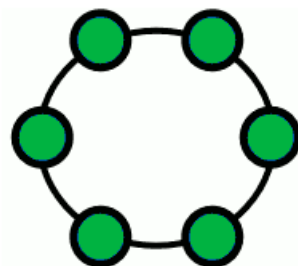


Figura 5. Topología red en anillo. recuperado de https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCZ_QJHY4i5bJrOzKKckCYOYUkEZWwrI8XxQ&usqp=CAU

Topología de red jerárquica.

Es la que más se parece a la topología de red estrella, pero la diferencia es que el acceso central es una computadora la cual controla todo el tráfico de la red.

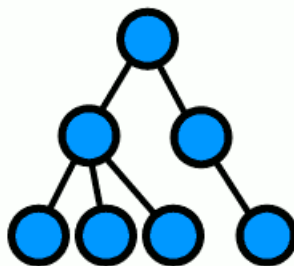


Figura 6. Topología red jerárquica recuperado de https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCZ_QJHY4i5bJrOzKKckCYOYUkEZWwrI8XxQ&usqp=CAU

Topología de red malla.

Cada dispositivo que se encuentra en la red está conectado o tiene conexión al resto de dispositivos, y cada dato que es enviado de un dispositivo o host a otro puede tomar diferente camino o ruta, esta red no puede tener ninguna interrupción de comunicación por lo que está totalmente conectada todos con todos (Limonas, 2023).

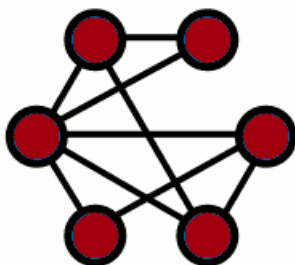


Figura 7. Topología red en malla recuperado de https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSCZ_QJHY4i5bJrOzKKckCYOYUkEZWwrI8XxQ&usqp=CAU.

Dirección IP.

Es un protocolo de internet que es el encargado de establecer la comunicación en todas las redes, la cual le asigna una dirección a cada dispositivo que se encuentra dentro de la red, es imposible que un dispositivo se pueda comunicar con otro sin tener una IP, las direcciones IP están conformadas por cuatro grupos numéricos donde cada grupo es un número de 0 a 255 y están separados por un punto, por ejemplo, 192.168.0.254 (Burdova, 2022) (Cyrille, s. f.).

Existen tres clases de direcciones IP: Clase A, Clase B y Clase C. Cada clase tiene un rango de direcciones IP que se asigna a una red en particular.

Clase A.

Las direcciones IP de Clase A tienen el primer octeto en el rango de 1 a 126. El primer octeto se utiliza para identificar la red, mientras que los tres octetos restantes se utilizan para identificar los hosts en la red. La dirección IP de Clase A puede ser utilizada para redes grandes, ya que permite un máximo de 126 redes, cada una con 16.777.214 hosts.

Clase B.

Las direcciones IP de Clase B tienen el primer octeto en el rango de 128 a 191. Los dos primeros octetos se utilizan para identificar la red, mientras que los dos octetos restantes se utilizan para identificar los hosts en la red. La dirección IP de Clase B puede ser utilizada para redes medianas, ya que permite un máximo de 16.384 redes, cada una con 65.534 hosts (Cuenca, s. f.).

Clase C.

Las direcciones IP de Clase C tienen el primer octeto en el rango de 192 a 223. Los tres primeros octetos se utilizan para identificar la red, mientras que el último octeto se utiliza para identificar los hosts en la red. La dirección IP de Clase C puede ser utilizada para redes pequeñas, ya que permite un máximo de 2.097.152 redes, cada una con 254 hosts.

VLAN (Red de área local virtual).

Se usan para dividir o agrupar la red en áreas lógicas para que un grupo de dispositivos no interrumpa en el tráfico de otro grupo de dispositivos, estos grupos de dispositivos se crean dependiendo de qué parámetros se quiere para cada grupo (*IPv4 - Clases de direcciones*, s. f.).

Beneficios de las VLAN

Las VLAN (Redes de Área Local Virtuales) ofrecen varios beneficios para las organizaciones y redes empresariales, entre ellos se encuentran:

Mayor seguridad: las VLAN permiten aislar y separar el tráfico de la red en diferentes segmentos, lo que ayuda a prevenir la propagación de ataques de seguridad y evita que los usuarios no autorizados accedan a recursos críticos de la red.

Mayor eficiencia de red: las VLAN permiten segmentar el tráfico en la red, lo que puede mejorar el rendimiento y la eficiencia de la red al reducir el tráfico de difusión y aumentar el ancho de banda disponible para los usuarios (*info@citel*, s. f.).

Mayor flexibilidad: las VLAN permiten a los administradores de red mover dispositivos y usuarios de una red a otra sin tener que reconfigurar la topología física de la red, lo que facilita la administración y el mantenimiento de la red.

Mejora de la gestión de la red: las VLAN permiten a los administradores de red agrupar dispositivos y usuarios en función de la función, ubicación o departamento, lo que facilita la gestión de la red y la solución de problemas.

Reducción de costos: las VLAN pueden reducir los costos de infraestructura de red al permitir que varios departamentos compartan la misma red física, lo que reduce la necesidad de comprar y mantener múltiples switches de red (De Admin, 2017).

DHCP.

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite la configuración dinámica de direcciones IP y otros parámetros de red para dispositivos en una red local.

DHCP funciona mediante un servidor DHCP, que asigna direcciones IP y otros parámetros de red a los dispositivos de la red automáticamente, en lugar de que los dispositivos tengan que ser configurados manualmente. El servidor DHCP mantiene un grupo de direcciones IP disponibles en la red, y cuando un dispositivo se conecta a la red, solicita una dirección IP al servidor DHCP. El servidor DHCP luego asigna una dirección IP disponible al dispositivo y también puede proporcionar otros parámetros de red como la dirección del servidor DNS y la puerta de enlace predeterminada (Arguelles, 2023).

DHCP utiliza un proceso de cuatro etapas para asignar una dirección IP a un dispositivo: descubrimiento, oferta, solicitud y confirmación. En la etapa de descubrimiento, el dispositivo busca un servidor DHCP disponible enviando un mensaje de solicitud de descubrimiento. En la etapa de oferta, el servidor DHCP responde con una oferta de una dirección IP disponible. En la etapa de solicitud, el dispositivo solicita la dirección IP ofrecida y otros parámetros de red. Finalmente, en la etapa de confirmación, el servidor DHCP confirma la dirección IP al dispositivo y actualiza su tabla de direcciones IP.

DHCP es ampliamente utilizado en redes locales y es especialmente útil para redes grandes donde la configuración manual de direcciones IP sería tediosa y propensa a errores. DHCP permite la asignación dinámica de direcciones IP y simplifica la administración de la red al eliminar la necesidad de configurar manualmente cada dispositivo en la red (Parada, 2023).

Base de datos

Las bases de datos son una herramienta esencial para la gestión de la información en las empresas. Una base de datos es un conjunto de datos organizados en un formato específico que permite su acceso y manipulación de manera eficiente (*Usos y herramientas de las bases de datos para las empresas* | Cámara de España, s. f.).

En las empresas, las bases de datos se utilizan para almacenar información sobre clientes, proveedores, empleados, productos, transacciones, entre otros datos relevantes para la operación y toma de decisiones del negocio. La gestión adecuada de una base de datos permite a las empresas obtener información valiosa y útil para mejorar la eficiencia y efectividad de sus operaciones (SL, 2021).

Algunas de las ventajas de tener una base de datos en las empresas son:

- Facilita la gestión y organización de la información
- Permite un acceso rápido y eficiente a la información
- Proporciona información valiosa para la toma de decisiones
- Mejora la eficiencia y efectividad de las operaciones
- Facilita la generación de informes y estadísticas
- Ayuda a evitar errores y duplicidad de información

Es importante que las empresas implementen medidas de seguridad adecuadas para proteger la información almacenada en la base de datos, como el uso de contraseñas seguras, cifrado de datos sensibles y limitar el acceso a la información solo a las personas autorizadas (Bucher, 2022).

Medidas de seguridad

Existen diversas medidas de seguridad que las empresas pueden implementar para proteger su base de datos y la información almacenada en ella. Algunas de estas medidas son:

- Control de acceso: limitar el acceso a la base de datos solo a las personas autorizadas, mediante la asignación de permisos de acceso y la creación de roles y perfiles de usuarios.

- Contraseñas seguras: exigir el uso de contraseñas seguras, que incluyan caracteres especiales, números y letras mayúsculas y minúsculas.
- Cifrado de datos sensibles: utilizar técnicas de cifrado para proteger los datos sensibles, como información financiera o datos personales de clientes o empleados.
- Actualizaciones y parches: mantener la base de datos actualizada con las últimas versiones y parches de seguridad, para evitar vulnerabilidades y exploits.
- Copias de seguridad: realizar copias de seguridad periódicas de la base de datos, para poder recuperar la información en caso de pérdida o daño.
- Auditorías de seguridad: realizar auditorías regulares de seguridad para detectar posibles vulnerabilidades y mejorar los sistemas de seguridad.
- Firewalls y sistemas de detección de intrusiones: utilizar firewalls y sistemas de detección de intrusiones para proteger la red y la base de datos de ataques externos.
- Capacitación del personal: capacitar al personal en medidas de seguridad básicas, como la creación de contraseñas seguras y la detección de correos electrónicos y sitios web fraudulentos (*5 consejos para mantener seguras tus bases de datos* | WeLiveSecurity, 2017) (Telcel, s. f.).

Tipos de base de datos

Existen varios tipos de bases de datos, que se clasifican según su estructura, el modelo de datos que utilizan, su capacidad de almacenamiento, su accesibilidad y su finalidad. A continuación, se describen algunos de los tipos de bases de datos más comunes (*¿Qué es una base de datos?*, s. f.):

Base de datos relacional

Es el tipo de base de datos más utilizado en la actualidad. Se basa en el modelo relacional, que organiza los datos en tablas relacionadas entre sí mediante claves primarias y foráneas. Estas bases de datos son ideales para almacenar grandes cantidades de datos y realizar consultas complejas.

Base de datos jerárquica

En este tipo de base de datos, los datos se organizan en una estructura de árbol jerárquico, donde cada registro tiene un solo padre y uno o varios hijos. Es útil para datos que tienen una estructura muy definida y jerarquizada.

Base de datos de red

Este tipo de base de datos es similar a la jerárquica, pero permite que un registro tenga varios padres y varios hijos. Es ideal para datos que tienen relaciones complejas y no se ajustan bien a una estructura jerárquica.

Base de datos orientada a objetos

En este tipo de base de datos, los datos se organizan en objetos con propiedades y métodos. Es útil para datos que tienen una estructura compleja y se benefician de la programación orientada a objetos.

Base de datos NoSQL

Este tipo de base de datos no utiliza el modelo relacional y es especialmente útil para almacenar grandes volúmenes de datos no estructurados o semiestructurados, como redes sociales o datos de sensores. Estas bases de datos son escalables y pueden manejar grandes cantidades de datos con alta velocidad de procesamiento.

Base de datos distribuida

Este tipo de base de datos se extiende a través de múltiples nodos o servidores, y permite la replicación de datos entre ellos. Es útil para entornos con múltiples sitios o ubicaciones geográficas (*Qué es un modelo de base de datos*, s. f.).

Importancia de una base de datos en el seguimiento y control de una red de comunicaciones

Una base de datos es fundamental en el seguimiento y control de dispositivos de redes por las siguientes razones:

- Registro de dispositivos: una base de datos permite mantener un registro completo de los dispositivos de red utilizados en una organización. Esto incluye información como la ubicación física, dirección IP, dirección MAC, fabricante, modelo, firmware, software, configuración y otros datos relevantes.
- Gestión de inventario: una base de datos también permite la gestión del inventario de dispositivos de red. Esto facilita la identificación de dispositivos que necesitan actualizaciones, reemplazos o reparaciones, y ayuda a garantizar que la organización tenga un inventario completo y actualizado de sus dispositivos de red.
- Monitoreo del rendimiento: una base de datos permite monitorear el rendimiento de los dispositivos de red. Esto incluye el uso del ancho de banda, la carga de trabajo, la disponibilidad, el rendimiento del servidor y otros aspectos que pueden afectar el rendimiento de la red.
- Seguridad de la red: una base de datos también permite el seguimiento y control de la seguridad de los dispositivos de red. Esto incluye el monitoreo de vulnerabilidades, la

gestión de parches, el control de acceso y otras medidas para garantizar que los dispositivos de red estén protegidos contra ataques externos e internos.

- **Mejora del rendimiento:** una base de datos también permite la identificación de oportunidades para mejorar el rendimiento de los dispositivos de red. Esto incluye la identificación de cuellos de botella, la implementación de políticas de gestión de ancho de banda y otras medidas para mejorar el rendimiento de la red.

Políticas y leyes en NY

En el Estado de Nueva York, existen varias leyes y políticas relacionadas con la seguridad y privacidad de la información. Algunas de las más importantes son:

- **Ley de Privacidad y Protección de Datos de Nueva York:** Esta ley, aprobada en 2019, establece requisitos para las empresas que recopilan datos personales de los residentes de Nueva York. Se exige a las empresas que informen a los consumidores sobre qué datos se recopilan, cómo se utilizan y se comparten, y se les da derecho a solicitar que se eliminen sus datos personales.
- **Ley de Seguridad de la Información y Notificación de Brechas de Nueva York:** Esta ley, en vigor desde 2005, establece requisitos para la protección de la información personal de los residentes de Nueva York. En caso de una brecha de seguridad, las empresas deben notificar a los consumidores afectados y a la fiscalía general de Nueva York.
- **Reglamento General de Protección de Datos (RGPD):** El RGPD es una ley de la Unión Europea que se aplica a las empresas que recopilan y procesan datos personales de los ciudadanos de la UE. Si una empresa con sede en Nueva York recopila datos de ciudadanos de la UE, debe cumplir con los requisitos del RGPD.

- Ley de Protección del Consumidor de Nueva York: Esta ley, aprobada en 2011, establece requisitos para las empresas que recopilan información personal de los consumidores de Nueva York. Las empresas deben notificar a los consumidores sobre qué información se recopila y cómo se utiliza, y se les da derecho a optar por no participar.
- Ley de Protección de Información Personal de Nueva York: Esta ley, en vigor desde 2017, establece requisitos para la protección de la información personal de los residentes de Nueva York. Las empresas deben tomar medidas razonables para proteger la información personal de los consumidores, y en caso de una brecha de seguridad, deben notificar a los consumidores afectados y a la fiscalía general de Nueva York.

En general, estas leyes y políticas establecen requisitos para la protección de la información personal de los residentes de Nueva York y para la notificación en caso de una brecha de seguridad. Las empresas que operan en Nueva York deben cumplir con estas leyes y políticas para proteger la privacidad y seguridad de los consumidores (*Política de privacidad | City of New York, s. f.*).

Desarrollo

Reconocimiento de la red

En este paso lo que se desea observar y analizar es la red de la empresa ocean restoration & construction corp, que topología tiene la red de que consta o que dispositivos consta. Para posteriormente dar mantenimiento dar solución a los Problemas en la red.

Nombre	Address	Hardware Addr	Interface	Fabricante	Dispositivo
sep503de5e95a2b.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Telefono
sep503de5e9243d.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Telefono
sep503de5e95a80.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Telefono
dtm-cmr-pt01.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Dell Inc	Computador
sep503de5e9572d.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Telefono
sep503de5e957c0.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Telefono
ap-dtm-p2.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Access Point
crv-dtm-pc01.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Micro-Star INT'L CO., LTD	Computador
pc2412.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Micro-Star INT'L CO., LTD	Computador
dtm-dst-pc04.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Dell Inc	Computador
dtm-dst-pc02.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Wistron Infocomm (Zhongshan) Corporation	Computador
dtm-cmr-pc08.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Dell Inc	Computador
DUITAMA	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Hewlett Packard	Computador
dtm-atc-pc04	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Dell Inc	Computador
ap-dtm-p1.ebsa.local	10.0.0.0	xxxx.xxxx.xxxx.xxxx	Vlan1	Cisco Systems, Inc	Access Point

Figura 8. Escaneo de la red actual **.

Definición de dispositivos

En este paso se desea saber cuántos dispositivos se puede encontrar y que tipos de dispositivos, para así poder configurar nuevos puntos de acceso.

Este proceso se piensa realizar con el software gratuito Advanced IP Scanner (AIS) donde este escáner el servicio que presta es confiable. Ya que AIP puede escanear redes locales y remotas, y puede proporcionar información detallada sobre cada dispositivo, incluyendo su dirección IP, nombre del host, fabricante, modelo y tipo de dispositivo.

AIS tiene varias características útiles, como la capacidad de apagar los equipos de forma remota, la integración con la herramienta de control remoto Radmin y la capacidad de exportar los resultados del escaneo en varios formatos, incluyendo CSV y XML. También es capaz de realizar pruebas de ping y tracert para diagnosticar problemas de conexión y de red.

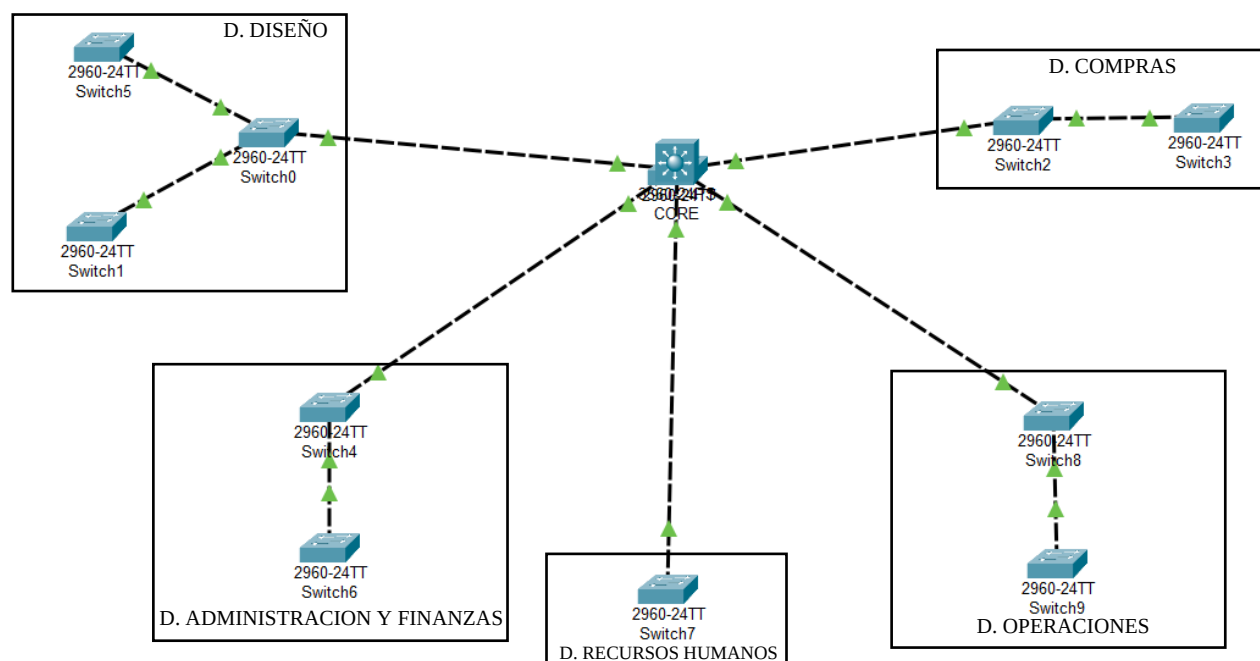


Figura 9. Estado actual de la red (elaboración propia)

Configurar puntos de red

El objetivo de la actividad es agregar nuevos puntos de red a la infraestructura existente de la empresa para satisfacer las necesidades de la organización y aumentar la eficiencia de la red. El proyecto se llevó a cabo en varias fases, como se describe a continuación:

Análisis de red: se analizó la red a detalle para comprender su estructura y topología. Se determinan los dispositivos de red utilizados, la topología de la red, las direcciones IP y los protocolos de red utilizados.

Aquí se busca que topología se encuentra en la red, se realizará el mapa lógico o físico de los dispositivos que se encuentran en ella misma. Saber la topología de la red es importante porque proporciona información sobre cómo se conectan los dispositivos de red entre sí y cómo fluye la información en la red. Esto nos permite identificar los dispositivos que forman parte de ella y cómo están conectados entre sí. De igual forma nos permite mejorar la eficiencia de la red,

detectar fallas en la red y diseñar y planificar la expansión de la red, al conocer la topología de la red existente, se puede planificar la expansión de la red de manera efectiva y diseñar una nueva topología que se adapte a las necesidades de la organización.

Nuevo diseño de red: Diseñe una nueva red, incluidos nuevos puntos de red. Se determinaron las ubicaciones de los nuevos puntos de red, la cantidad de dispositivos que se conectarán a la red y la topología de la nueva red.

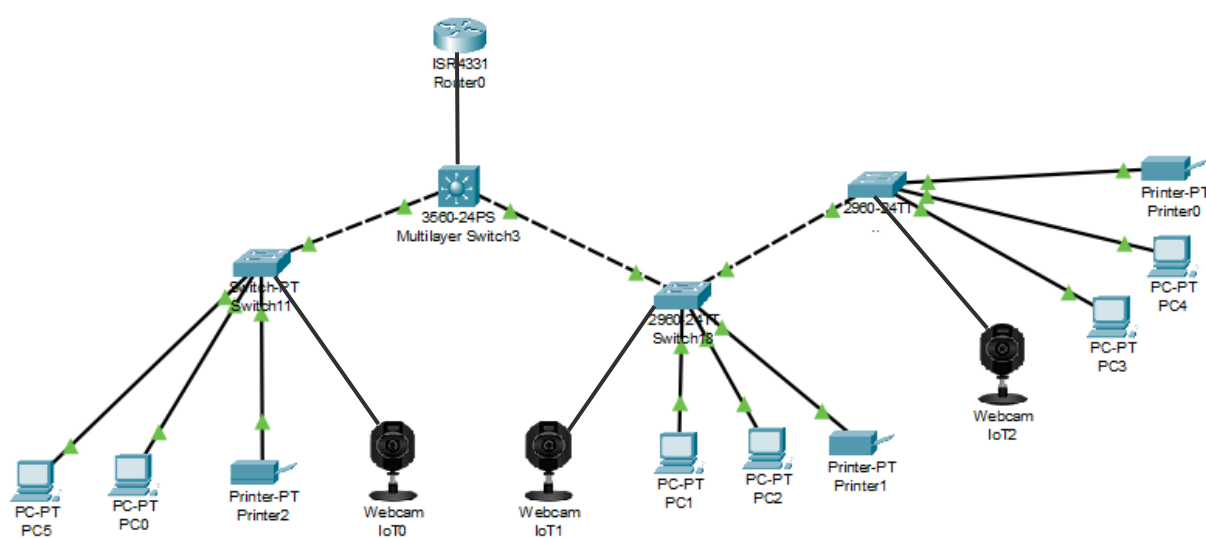


Figura 10. Organización de la red futura (elaboracion propia).

Selección de equipos de red: seleccione el equipo de red adecuado, como conmutadores y enrutadores. El equipo de red seleccionado es compatible con las redes existentes y está diseñado para manejar de manera eficiente el tráfico de la red.

Estado	Nombre	IP	Fabricante	Dirección MAC
>	192.168.1.1	192.168.1.1	Technology Co...	D8:1B:1F:1E:1D:1C
	192.168.1.101	192.168.1.101		52:54:00:12:34:56
	T...	192.168.1.108	ASUSTek COMPUTER I...	38:51:AB:7D:13:11

Figura 11. identificación de dispositivos **

Configuración de los nuevos puntos de red: Se configuraron los nuevos puntos de red, lo que incluyó la asignación de direcciones IP y la configuración de los protocolos de red. También se configuraron los puertos del switch para que se comunicaran con los dispositivos conectados.

```
awplus login: manager
Password:

AlliedWare Plus (TM) 5.4.6 12/15/16 01:02:33

awplus>enable
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#vlan database
awplus(config-vlan)#vlan 10 name Usuarios state enable
awplus(config-vlan)#vlan 20 name CCTV state enable
awplus(config-vlan)#exit
awplus(config)#exit
awplus#
```

Figura 12. Configuración de puntos (representativa para la configuración de puntos).

Creación de los DHCP para cada tipo de dispositivos.

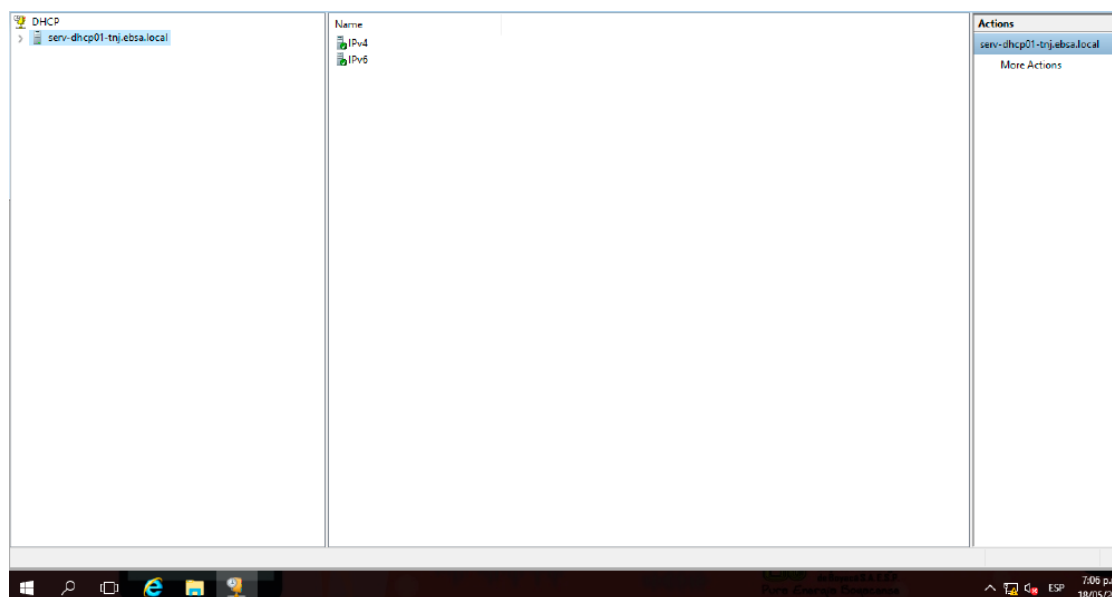


Figura 13. Conexión con el servidor DHCP

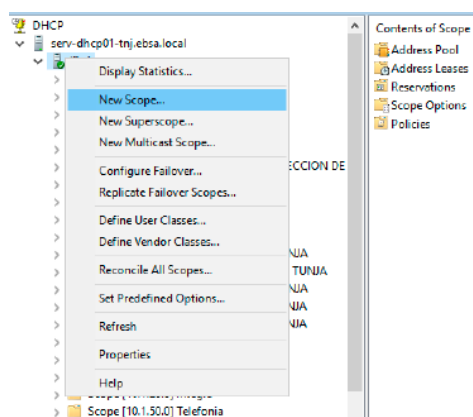


Figura 14. Creación de nuevos segmentos.

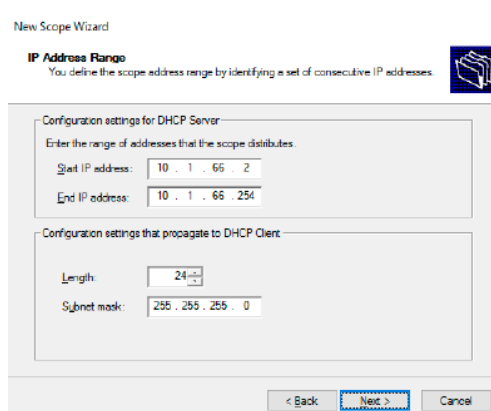


Figura 15. Definir rango de direcciones IP.

Pruebas y verificación: Se realizaron pruebas y verificaciones para asegurarse de que la nueva red estuviera funcionando correctamente. Se llevaron a cabo pruebas de conectividad de red y pruebas de velocidad de red.

Documentación: Se documentó todo el proceso de configuración de la nueva red, incluyendo los cambios realizados en la red existente y los nuevos equipos de red agregados.

Como resultado de esta actividad, se logró configurar los nuevos puntos de red en la red existente de la empresa sin interrupciones en el servicio. Además, se mejoró la eficiencia de la red y se logró una mayor capacidad para manejar el tráfico de red.

En conclusión, la configuración de nuevos puntos de red en una empresa que ya tiene una red instalada es un proceso que debe llevarse a cabo con cuidado y planificación para garantizar el éxito del proyecto. La realización de un análisis detallado de la red existente, el diseño cuidadoso de la nueva red, la selección adecuada de equipos de red, la configuración precisa de los nuevos puntos de red, las pruebas y verificaciones completas y la documentación detallada son pasos cruciales para lograr un resultado exitoso.

Supervisar y mejorar el rendimiento de la red

La actividad de supervisar y mejorar el rendimiento de la red de la empresa. En este reporte, describiré los pasos que seguí para cumplir con este objetivo.

Supervisión de la Red: En primer lugar, realicé una evaluación exhaustiva de la red para identificar cualquier problema de rendimiento. Utilicé herramientas de monitoreo de red como Wireshark y SolarWinds para analizar el tráfico de red y encontrar cuellos de botella, congestiones y otros problemas de rendimiento.

Una vez identificados los problemas de rendimiento, implementé una solución para mejorar el rendimiento de la red. Por ejemplo, si encontré que la red estaba congestionada debido a un gran número de usuarios que descargaban archivos grandes, implementé un límite de ancho de banda para limitar la cantidad de datos que cada usuario podía descargar simultáneamente.

Mejora del Rendimiento de la Red: Además de solucionar los problemas de rendimiento identificados, también realicé algunas mejoras generales en la red para mejorar su rendimiento en general. Por ejemplo, actualicé el firmware de los dispositivos de red y optimicé la configuración de la red para garantizar que se estuvieran utilizando los protocolos y algoritmos más eficientes.

También llevé a cabo pruebas de rendimiento regulares para monitorear el rendimiento de la red y asegurarme de que las mejoras implementadas estuvieran funcionando de manera efectiva. Utilicé herramientas como Ping y Traceroute para evaluar la latencia de la red y garantizar que los paquetes de datos estuvieran siendo entregados en el menor tiempo posible.

Conclusiones: En resumen, durante mi residencia profesional, supervisé y mejoré el rendimiento de la red de la empresa utilizando herramientas de monitoreo y evaluación, implementando soluciones para los problemas de rendimiento identificados y realizando mejoras generales en la red. También llevé a cabo pruebas regulares de rendimiento para monitorear el rendimiento de la red y asegurarme de que las mejoras implementadas estuvieran funcionando de manera efectiva.

Crear y mantener la documentación de la red

Durante la actividad de crear y mantener la documentación de la red de la empresa. En este informe, describiré los pasos que seguí para cumplir con este objetivo y cómo se mantuvo la documentación actualizada.

Creación de la Documentación de la Red: Para crear la documentación de la red, comencé por realizar un relevamiento de esta para obtener una vista general de la red y sus componentes. Luego, recopilé información detallada sobre cada componente, como direcciones IP, nombres de dispositivos, configuraciones, topología de red y otros detalles importantes.

Una vez que tuve toda la información necesaria, comencé a organizarla en un formato coherente y fácil de entender. Para ello, utilicé una combinación de diagramas de red, tablas y documentos de texto.

En los diagramas de red, incluí información sobre la topología de la red, las conexiones y los dispositivos de red, así como también la ubicación física de cada componente. En las tablas, incluí detalles como direcciones IP, nombres de dispositivos y otros detalles específicos de cada componente. Finalmente, en los documentos de texto, proporcioné una descripción detallada de la configuración de la red y cualquier otra información importante.

Mantenimiento de la Documentación de la Red: Para mantener la documentación de la red actualizada, es importante establecer un proceso de mantenimiento regular. Personalmente, opté por llevar a cabo las siguientes prácticas:

Actualización periódica de la documentación: Es importante establecer una rutina para actualizar la documentación de la red, al menos una vez al mes, con cualquier cambio que se haya realizado. Cada vez que se implementa un cambio en la red, se debe documentar inmediatamente.

Control de versiones: Es importante mantener un historial de versiones de la documentación para que sea fácil de rastrear los cambios realizados. Utilicé un sistema de control de versiones para gestionar la documentación de la red.

Revisión por parte del equipo de TI: Para garantizar que la documentación de la red sea precisa y completa, es importante que el equipo de TI revise regularmente la documentación y haga comentarios y sugerencias para mejorarla.

En resumen, se creó y mantuvo la documentación de la red de la empresa utilizando una combinación de diagramas de red, tablas y documentos de texto. Para mantener la documentación actualizada, establecí un proceso de actualización periódica, control de versiones y revisión por parte del equipo de TI. Esto permitió a la empresa mantener una vista clara y precisa de su red y ayudó a facilitar cualquier futura implementación de cambios en la misma.

Garantizar el Cumplimiento de las Políticas de la Red

Se describirán los pasos que seguí para cumplir con este objetivo y cómo se aseguró que la empresa cumpliera con las leyes y regulaciones de los Estados Unidos.

Garantizando el Cumplimiento de las Políticas de la Red: Para garantizar el cumplimiento de las políticas de la red, comencé por comprender completamente las políticas y los requisitos legales. Revisé las políticas y las leyes de los Estados Unidos relacionadas con la seguridad y privacidad de la información y determiné los requisitos específicos que se aplicaban a la red de la empresa.

Luego, realicé una auditoría de la red para identificar cualquier incumplimiento de las políticas y los requisitos legales. Durante esta auditoría, revisé las políticas de la empresa y sus prácticas en relación con la seguridad y la privacidad de la información, y comparé estas prácticas con los requisitos legales.

Basándome en los resultados de la auditoría, implementé medidas correctivas para garantizar que la empresa cumpliera con las políticas y los requisitos legales. Estas medidas incluyeron la actualización de las políticas de seguridad y privacidad de la información de la empresa, la implementación de nuevas medidas de seguridad en la red y la realización de capacitaciones y concientización del personal sobre las políticas y los requisitos legales.

Además, se estableció un proceso de seguimiento continuo para asegurar que la empresa mantuviera el cumplimiento de las políticas y los requisitos legales. Esto incluyó la realización de auditorías regulares de la red y el monitoreo constante de la actividad en la red para identificar cualquier posible incumplimiento.

En resumen, garantizar el cumplimiento de las políticas de la red fue de vital importancia para la empresa y para cumplir con las leyes y regulaciones de los Estados Unidos. Implementé medidas correctivas y establecí un proceso de seguimiento continuo para asegurarme de que la empresa mantuviera el cumplimiento de las políticas y los requisitos legales. Esto permitió a la empresa operar de manera segura y legal, y proteger la información de sus clientes y empleados.

Asegurar la red contra todo tipo de amenazas

En primer lugar, es importante destacar que se utilizó una combinación de medidas técnicas y políticas de seguridad para garantizar la protección de la red. Una de las medidas más importantes que se implementó fue un sistema de cortafuegos. El cortafuegos se encarga de filtrar y bloquear el tráfico no deseado, lo que minimiza las posibilidades de ataques externos a la red. Además, se configuraron adecuadamente las políticas de seguridad del cortafuegos para evitar brechas en la red. Estas políticas incluyen reglas de filtrado de tráfico, políticas de autenticación y autorización, así como reglas de acceso a recursos de la red.

Otra medida que se tomó para garantizar la seguridad de la red fue establecer protocolos de seguridad para la gestión de contraseñas y la autenticación de usuarios. Se fomentó el uso de contraseñas seguras y se realizaron cambios periódicos en las mismas. Además, se implementaron políticas de bloqueo de cuentas y limitación de acceso a los recursos de red en función de la autenticación del usuario. Esto aseguró que solo los usuarios autorizados pudieran acceder a los recursos de la red.

Además de estas medidas técnicas, también se llevó a cabo una supervisión constante de la red mediante el uso de herramientas de monitoreo y detección de intrusiones. De esta manera, se pudo identificar rápidamente cualquier actividad sospechosa y tomar medidas para evitar posibles ataques. Se utilizaron herramientas como IDS/IPS (Sistemas de Detección y Prevención de

Intrusos), SIEM (Sistema de Gestión de Eventos e Información de Seguridad) y HIDS (Sistemas de Detección de Intrusos a Nivel de Host) para supervisar y analizar la actividad de la red.

Por último, se realizaron actualizaciones periódicas de los sistemas y aplicaciones de la red. Esto permitió corregir posibles vulnerabilidades y asegurar que la red estuviera actualizada en todo momento. Las actualizaciones incluyen parches de seguridad, actualizaciones de software y firmware, y actualizaciones de la base de datos de vulnerabilidades.

En conclusión, la combinación de medidas técnicas y políticas de seguridad permitió asegurar la red contra todo tipo de amenazas. Durante mi residencia profesional, se implementaron medidas significativas para garantizar la seguridad de la red, y la supervisión constante de la actividad de la red permitió detectar y prevenir posibles amenazas. La implementación de estas medidas garantizó que la red fuera robusta y confiable, cumpliendo con los estándares de seguridad de la empresa y protegiendo los datos y la infraestructura de la red contra posibles ataques.

Creación de base de datos para el control de la red

En primer lugar, se estableció un equipo multidisciplinario que incluía especialistas en redes, administradores de bases de datos, desarrolladores y analistas de datos. Este equipo trabajó junto para definir los objetivos, los requisitos y las limitaciones del proyecto. También se establecieron los plazos y el presupuesto del proyecto.

Definición de requisitos:

Se realizaron reuniones exhaustivas para comprender en profundidad los objetivos y requisitos de la base de datos.

Se documentaron las necesidades específicas en términos de datos a almacenar, operaciones a realizar y requisitos de rendimiento y seguridad.

Selección del sistema de gestión de bases de datos (SGBD):

Se llevaron a cabo investigaciones y análisis comparativos de diversos SGBD disponibles en el mercado.

Tras un análisis detallado, se seleccionó MySQL como la solución más adecuada para el proyecto, considerando aspectos como escalabilidad, rendimiento, seguridad y compatibilidad con el entorno existente.

Se justifico el uso del gestor de bases de datos MySQL en función de sus características y beneficios:

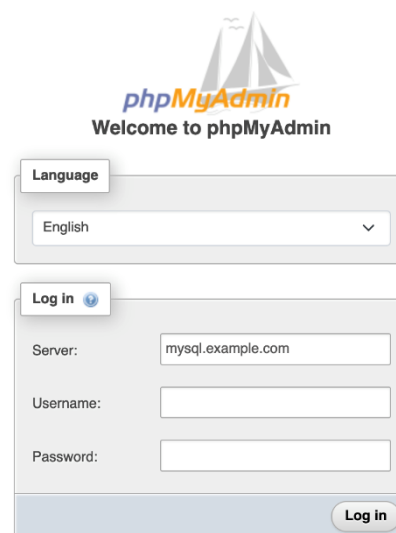


Figura 16. Primera pantalla del SGBD.

Amplia adopción y comunidad activa: MySQL es uno de los sistemas de gestión de bases de datos más populares y ampliamente utilizados en el mundo. Esto significa que existe una gran comunidad de usuarios y desarrolladores que brindan soporte, comparten conocimientos y contribuyen al crecimiento y mejora continua del sistema.

Escalabilidad y rendimiento: MySQL ofrece un rendimiento excepcional y es capaz de manejar grandes volúmenes de datos y cargas de trabajo intensivas. Puede escalar tanto verticalmente (agregando más recursos a un servidor) como horizontalmente (distribuyendo la carga en múltiples servidores).

Versatilidad y compatibilidad: MySQL es compatible con múltiples sistemas operativos, lo que lo hace flexible y adaptable a diferentes entornos. Además, es compatible con diversos lenguajes

de programación y tecnologías, lo que facilita la integración con otras aplicaciones y herramientas.

Seguridad: MySQL ofrece una amplia gama de características de seguridad, como encriptación de datos, autenticación avanzada, gestión de usuarios y privilegios, auditoría de eventos y más. Estas características ayudan a proteger la integridad y confidencialidad de los datos almacenados en la base de datos.

Estabilidad y confiabilidad: MySQL ha demostrado ser una opción estable y confiable para entornos de producción durante muchos años. Ha sido ampliamente probado y utilizado en aplicaciones de misión crítica en diversos sectores, lo que demuestra su robustez y capacidad para manejar cargas de trabajo exigentes.

Costo: MySQL es una opción de código abierto, lo que significa que es gratuito para su uso y distribución. Esto puede resultar beneficioso en términos de costos, especialmente en comparación con sistemas de gestión de bases de datos comerciales.

En resumen, se utilizó el gestor de bases de datos MySQL debido a su amplia adopción, escalabilidad, rendimiento, versatilidad, compatibilidad, seguridad, estabilidad y costo efectivo.

Diseño del modelo de datos:

Se realizó un análisis exhaustivo de los requisitos y se elaboró un modelo de datos detallado utilizando el enfoque del Modelo Entidad-Relación (MER).

Se identificaron las entidades principales, atributos y relaciones entre los datos para representar de manera precisa y lógica la estructura de la base de datos.

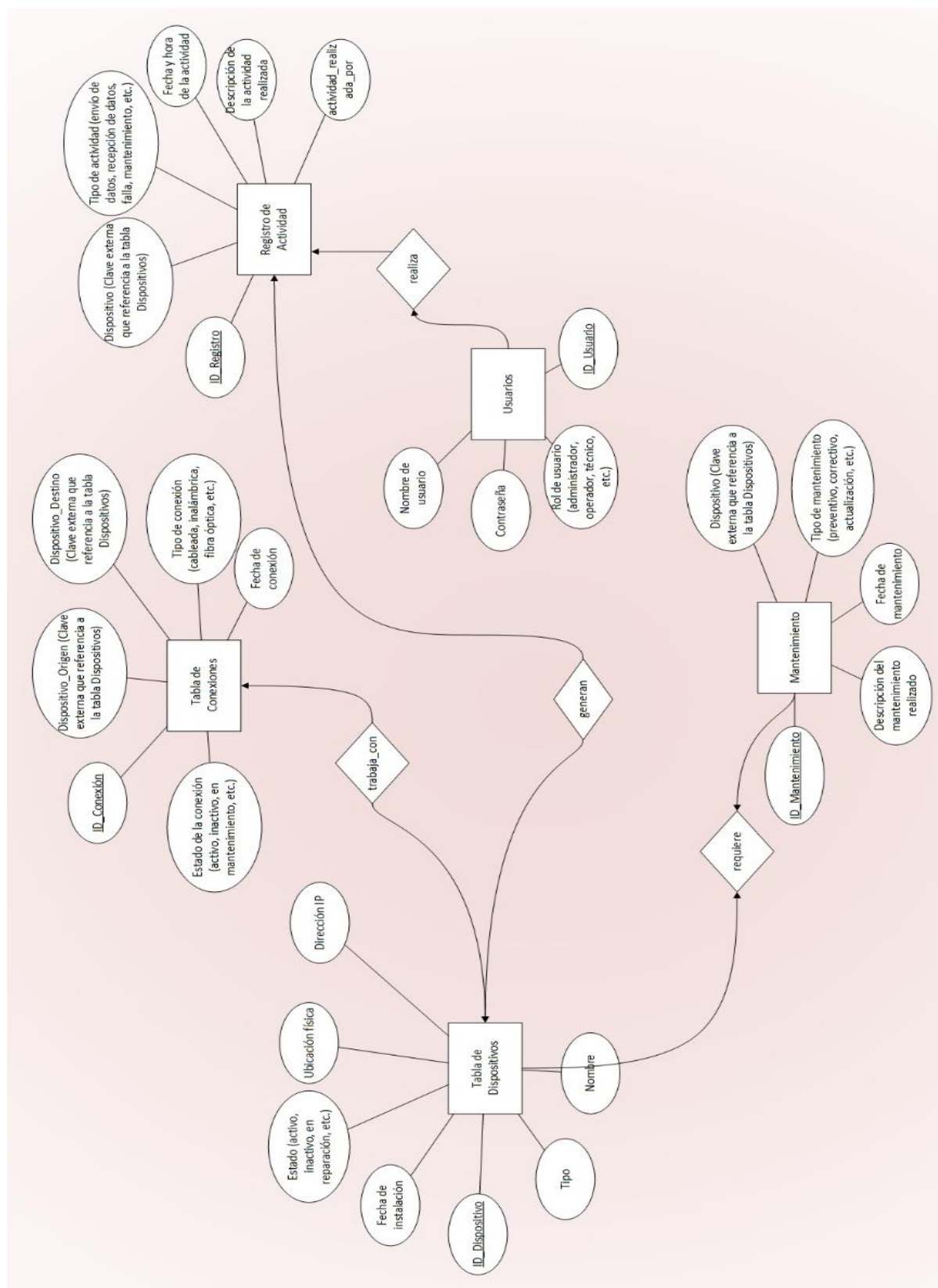


Figura 17. Primera propuesta para la BD (elaboración propia).

Creación de las tablas y definición de los campos:

Utilizando el lenguaje SQL proporcionado por MySQL, se crearon las tablas necesarias en la base de datos.

Se definieron cuidadosamente los campos de cada tabla, incluyendo el tipo de datos, la longitud, las restricciones de integridad y las claves primarias, de acuerdo con los requisitos establecidos.

Para esto se hicieron unas modificaciones a la propuesta inicial.

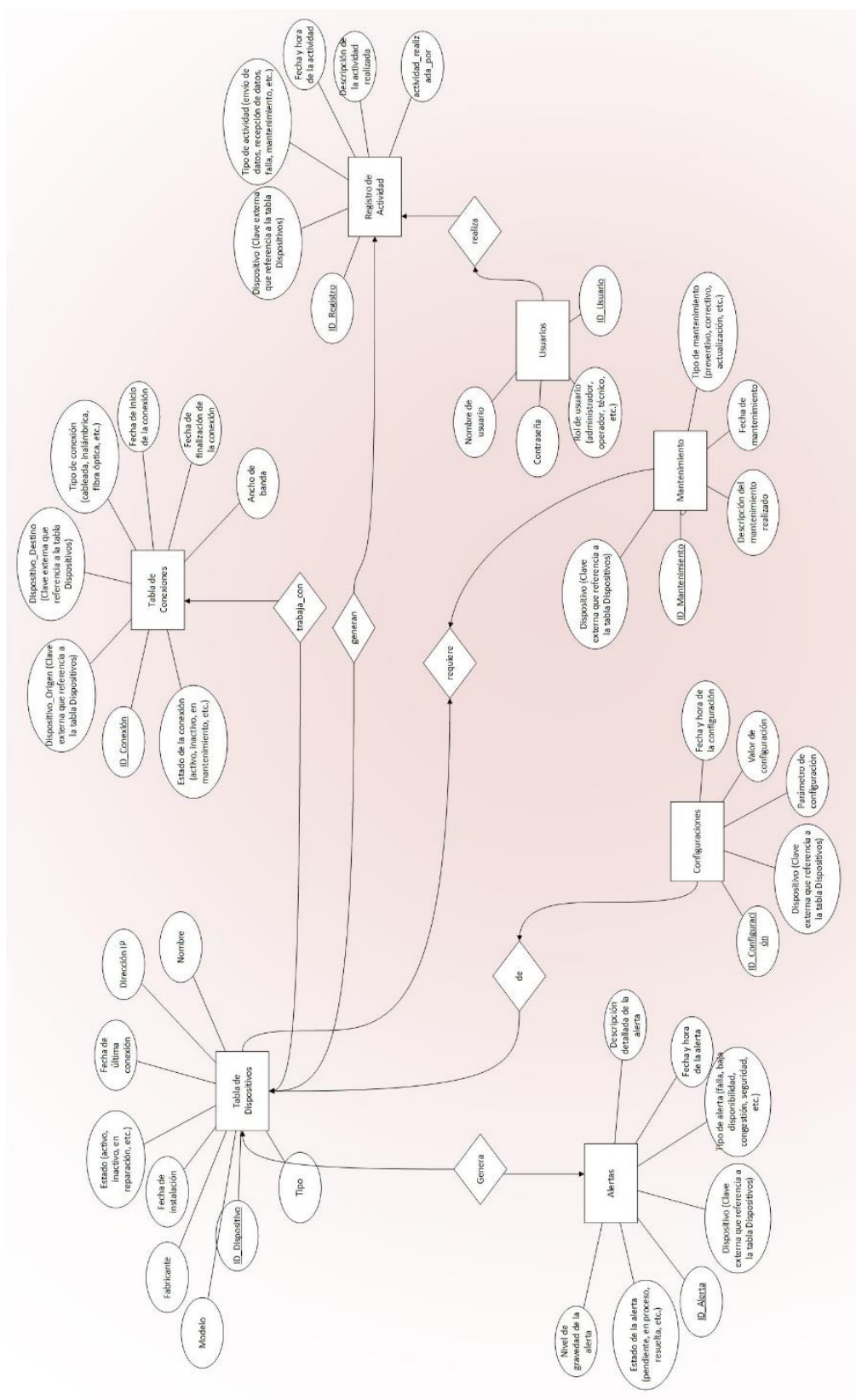


Figura 18. Propuesta final para la BD (elaboración propia).

Establecimiento de relaciones entre las tablas:

Se establecieron las relaciones entre las tablas mediante el uso de claves primarias y claves externas (claves foráneas).

Se garantizó la integridad referencial al asegurar que los valores en las claves externas hicieran referencia a registros válidos en las tablas relacionadas.

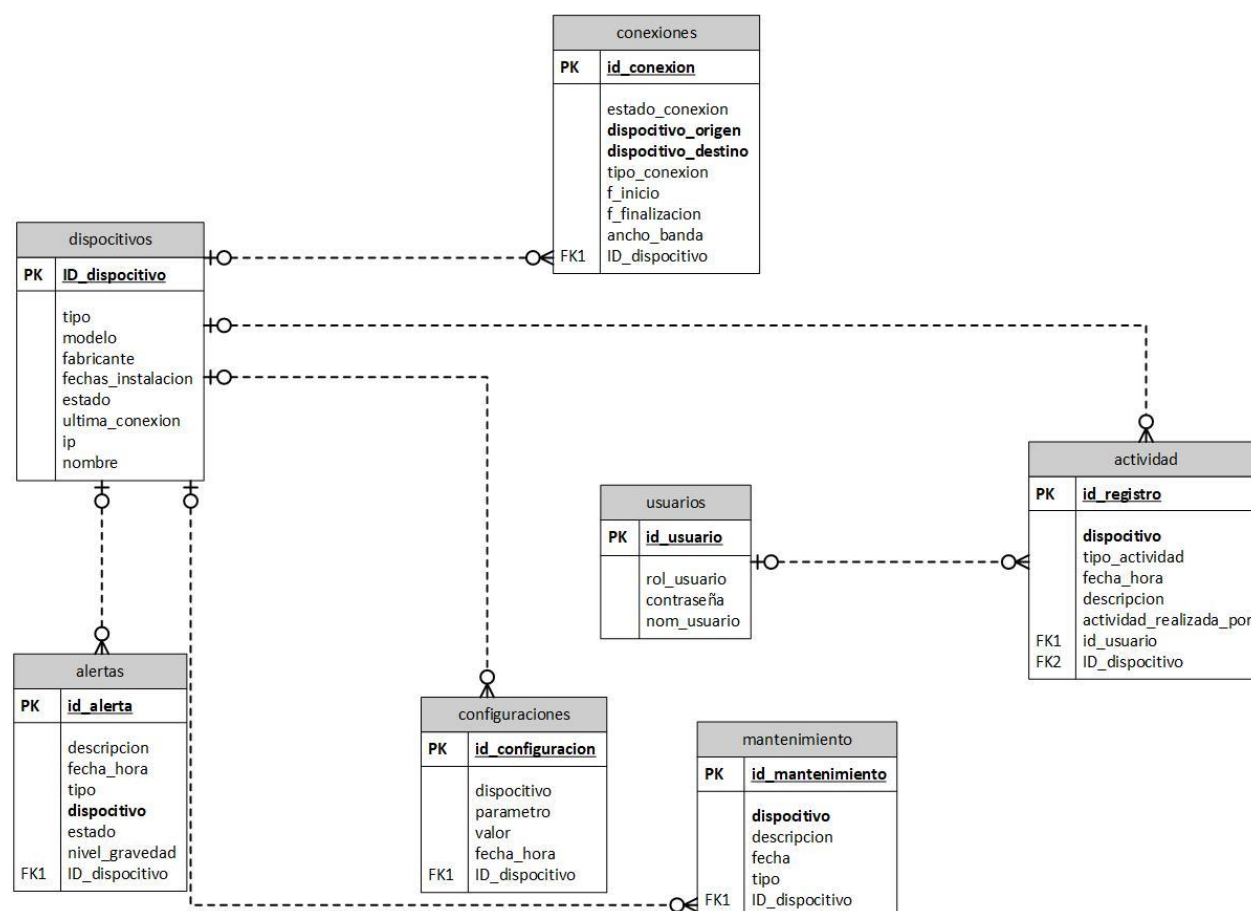


Figura 19. Modelo relacional (elaboración propia).

Creación de tablas: La creación de una tabla implica definir su estructura y las columnas que la componen. Se utiliza el comando CREATE TABLE para crear una nueva tabla en MySQL. Se debe especificar el nombre de la tabla y las columnas junto con sus tipos de datos y restricciones si es necesario.

```
CREATE TABLE nombre_tabla (
    columna1 int,
    columna2 int,
    ...
);
```

Figura 20. código de creación de tablas.

Tabla	Acción
☐ actividad	★ Examinar Estructura Buscar Insertar Vaciar E
☐ alertas	★ Examinar Estructura Buscar Insertar Vaciar E
☐ conexiones	★ Examinar Estructura Buscar Insertar Vaciar E
☐ configuraciones	★ Examinar Estructura Buscar Insertar Vaciar E
☐ dispositivos	★ Examinar Estructura Buscar Insertar Vaciar E
☐ mantenimiento	★ Examinar Estructura Buscar Insertar Vaciar E
☐ usuarios	★ Examinar Estructura Buscar Insertar Vaciar E
7 tablas	Número de filas

Figura 22. tablas creadas en la BD.

<code>SELECT * FROM `actividad`</code> ☐ Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]
id_registro dispositivo tipo_act fecha descripcion act_realizada_por id_usuario id_dispositivo
<code>SELECT * FROM `alertas`</code> ☐ Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]
id_alerta descripcion fecha tipo dispositivo estado nivel_gravedad id_dispositivo
<code>SELECT * FROM `conexiones`</code> ☐ Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]
id_conexion estado_conexion dispositivo_origen dispositivo_destino tipo_conexion f_inicio f_finalizacion ancho_banda id_dispositivo
<code>SELECT * FROM `configuraciones`</code> ☐ Perfilando [Editar en línea] [Editar] [Explicar SQL] [Crear código PHP] [Actualizar]
id_config dispositivo parametro valor fecha id_dispositivo

Figura 21. visualización de las filas de cada tabla.

```
ALTER TABLE `mantenimiento`
  DROP PRIMARY KEY,
  ADD PRIMARY KEY(
    `dispositivo`
  );
```

Figura 23. Asignación de llaves primarias.

```
ALTER TABLE `configuraciones` ADD UNIQUE(`id_dispositivo`);
```

Figura 24. asignación de llaves foráneas.

	#	Nombre	Tipo
☐	1	id_manten 	int
☐	2	dispositivo	varchar(50)
☐	3	descripcion	varchar(45)
☐	4	fecha	date
☐	5	tipo	varchar(46)
☐	6	id_dispositivo 	varchar(25)

Figura 25. llaves primarias y foráneas asignadas.

Una vez creada la tabla, puedes realizar diversas operaciones para manipularla.

```
INSERT INTO nombre_tabla (columna1, columna2, ...)
VALUES (valor1, valor2, ...);
```

Figura 26. Código para insertar datos.



Figura 27. inserción de datos genéricos en la BD.

Definición de restricciones y validaciones:

Se establecieron restricciones y validaciones para garantizar la integridad y coherencia de los datos almacenados.

Se implementaron restricciones de unicidad, restricciones de integridad referencial, restricciones de verificación y otras restricciones necesarias según los requisitos.

A continuación, se detallan las acciones llevadas a cabo:

Análisis de requisitos:

Se revisaron los requisitos funcionales y no funcionales establecidos para el sistema de base de datos.

Se identificaron las restricciones y validaciones necesarias para cumplir con los requisitos y asegurar la calidad de los datos.

Restricciones de integridad referencial:

Se definieron las relaciones entre las tablas de la base de datos y se establecieron las restricciones de integridad referencial.

Se implementaron las claves primarias y claves externas para asegurar que los datos relacionados se mantengan consistentes en todas las tablas.

Restricciones de unicidad:

Se identificaron los campos que deben ser únicos en la base de datos y se establecieron restricciones de unicidad en esos campos.

Esto asegura que no se puedan almacenar duplicados en la base de datos y mantiene la consistencia de los datos.

Validaciones de datos:

Se definieron validaciones para garantizar la precisión y coherencia de los datos ingresados en la base de datos.

Se utilizaron restricciones de verificación, como comprobaciones de rangos, formatos de datos, valores permitidos, entre otros, según los requisitos específicos del proyecto.

Actualización de la estructura de la base de datos:

Se realizaron modificaciones en la estructura de la base de datos para incluir las restricciones y validaciones definidas.

Esto implicó la actualización de los esquemas de las tablas, la adición de restricciones y la modificación de los procedimientos almacenados, si fuera necesario.

Pruebas de validación:

Se llevaron a cabo pruebas exhaustivas para verificar el correcto funcionamiento de las restricciones y validaciones implementadas.

Se realizaron pruebas de inserción, actualización y eliminación de datos, asegurando que las restricciones se apliquen correctamente y los datos cumplan con las validaciones establecidas.

Creación de índices:

Se identificaron las columnas que se utilizarán frecuentemente en las consultas y se crearon índices en esas columnas.

Los índices mejoran el rendimiento de las consultas al acelerar la búsqueda y recuperación de datos.

A continuación, se detallan las acciones llevadas a cabo:

Análisis de rendimiento:

Se realizó un análisis exhaustivo del rendimiento de la base de datos, identificando las consultas más frecuentes y las áreas que requerían optimización.

Se evaluaron los campos que se utilizaban con mayor frecuencia en las consultas y se identificaron los campos candidatos para la creación de índices.

Selección de campos para indexar:

Se seleccionaron los campos que eran utilizados con mayor frecuencia en las cláusulas WHERE, JOIN y ORDER BY de las consultas.

Estos campos fueron considerados como candidatos para la creación de índices, ya que su indexación podría mejorar significativamente el rendimiento de las consultas.

Tipos de índices:

Se evaluaron los diferentes tipos de índices disponibles en el sistema de gestión de bases de datos utilizado.

Se seleccionaron los tipos de índices más adecuados para cada campo, considerando factores como el tipo de datos, el tamaño de la tabla y el tipo de consultas que se realizarían.

Creación de índices:

Se procedió a crear los índices en los campos seleccionados.

Se utilizaron sentencias SQL para definir los índices y se aseguró que estuvieran correctamente configurados según las necesidades del proyecto.

Pruebas de rendimiento:

Se llevaron a cabo pruebas exhaustivas para medir el impacto de los índices en el rendimiento de las consultas.

Se compararon los tiempos de ejecución de las consultas antes y después de la creación de los índices para evaluar su efectividad.

Monitoreo y ajustes:

Se estableció un proceso de monitoreo continuo para evaluar el rendimiento de la base de datos y los índices creados.

En caso de ser necesario, se realizaron ajustes adicionales en los índices para optimizar aún más el rendimiento de las consultas.

Establecimiento de seguridad:

Se diseñó y aplicó un plan de seguridad sólido para proteger los datos almacenados en la base de datos.

Se definieron roles de usuario y se asignaron los permisos y privilegios correspondientes para garantizar un acceso adecuado y seguro a la base de datos.

A continuación, se detallan las acciones llevadas a cabo:

Análisis de riesgos:

Se realizó un análisis exhaustivo de los posibles riesgos de seguridad asociados a la base de datos, considerando aspectos como el acceso no autorizado, la pérdida de datos y la violación de la privacidad.

Se evaluaron las vulnerabilidades y amenazas potenciales, así como las posibles consecuencias de un incidente de seguridad.

Políticas de seguridad:

Se establecieron políticas y procedimientos de seguridad claros y documentados para la base de datos.

Estas políticas incluyeron aspectos como la gestión de contraseñas, el control de acceso, la auditoría de eventos, las copias de seguridad y recuperación, entre otros.

Gestión de usuarios y roles:

Se definió un esquema de gestión de usuarios y roles para controlar el acceso a la base de datos.

Se crearon cuentas de usuario individuales con privilegios adecuados, limitando el acceso solo a las funcionalidades y datos necesarios para cada usuario.

Control de acceso:

Se establecieron reglas y restricciones de acceso para garantizar que solo los usuarios autorizados puedan acceder a la base de datos.

Se implementaron medidas de autenticación, como contraseñas seguras y técnicas de cifrado, para validar la identidad de los usuarios.

Auditoría y registro de eventos:

Se implementó un sistema de auditoría para registrar y monitorear los eventos relevantes en la base de datos.

Se configuraron registros de auditoría para rastrear los intentos de acceso no autorizados, cambios en los datos y otras actividades críticas.

Protección de datos sensibles:

Se implementaron medidas de protección de datos sensibles, como la encriptación, para garantizar su confidencialidad.

Se identificaron los datos críticos y se aplicaron técnicas de encriptación adecuadas para protegerlos tanto en reposo como en tránsito.

Mantenimiento y actualizaciones:

Se estableció un programa regular de mantenimiento y actualizaciones de la base de datos para aplicar parches de seguridad y corregir posibles vulnerabilidades.

Se realizaron pruebas de seguridad periódicas para identificar y abordar posibles brechas de seguridad.

Pruebas y optimizaciones:

Se realizaron pruebas exhaustivas para verificar el correcto funcionamiento de la base de datos.

Se verificó la inserción, actualización y recuperación de datos, así como la ejecución eficiente de consultas complejas.

Se llevaron a cabo optimizaciones, como ajuste de consultas, indexación adecuada y optimización del rendimiento general de la base de datos.

A continuación, se detallan las acciones llevadas a cabo:

Pruebas de rendimiento:

Se diseñaron y ejecutaron pruebas de rendimiento para evaluar el tiempo de respuesta de las consultas, el rendimiento de inserción y actualización de datos, y el manejo de cargas de trabajo intensivas.

Se utilizaron herramientas de prueba adecuadas para simular escenarios de uso real y medir el rendimiento de la base de datos bajo diferentes condiciones.

Identificación de cuellos de botella:

Se identificaron las áreas de la base de datos que presentaban cuellos de botella o un rendimiento deficiente.

Se analizaron los registros de consulta, los tiempos de respuesta y otros indicadores para identificar las consultas, tablas o estructuras que afectaban negativamente el rendimiento.

Análisis de índices:

Se evaluaron los índices existentes y se identificaron las oportunidades de optimización.

Se revisaron los campos utilizados en las consultas más frecuentes y se crearon índices adicionales para mejorar el rendimiento de esas consultas.

Optimización de consultas:

Se revisaron y optimizaron las consultas SQL para mejorar su rendimiento.

Se realizaron ajustes en las cláusulas WHERE, JOIN y ORDER BY, y se utilizaron técnicas como la desnormalización o el uso de vistas materializadas para optimizar consultas complejas.

Configuración del sistema:

Se revisaron y ajustaron las configuraciones del sistema de gestión de bases de datos para mejorar el rendimiento.

Se realizaron cambios en los parámetros de memoria, los tamaños de caché y otros ajustes de configuración según las recomendaciones del proveedor de la base de datos.

Particionamiento de datos:

Se implementó el particionamiento de datos para mejorar la eficiencia de las consultas en tablas grandes.

Se distribuyeron los datos en múltiples particiones basadas en criterios como rangos de valores o regiones geográficas, lo que permitió una mejor segmentación y acceso a los datos.

Monitoreo y ajustes continuos:

Se estableció un proceso de monitoreo continuo para evaluar el rendimiento de la base de datos y realizar ajustes adicionales según sea necesario.

Se implementaron alertas y sistemas de seguimiento para detectar problemas de rendimiento y abordarlos de manera proactiva.

Copias de seguridad y plan de recuperación:

Se estableció un plan de copias de seguridad periódicas para asegurar la disponibilidad y protección de los datos almacenados.

Se definió un plan de recuperación en caso de fallos del sistema, que incluye procedimientos de restauración y recuperación para minimizar la pérdida de datos y garantizar la continuidad del sistema.

En conclusión, el proceso de creación de la base de datos se llevó a cabo con atención meticulosa a los requisitos establecidos y las mejores prácticas en la industria. La base de datos resultante está lista para su implementación y contribuirá de manera significativa al éxito de su proyecto.

Competencias desarrolladas

Conocimientos técnicos en redes: se aplicaron conocimientos técnicos en el diseño, implementación y configuración de la red de la empresa. Esto incluyó el diseño de la arquitectura de la red, la selección de los componentes de red adecuados, la configuración de los equipos de red, la implementación de políticas de seguridad y la configuración de firewalls y otros dispositivos de seguridad.

Solución de problemas: se aplicó la capacidad de identificar y resolver problemas relacionados con la red. Esto incluyó la capacidad de diagnosticar problemas de red, realizar pruebas y análisis, y desarrollar soluciones efectivas para solucionar los problemas.

Documentación: se aplicaron habilidades para la creación de documentación precisa y detallada de la red, incluyendo diagramas de red, manuales de usuario y políticas de seguridad. La documentación fue fundamental para garantizar una comprensión clara de la red por parte de todos los usuarios y para facilitar el mantenimiento y la resolución de problemas en el futuro.

Seguridad: se aplicaron conocimientos y habilidades para garantizar que la red de la empresa estuviera asegurada contra todo tipo de amenazas. Esto incluyó la implementación de políticas de seguridad sólidas, la configuración de firewalls y otros dispositivos de seguridad, y la supervisión constante de la red para detectar y resolver posibles vulnerabilidades.

Gestión de bases de datos: se aplicaron conocimientos y habilidades para el diseño, implementación y gestión de la base de datos utilizada para el control y mantenimiento de la red. Esto incluyó la selección del sistema de gestión de bases de datos adecuado, el diseño de la estructura de la base de datos, la implementación de un sistema de recolección de datos y la creación de informes y alertas.

Trabajo en equipo: se aplicaron habilidades para trabajar de manera efectiva en equipo, lo que incluyó la comunicación clara y efectiva, la colaboración en la resolución de problemas y la capacidad de trabajar en conjunto para lograr los objetivos del proyecto.

Conocimientos en virtualización: se aplicaron conocimientos en virtualización para crear ambientes virtuales seguros y confiables. Esto permitió crear diferentes redes virtuales para diferentes usuarios y departamentos de la empresa, garantizando la seguridad y privacidad de la información.

Planificación y organización: se aplicaron habilidades para planificar y organizar el proyecto de creación de la red y la implementación de la base de datos. Esto incluyó la elaboración de un cronograma de actividades, asignación de tareas y seguimiento de estas para garantizar la finalización del proyecto en tiempo y forma.

Monitoreo y análisis de la red: se aplicaron conocimientos y habilidades para monitorear y analizar el desempeño de la red de la empresa. Esto permitió detectar posibles fallas o amenazas y tomar medidas preventivas para evitar daños en la red y la información que en ella circula.

Soluciones innovadoras: se aplicó la creatividad y habilidades para la innovación con el fin de desarrollar soluciones innovadoras a problemas y desafíos que surgieron durante la creación de la red y la implementación de la base de datos.

Comunicación efectiva: se aplicaron habilidades de comunicación efectiva para mantener una comunicación fluida y clara con los usuarios de la red, los directivos de la empresa y otros colaboradores del proyecto.

Conocimientos de normativas y regulaciones: se aplicaron conocimientos sobre normativas y regulaciones que deben cumplirse en el sector en que se desenvuelve la empresa. Esto permitió garantizar que la red de la empresa cumpliera con todas las leyes y regulaciones pertinentes.

Análisis de riesgos: se aplicaron conocimientos y habilidades para identificar y analizar los riesgos de seguridad de la red y de la base de datos, y tomar medidas para minimizar o eliminar esos riesgos.

Conocimientos en sistemas operativos: se aplicaron conocimientos en sistemas operativos para instalar, configurar y administrar los sistemas operativos de los servidores y los dispositivos de red.

Administración de bases de datos: se aplicaron conocimientos y habilidades en administración de bases de datos para diseñar y crear la base de datos, y mantenerla actualizada y funcionando adecuadamente.

Resolución de problemas: se aplicaron habilidades para la resolución de problemas técnicos que surgieron durante la creación de la red y la implementación de la base de datos.

Conocimientos en seguridad informática: se aplicaron conocimientos en seguridad informática para diseñar e implementar medidas de seguridad para proteger la red y la base de datos contra amenazas.

Actualización y capacitación continua: se aplicó un compromiso con la actualización y capacitación continua para mantenerse al día con las nuevas tecnologías y tendencias en el área de redes y bases de datos.

La creación de la red en la empresa y la implementación de la base de datos para su control y mantenimiento, implicaron la aplicación de diversas competencias y habilidades técnicas, de solución de problemas, de documentación, de seguridad, de gestión de bases de datos y de trabajo en equipo. Todo ello permitió garantizar el correcto funcionamiento de la red de la empresa y garantizar su seguridad en todo momento.

Fuentes de información

Daniel, P., (2018). Redes CISCO: Curso práctico de formación para la certificación CCNA, Bogotá, Colombia: Alfaomega RC Libros.

Matías, K., (2013). Redes y seguridad, Buenos aires, Argentina: Alfaomega.

Bob, V., Rick, G., (2009). Acceso a la WAN, Madrid, España: Person Educación S.A.

Acerca de Redes Virtuales de Área Local (VLAN). (s. f.).

https://www.watchguard.com/help/docs/fireware/12/es-419/Content/es-419/networksetup/vlans_about_c.html

Anmeran, A. (2017, 11 enero). *4.Normas y estándares*. Instalación y mantenimiento de redes para transmisión de datos. <https://cableadoestructuradosasel.tech.blog/2017/01/11/4-normas-y-estandares/>

¿Cuáles son las medidas de la seguridad de red? (s. f.). Trend Micro.

https://www.trendmicro.com/es_es/what-is/network-security/network-security-measures.html

De Luz, S. (2023, 1 mayo). Qué es el DHCP, funcionamiento y ejemplos de configuración.

RedesZone. <https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>

Política de privacidad. (s. f.). New York State Attorney General. <https://es.ag.ny.gov/privacy-policy>

Política de privacidad | Ayuda | Oficina de Servicios a la Infancia y la Familia. (s. f.).

<https://es.ocfs.ny.gov/help/privacy-policy.php>

Política de privacidad (Privacy Policy) revisada de la Biblioteca Pública de Nueva York. (s. f.).

The New York Public Library. <https://www.nypl.org/help/about-nypl/legal-notices/privacy-policy/es>

Posey, B. (2021). Privacidad de datos, seguridad de datos y protección de datos.

ComputerWeekly.es. <https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos>

¿Qué es la gestión de la nube? (s. f.). <https://www.redhat.com/es/topics/cloud-computing/what-is-cloud-management>

¿Qué es una base de datos? (s. f.). <https://www.oracle.com/mx/database/what-is-database/>

Rangos y Clases de la IP - Redes de Comunicación en la UDI. (s. f.).

<https://sites.google.com/site/redesdecomunicacionenlaudi/rangos-y-clases-de-la-ip>

Tablado, F. (2020). Bases de datos. ¿Qué son? Tipos y ejemplos. *Ayuda Ley Protección Datos*.

<https://ayudaleyprotecciondatos.es/bases-de-datos/>

5 consejos para mantener seguras tus bases de datos | WeLiveSecurity. (2017, 5 septiembre).

WeLiveSecurity. <https://www.welivesecurity.com/la-es/2017/09/05/consejos-bases-de-datos-seguras/>

Arguelles, G. T. (2023, 30 abril). ¿Qué es DHCP? ¿Cómo Funciona? Ventajas. *Access Quality -*

Líderes en Servicios TI y SOC y NOC. <https://www.accessq.com.mx/que-es-dhcp/>

Bucher, R. (2022). Bases de datos - 5 ventajas sobre las tablas simples. *SeaTable*.

<https://seatable.io/es/vorteile-datenbank/>

Burdova, C. (2022). ¿Qué es una dirección IP y cómo funciona? *¿Qué es una dirección IP y*

cómo funciona? <https://www.avg.com/es/signal/what-is-an-ip-address>

Calderon, C., & Calderon, C. (2021, 13 enero). ¿Qué tipos de mantenimiento de Redes existen? -

Empresa de Mantenimiento de Computadores. *Empresa de Mantenimiento de*

Computadores -. <https://plotandesign.net/mantenimiento-de-redes/tipos-de-mantenimiento-de-redes.html>

Cuenca, F. A. (s. f.). *Operacion y Administracion de Redes TCP/IP bajo Unix: Direcciones IP*.

<https://www.investigacion.frc.utn.edu.ar/labsis/publicaciones/admintcp/direcciones-ip.html>

Cyrille. (s. f.). *Dirección IP - Mi IP - Localiza una dirección IP*. MON-IP. [https://www.mon-](https://www.mon-ip.com/es/mi-ip/)

[ip.com/es/mi-ip/](https://www.mon-ip.com/es/mi-ip/)

De Admin, V. T. L. E. (2017, 1 mayo). *BENEFICIOS DE LAS REDES VLAN*. Interpolados.

<https://interpolados.wordpress.com/2017/05/01/beneficios-de-las-redes-vlan/>

Estándares para la comunicación industrial - Comunicaciones Industriales - Logitek. (2015, 18

mayo). *Comunicaciones Industriales - Logitek*.

<https://www.comunicacionesindustrialeslogitek.com/servicios/estandares-comunicacion-industrial/>

info@citel. (s. f.). https://www.oas.org/en/citel/infocitel/2008/junio/inictel_e.asp

IPv4 - Clases de direcciones. (s. f.).

https://www.tutorialspoint.com/es/ipv4/ipv4_address_classes.htm

Limones, E. (2023, 12 abril). Qué son las redes informáticas y qué tipos existen.

OpenWebinars.net. <https://openwebinars.net/blog/que-son-las-redes-informaticas-y-que-tipos-existen/>

Los 4 tipos de mantenimiento de software: ¿qué es el mantenimiento de software? (s. f.).

<https://cpl.thalesgroup.com/es/software-monetization/four-types-of-software-maintenance>

Parada, M. (2023, 14 abril). Qué es un Servidor DHCP. *OpenWebinars.net*.

<https://openwebinars.net/blog/que-es-un-servidor-dhcp/>

Política de privacidad | City of New York. (s. f.). <https://www.nyc.gov/home/privacy-policy-espanol.page>

Qué es un modelo de base de datos. (s. f.). Lucidchart. <https://www.lucidchart.com/pages/es/que-es-un-modelo-de-base-de-datos>

¿Qué es una base de datos? (s. f.). <https://www.oracle.com/mx/database/what-is-database/>

School, T. (2023). ¿Qué tipos de redes informáticas existen? *Tokio School*.

<https://www.tokioschool.com/noticias/tipos-redes-informaticas/>

SL, C. (2021, 24 febrero). ▷*La importancia de las bases de datos para las empresas -*

Coregistros. Coregistros. <https://www.coregistros.com/la-importancia-de-las-bases-de-datos-para-las-empresas/>

Telcel. (s. f.). *Medidas de seguridad para proteger información* | Telcel Empresas.

<https://www.telcel.com/empresas/tendencias/notas/medidas-seguridad-proteger-informacion-negocio>

Usos y herramientas de las bases de datos para las empresas | Cámara de España. (s. f.).

Cámara de España. <https://www.camara.es/blog/innovacion-y-competitividad/usos-herramientas-bases-datos-empresas>

Anmeran, A. (2017, 11 enero). *4. Normas y estándares*. Instalación y mantenimiento de redes para transmisión de datos. <https://cableadoestructuradosasel.tech.blog/2017/01/11/4-normas-y-estandares/>