INSTRUMENTO DE EVALUACIÓN

1. DATOS GENERALES

Programa de formación	Gestión de redes de datos
Proyecto formativo	Planeación, implementación y gestión de infraestructura informática en el sector Mipyme para la mejora de la productividad, desarrollo e innovación.
Fase proyecto	Evaluación
Resultado de aprendizaje	**220501106-03** - Verificar el funcionamiento de dispositivos de cómputo y servicios de red de acuerdo a políticas de la organización.
Actividad de aprendizaje	**GA9-220501106-AA1** - Validar servicios implementados, teniendo definidas las necesidades, utilizando diferentes herramientas de testeo y criterios de evaluación.
Evidencia de producto	Informe sobre detección de fallos en el rendimiento y operación de la solución. **GA9-220501106-AA1-EV01.**

Criterios de evaluación

- Realiza pruebas de funcionamiento de los servicios de infraestructura, plataformas y aplicaciones instalados según el diseño establecido
- Verifica el desempeño de la solución desplegada según los niveles de operación acordados en la solución.
- Identifica fallos en el rendimiento y operación de la solución con base en los niveles de operación acordados.

2. RÚBRICA

Criterios	Excelente	Bueno	Deficiente	Total
Estructura del informe	El documento contiene una excelente presentación, se entrega en el	Aunque el documento presenta una estructura base, la misma carece de	No tuvo en cuenta las normas básicas para la presentación del trabajo.	

INSTRUMENTO DE EVALUACIÓN

Criterios	Excelente	Bueno	Deficiente	Total
	formato adecuado con todo lo solicitado.	algunos elementos del cuerpo solicitado.		
Máximo 5 puntos	**5 puntos**	**2 puntos**	**0 puntos**	
Fines de la actividad	El documento da respuesta a todos los requerimientos de las actividades propuestas de acuerdo a lo solicitado en la guía. Los aportes por parte del aprendiz son significativos.	El documento da respuesta a la mayoría de los requerimientos de las actividades propuestas de acuerdo a lo solicitado en la guía. Los aportes por parte del aprendiz son importantes, pero podría mejorar su proceso de apropiación.	El documento no da respuesta a los requerimientos de las actividades propuestas.	
Máximo 60 puntos	**60 puntos**	**30 puntos**	**0 puntos**	
Aprendizajes obtenidos	Se identifica una reflexión acerca de los aprendizajes obtenidos durante la sesión de trabajo.	Se identifican ideas vagas que permiten ver algunos de los aprendizajes que se obtuvo durante la sesión de trabajo.	En ningún apartado o momento se identifican los aprendizajes dentro del proceso de las actividades durante la sesión de trabajo.	

INSTRUMENTO DE EVALUACIÓN

Criterios	Excelente	Bueno	Deficiente	Total
Máximo 20 puntos	**20 puntos**	**10 puntos.**	**0 puntos.**	
Ortografía, puntuación y gramática	La redacción es excelente, las ideas están correlacionadas, el texto es coherente en su totalidad. Su ortografía es adecuada.	La redacción del documento articula medianamente las ideas y no se usa conectores apropiadamente. Además, presenta: de cuatro a seis errores ortográficos o de puntuación o de cuatro a seis errores gramaticales.	El documento presenta deficiencias en redacción y errores ortográficos.	
Máximo 10 puntos	**10 puntos**	**5 puntos.**	**2 puntos.**	
Bibliografía / webgrafía	Incluye más de dos fuentes de información y las cita según las normas APA.	Incluye solo una fuente de información y la cita según las normas APA.	No cita ni utiliza fuentes de información.	
Máximo 5 puntos	**5 puntos**	**2 puntos.**	**0 puntos**	

3. EVALUACIÓN

Observaciones: El aprendiz cumple con los instrumentos de evaluación propuestos

Juicio de valor: Aprobado

***Nombre**: Jhojan stiven jaramillo.*

***Nombre:** Yuri cuervo.*

***Programa:** Gestión de Redes de Datos.*

***Ficha de caracterización:** 3118456.*

***Instructora:** Sandra Zapata.*

Solución de los 3 informes propuestos:

Evidencia GA8-220501104-AA2-EV01. Informe sobre detección de fallas en el funcionamiento de la red.

Evidencia GA8-220501107-AA1-EV01. Lista de verificación para validar parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión.

Evidencia GA9-220501106-AA1-EV01. Informe sobre detección de fallos en el rendimiento y operación de la solución.

Contenido de los Informes:

- ✓ *Topología de red para detección de fallas.*
- ✓ *Tabla de descripción de equipos de dicha topología.*
- ✓ *Resultado de las Pruebas de detección de fallas en la herramienta de simulación.*
- ✓ *Reporte Wlan-Report-Latest de un equipo de la red.*
- ✓ *Lista de verificación para validar parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión.*
- ✓ *Solución de los 5 puntos sugeridos para detección de fallas.*
- ✓ *Registro fotográfico del proceso de pruebas.*
- ✓ *Conclusiones.*
- ✓ *Bibliografías.*



Evidencia GA8-220501104-AA2-EV01. Informe sobre detección de fallas en el funcionamiento de la red.

INTRODUCCION:

En el presente informe se documenta el proceso de detección de fallas en el funcionamiento de la red de la empresa Enter Ltda., mediante la simulación de una topología de red en la herramienta GNS3 y la implementación de mecanismos de monitoreo, generación de tráfico y gestión de configuración.

El objetivo principal es evaluar el comportamiento del sistema bajo condiciones normales y anormales de operación, generando alarmas, clasificando incidentes y documentando los resultados conforme a las políticas y procedimientos establecidos para la gestión de fallas en redes empresariales.

Es decir, se analizan métricas como utilización de CPU, consumo de ancho de banda, latencia, pérdida de paquetes y generación de alarmas, clasificando los resultados como positivos o negativos según el cumplimiento de los parámetros esperados.

Asimismo, se establece un proceso estructurado de gestión de incidentes, que incluye niveles de prioridad, tiempos de respuesta, identificación única de anormalidades y registro documental en la CMDB, alineándose con buenas prácticas de administración de servicios TI y estándares de gestión.

De esta manera, el presente informe no solo evidencia la capacidad técnica para detectar y aislar fallas en una infraestructura de red simulada, sino también la aplicación de procedimientos organizacionales que fortalecen la gestión integral del servicio, garantizando trazabilidad, control y mejora continua en la operación de la red empresarial.

Topología de red para detección de fallas:

Para la detección de fallas en la infraestructura de la empresa Enter Ltda, se implementó una topología en estrella extendida, diseñada y simulada en GNS3. Esta topología fue seleccionada porque la estructura organizacional de Enter Ltda está compuesta por una sede principal y una sede remota, lo que requiere un diseño jerárquico que permita centralizar la administración y facilitar el diagnóstico de problemas en la red.

La topología en estrella extendida se caracteriza por contar con un nodo central que concentra y distribuye el tráfico hacia distintos segmentos de red. A partir de este punto principal se conectan otros dispositivos que permiten la comunicación de los equipos finales. Esta organización crea una estructura ordenada y escalable, adecuada para entornos empresariales como el de Enter Ltda.

Se eligió esta topología porque facilita la detección de fallas de manera rápida y precisa. Gracias a su diseño jerárquico, es posible identificar si un problema se encuentra en un equipo específico, en un segmento determinado o en el punto central de la red. Además, si ocurre una interrupción en una de las sedes, el diagnóstico puede enfocarse directamente en ese punto sin afectar el análisis del resto de la infraestructura.

Otra ventaja importante es que las fallas se pueden aislar con mayor facilidad, evitando que un error en un segmento comprometa toda la red. Esto mejora la eficiencia en el proceso de mantenimiento y solución de problemas.

Es decir, la topología implementada permite una mejor organización lógica de la red mediante la segmentación de los diferentes departamentos o áreas de la empresa Enter Ltda. Esta estructuración contribuye a que el tráfico esté distribuido de manera más eficiente, evitando congestiones innecesarias y facilitando el análisis cuando se presentan inconvenientes.

Otro aspecto importante es que la estrella extendida favorece la escalabilidad. Si la empresa Enter Ltda requiere agregar nuevos dispositivos o incluso ampliar su infraestructura, la estructura permite integrar nuevos nodos sin alterar significativamente el diseño general. Esto garantiza que el crecimiento de la red no complique el proceso de supervisión o mantenimiento.

Desde el punto de vista operativo, esta topología mejora la gestión administrativa, ya que el control del tráfico y la supervisión del funcionamiento de los dispositivos puede realizarse de manera centralizada. Esto permite aplicar configuraciones, realizar verificaciones y ejecutar pruebas de diagnóstico de forma ordenada y sistemática.

Finalmente, la estructura implementada contribuye a mantener estabilidad y control dentro de la red, reduciendo tiempos de respuesta ante incidentes y permitiendo una administración más eficiente del entorno tecnológico de la empresa Enter Ltda.



Tabla de descripción de equipos de dicha topología:

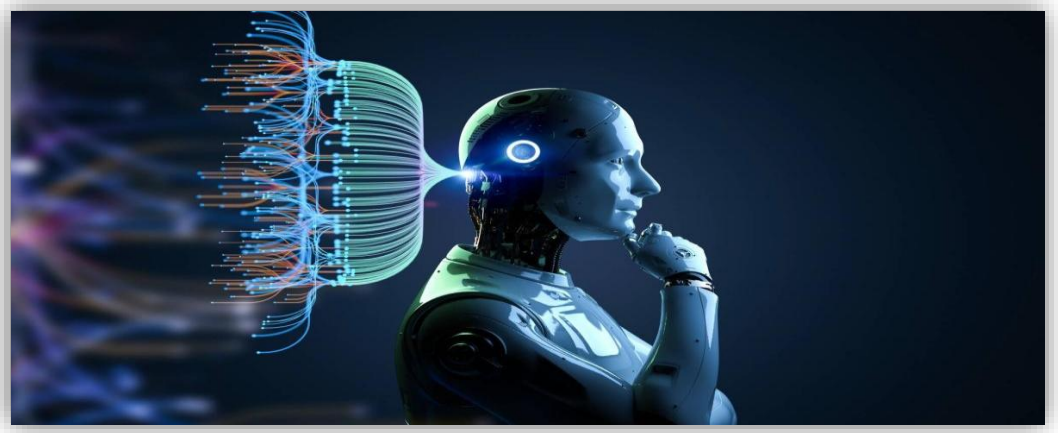
DISPOSITIVO	*CANTIDAD*	*UBICACIÓN*	*FUNCION DENTRO DE LA RED / DESCRIPCIÓN*
Router	*2*	*1 en Sede Principal y 1 en Sede Remota*	*Dispositivo encargado de conectar las diferentes redes de la empresa y permitir la comunicación entre la sede principal y la sede remota. Administra el tráfico de datos entre los distintos segmentos de red.*
Switch	*3*	*2 en Sede Principal y 1 en Sede Remota*	*Equipo que permite la interconexión de los dispositivos dentro de cada sede, facilitando la comunicación interna entre computadores, servidores y demás equipos conectados por cable.*
Access Point	*5*	*3 en Sede Principal y 2 en Sede Remota*	*Dispositivo que brinda acceso inalámbrico a la red, permitiendo que equipos como laptops, tablets y smartphones se conecten sin necesidad de cableado físico.*
Servidor (DNS)	*1*	*En Sede Principal*	*Equipo que proporciona servicios de red, específicamente la resolución de nombres, permitiendo que los usuarios accedan a recursos utilizando nombres en lugar de direcciones numéricas.*
Cliente de pruebas	*1*	*En Sede Principal*	*Equipo utilizado para verificar la conectividad y el funcionamiento general de la red mediante pruebas de comunicación y generación de tráfico.*
NMS	*1*	*En Sede Principal*	*Sistema destinado al monitoreo de los dispositivos de la red, permitiendo supervisar su estado y funcionamiento.*
PCs Administrativas	*3*	*2 en Sede Principal y 1 en Sede Remota*	*Equipos de usuario final utilizados para actividades administrativas y conectados a la red interna de la empresa.*
PCs Técnicos	*3*	*2 en Sede Principal y 1 en Sede Remota*	*Computadores utilizados por el área técnica para el desarrollo de actividades operativas dentro de la red corporativa.*
PCs Financieras	*2*	*2 en Sede Principal*	*Equipos asignados al área financiera para el manejo de información y acceso a sistemas internos.*
PCs Visitantes	*3*	*2 en Sede Principal y 1 en Sede Remota*	*Equipos destinados a usuarios externos con acceso controlado dentro de la infraestructura de red.*
Laptops	*5*	*3 en Sede Principal y 2 en Sede Remota*	*Dispositivos portátiles que se conectan a la red principalmente mediante conexión inalámbrica.*
Tablets	*5*	*3 en Sede Principal y 2 en Sede Remota*	*Dispositivos móviles que acceden a los recursos de red a través de los puntos de acceso inalámbricos.*
Smartphones	*5*	*3 en Sede Principal y 2 en Sede Remota*	*Equipos móviles conectados a la red WiFi para el acceso a servicios y recursos disponibles.*

NOTA: *Como mencionamos anteriormente, la topología de red implementada corresponde a una estructura en estrella extendida, en la cual los dispositivos de interconexión se organizan de manera jerárquica, permitiendo que los equipos finales se conecten a través de puntos de distribución centrales. Esta arquitectura facilita la administración de la red y mantiene un esquema ordenado de comunicación entre los distintos segmentos ubicados en la sede principal y la sede remota.*

La infraestructura está conformada por dispositivos de interconexión, equipos de servicio, monitoreo y dispositivos finales distribuidos estratégicamente entre ambas sedes. Los routers permiten la comunicación entre redes y garantizan el intercambio de información entre la sede principal y la sede remota. Los switches actúan como puntos de concentración de conexiones dentro de cada piso o área, organizando el tráfico de datos de forma estructurada. Por su parte, los puntos de acceso amplían la conectividad mediante acceso inalámbrico, integrando dispositivos móviles a la red.

Dentro de los equipos de servicio se encuentra el servidor, encargado de proporcionar funciones esenciales para el funcionamiento interno de la red. El sistema de monitoreo (NMS) permite supervisar el estado de los dispositivos y verificar su operatividad. Asimismo, el cliente de pruebas cumple la función de validar la conectividad y comprobar el correcto intercambio de información dentro de la infraestructura implementada.

En conjunto, esta estructura en estrella extendida permite una organización clara de los dispositivos, facilita la administración de la red y contribuye a mantener un entorno estable y funcional para el desarrollo de las actividades empresariales.



Resultado de las Pruebas de detección de fallas en la herramienta de simulación:

Tabla de pruebas:

Número test	***Tipo de condición***	***Alarmas generadas***	***Clasificación***
1	*FNR – Tráfico bajo general.*	*Sin alarmas en router y switch. Estado normal registrado en CMDB ITOP.*	***Positivo:*** *comportamiento esperado en operación normal.*
2	*FNR – Cliente accediendo al servidor.*	*Servicio disponible sin generación de alertas.*	***Positivo:*** *comunicación estable entre cliente y servidor.*
3	*FNR – Monitoreo continuo de infraestructura.*	*Interfaces activas sin eventos anormales.*	***Positivo:*** *correcta calibración sin falsas alarmas.*
4	*FAR – Generación de alto tráfico desde laptops.*	*Alarma de alto consumo en interfaz del switch.*	***Positivo:*** *detección adecuada de congestión.*
5	*FAR – Saturación de enlace WAN.*	*Alarma de congestión en router principal.*	***Positivo:*** *sistema detectó la condición anormal.*
6	*FAR – Apagado del switch de acceso.*	*Alarma de dispositivo inactivo registrada en CMDB ITOP.*	***Positivo:*** *identificación inmediata de la falla.*
7	*FAR – Caída del servidor mientras el cliente intentaba acceder.*	*Alarma crítica por indisponibilidad del servicio.*	***Positivo:*** *detección correcta del fallo.*
8	*FNR – Operación estable del switch bajo carga moderada.*	*Sin alarmas por saturación de puertos.*	***Positivo:*** *rendimiento dentro de parámetros normales.*
9	*FAR – Error de configuración en puerto que conecta PCs y cliente.*	*Alarma de pérdida de conectividad en el switch.*	***Positivo:*** *identificación precisa del punto afectado.*
10	*FAR – Deshabilitación de interfaz en router.*	*Alarma de interfaz fuera de servicio.*	***Positivo:*** *localización correcta del problema.*
11	*FNR – Comunicación estable entre sedes con cliente activo.*	*Sin generación de eventos críticos.*	***Positivo:*** *red operando bajo parámetros normales.*
12	*FAR – Cliente sin conectividad por mala configuración IP.*	*Alarma de fallo de comunicación detectada en el switch.*	***Positivo:*** *el sistema identificó correctamente la anomalía.*
13	*FAR – Incremento extremo de tráfico no detectado.*	*No se generó alarma en el router.*	***Negativo:*** *falla en la calibración del sistema.*
14	*FAR – Latencia elevada prolongada.*	*Alarma generada con retraso.*	***Negativo:*** *detección tardía frente a condición anormal.*
15	*FNR – Operación prolongada sin interrupciones.*	*Sin falsas alarmas registradas.*	***Positivo:*** *sistema correctamente ajustado.*
16	*FAR – Generación de tráfico masivo desde tablets y smartphones.*	*Alarma de saturación en puerto del switch.*	***Positivo:*** *sistema identificó correctamente la anomalía.*
17	*FNR – Supervisión general de equipos y cliente.*	*Todos los dispositivos reportando estado activo en CMDB ITOP.*	***Positivo:*** *sincronización correcta con base de datos.*
18	*FAR – Fallo intermitente en puerto de acceso.*	*Alarmas inconsistentes o no continuas.*	***Negativo:*** *aislamiento incompleto de la falla.*
19	*FAR – Pérdida total de comunicación entre switch y router.*	*Alarma crítica por enlace caído registrada en ambos equipos.*	***Positivo:*** *el sistema detectó y aisló correctamente la falla.*
20	*FNR – Restablecimiento del servicio después de falla controlada.*	*Evento registrado sin generar alarma crítica posterior.*	***Positivo:*** *el sistema confirmó la recuperación adecuada sin falsas alertas.*

RESULTADO: *Las pruebas realizadas en el entorno de simulación mediante GNS3 tuvieron como objetivo evaluar el comportamiento del sistema de detección y aislamiento de fallas bajo condiciones controladas de Funcionamiento Normal de la Red (FNR) y Funcionamiento Anormal de la Red (FAR), conforme a los lineamientos establecidos. Para la gestión de los activos de red y el registro de eventos, se adoptó una base de datos de gestión de configuración (CMDB) implementada en ITOP, lo que permitió asociar cada alarma generada con el equipo correspondiente dentro de la topología en estrella extendida.*

En los escenarios clasificados como FNR, la red operó con niveles de tráfico bajos o moderados, manteniendo estabilidad en la comunicación entre router, switch, servidor y cliente. Durante estas pruebas no se generaron alarmas críticas, lo cual evidencia una adecuada calibración de los umbrales de monitoreo. La ausencia de falsas alarmas demuestra que el sistema diferencia correctamente entre eventos normales de operación y condiciones que realmente afectan el rendimiento o la disponibilidad. Este comportamiento es fundamental en entornos productivos, ya que evita sobrecarga en la administración y reduce la probabilidad de interpretaciones erróneas por parte del administrador de red.

Por otro lado, en las pruebas FAR se simularon condiciones anormales como generación masiva de tráfico desde dispositivos finales, saturación de puertos del switch, caída del servidor, deshabilitación de interfaces en el router, pérdida de conectividad entre sedes y fallos intermitentes en enlaces. En la mayoría de estos casos, el sistema generó alarmas a nivel de equipo, identificando con precisión el dispositivo afectado y registrando el evento en la CMDB ITOP. Esto evidencia que el mecanismo de detección responde adecuadamente ante variaciones significativas en el comportamiento de la red y permite aislar el punto de falla dentro de la infraestructura.

Sin embargo, algunas pruebas fueron clasificadas como negativas debido a la ausencia de alarma frente a condiciones de tráfico extremo o a la generación tardía de alertas ante incrementos prolongados de latencia. Estos resultados indican que, aunque el sistema es funcional, requiere ajustes adicionales en la calibración de umbrales y tiempos de respuesta. La detección tardía puede impactar la disponibilidad del servicio y afectar la experiencia del usuario, especialmente en entornos donde múltiples dispositivos finales dependen de la estabilidad del switch y del router principal.

El uso de la CMDB ITOP permitió mantener un control estructurado de los activos, registrar el estado operativo de cada equipo y documentar los eventos generados durante las pruebas. Esta integración facilita la trazabilidad de las fallas, el análisis posterior de incidentes y la toma de decisiones por parte del administrador de la red. Además, contribuye a una gestión más eficiente de la infraestructura, al relacionar cada evento con su respectivo componente dentro de la topología en estrella extendida.

En términos generales, los resultados obtenidos demuestran que el sistema de detección y aislamiento de fallas presenta un desempeño satisfactorio bajo la mayoría de los escenarios evaluados. No obstante, las pruebas negativas evidencian la necesidad de optimizar la configuración del sistema para mejorar la sensibilidad ante anomalías críticas sin generar falsas alarmas. La calibración adecuada dependerá de las necesidades específicas de la red y del comportamiento esperado del tráfico en cada entorno operativo.

Finalmente, las pruebas realizadas validan el correcto funcionamiento del sistema en condiciones normales y confirman su capacidad de identificar fallas relevantes en condiciones anormales, resaltando al mismo tiempo oportunidades de mejora en la precisión y tiempo de respuesta del mecanismo de detección.

Conclusiones:

A lo largo del desarrollo de la presente evidencia se llevó a cabo el diseño, simulación y evaluación de una infraestructura de red con el objetivo de analizar el comportamiento del sistema ante diferentes escenarios relacionados con la detección de fallas en su funcionamiento. Para ello se implementó una topología de red en estrella extendida que representa la estructura de la empresa Enter Ltda, compuesta por una sede principal y una sede remota, permitiendo simular un entorno de red similar a uno real. Esta topología facilitó la interconexión de distintos dispositivos de red como routers, switches, servidores, clientes y otros dispositivos finales, los cuales fueron gestionados y monitoreados durante el proceso de pruebas.

La simulación fue realizada mediante la herramienta GNS3, la cual permitió recrear el funcionamiento de la red y generar diferentes condiciones de operación. A partir de este entorno se realizaron diversas pruebas orientadas a evaluar el comportamiento del sistema de detección y aislamiento de fallas bajo dos condiciones principales: el Funcionamiento Normal de la Red (FNR) y el Funcionamiento Anormal de la Red (FAR). Durante las pruebas de funcionamiento normal se evidenció que la red opera de manera estable, manteniendo la comunicación entre los dispositivos sin generar alarmas innecesarias, lo cual demuestra que el sistema de monitoreo se encuentra correctamente configurado para evitar falsas alertas que puedan afectar la administración de la infraestructura.

Por otro lado, en los escenarios de funcionamiento anormal se simularon situaciones que pueden afectar el rendimiento y la disponibilidad de la red, tales como generación excesiva de tráfico, caída de equipos, saturación de enlaces, errores de configuración y pérdida de conectividad entre dispositivos. Estas pruebas permitieron verificar la capacidad del sistema para detectar anomalías y generar alarmas a nivel de equipo, identificando de manera oportuna el punto donde se origina la falla. La mayoría de los resultados obtenidos fueron clasificados como positivos, lo que evidencia que el sistema es capaz de reaccionar adecuadamente ante eventos que comprometen la operación normal de la red.

Por otro lado, en los escenarios de funcionamiento anormal se simularon situaciones que pueden afectar el rendimiento y la disponibilidad de la red, tales como generación excesiva de tráfico, caída de equipos, saturación de enlaces, errores de configuración y pérdida de conectividad entre dispositivos. Estas pruebas permitieron verificar la capacidad del sistema para detectar anomalías y generar alarmas a nivel de equipo, identificando de manera oportuna el punto donde se origina la falla. La mayoría de los resultados obtenidos fueron clasificados como positivos, lo que evidencia que el sistema es capaz de reaccionar adecuadamente ante eventos que comprometen la operación normal de la red.

No obstante, algunas pruebas evidenciaron resultados negativos relacionados con la detección tardía o ausencia de alarmas ante determinadas condiciones anormales. Estos resultados son relevantes, ya que permiten identificar oportunidades de mejora en la calibración del sistema de monitoreo, especialmente en lo referente a la configuración de umbrales de alerta y tiempos de respuesta. La correcta calibración del sistema es fundamental para garantizar una detección más precisa de las fallas y reducir el impacto que estas pueden generar en el desempeño de la red.

En términos generales, el desarrollo de esta evidencia permitió comprender la importancia de implementar mecanismos de monitoreo y detección de fallas dentro de una infraestructura de red. Asimismo, evidenció cómo el uso de herramientas de simulación, junto con sistemas de gestión de configuración, contribuye al análisis del comportamiento de la red, la identificación de posibles problemas y la mejora continua en la administración de los recursos tecnológicos.

Finalmente, la implementación de un sistema de detección y aislamiento de fallas, apoyado en herramientas de simulación y en una base de datos de gestión de configuración, constituye una estrategia fundamental para garantizar la disponibilidad, estabilidad y correcto funcionamiento de la red. Esto permite a las organizaciones anticiparse a posibles incidentes, optimizar el rendimiento de la infraestructura y asegurar la continuidad de los servicios que dependen de la conectividad de la red.

Bibliografías:

https://zajuna.sena.edu.co/Repositorio/Titulada/institution/SENA/CienciasNaturales/228183/Contenido/OVA/CF14/index.html#/

https://www.youtube.com/watch?v=1HGpr48Sjys

https://www.youtube.com/watch?v=Oon4hdBKedY

https://www.youtube.com/watch?v=eO57y8GHztA

https://www.youtube.com/watch?v=FMzBWUCU7VI

https://www.youtube.com/watch?v=anhtStlRvA4

https://ccnadesdecero.es/que-es-gns3-como-usarlo/

https://topologiasdered.com/simulador/que-es-gns3-vm/

Evidencia GA8-220501107-AA1-EV01. Lista de verificación para validar parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión.

Reporte Wlan-Report-Latest de un equipo de la red:

Lista de verificación para validar parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión:

Ítem	***Caso I***		***Caso II***		***Caso III***	
	Cumple - Si	***Cumple - No***	***Cumple - Si***	***Cumple - No***	***Cumple - Si***	***Cumple - No***
Ancho de banda.	*4 MHz*		*8 MHz*		*4 MHz*	
Frecuencia de operación.	*1 MHz*		*2 MHz*		*2 MHz*	
Período de la Señal (T).	*1µs* *X*			*3µs* *X*	*2 µs* *X*	
Duración de 1 Bit.	*1µs*		*3µs*		*2 µs*	
Velocidad de Transmisión.	*1 Mbps*		*0.33 Mbps*		*0.5 Mbps*	
Calidad.	*Buena*		*Baja*		*Media*	
Uso de Canal.	*Canal estable con baja interferencia*		*Canal con mayor ocupación y posible congestión*		*Canal con uso moderado y estabilidad aceptable*	

Nota: Análisis de los casos evaluados

Con el objetivo de validar los parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión de la red inalámbrica implementada en la infraestructura de la empresa Enter Ltda., se realizó un análisis comparativo a partir de tres casos de estudio. Cada caso representa diferentes condiciones de operación de la red, permitiendo identificar el comportamiento del sistema de comunicación en función de los parámetros evaluados.

*En el **Caso I**, la red opera con un ancho de banda de 4 MHz y una frecuencia de operación de 1 MHz, presentando un período de la señal de 1 µs. Bajo estas condiciones, la duración de un bit corresponde igualmente a 1 µs, lo que permite alcanzar una velocidad de transmisión aproximada de 1 Mbps. Estas características permiten que la comunicación de datos se realice de manera eficiente, manteniendo una buena estabilidad en la señal y un uso adecuado del canal de transmisión. Debido a que el período de la señal es corto, el sistema puede transmitir información con mayor rapidez, lo que se traduce en una buena calidad de servicio para los dispositivos conectados a la red inalámbrica.*

*En el **Caso II**, se observa un aumento en el ancho de banda hasta 8 MHz y una frecuencia de operación de 2 MHz; sin embargo, el período de la señal se incrementa a 3 µs. Este aumento en el período genera que la duración de un bit también sea de 3 µs, reduciendo la velocidad de transmisión a aproximadamente 0.33 Mbps. Aunque el ancho de banda es mayor, el incremento del período de la señal afecta el rendimiento general de la comunicación, disminuyendo la eficiencia en la transmisión de datos. En este escenario se evidencia una menor calidad en la comunicación y una mayor ocupación del canal, lo que puede generar congestión o retrasos en la transferencia de información.*

*Por consiguiente, en el **Caso III**, se propone un período de señal de 2 µs como valor intermedio entre los dos casos anteriores. En este escenario la duración de un bit es igualmente de 2 µs, lo que permite alcanzar una velocidad de transmisión aproximada de 0.5 Mbps. Este comportamiento representa una condición de funcionamiento moderada de la red, en la cual el rendimiento no es tan alto como en el Caso I, pero tampoco presenta las limitaciones observadas en el Caso II. Bajo estas condiciones, la calidad de la conexión puede considerarse aceptable y el uso del canal se mantiene en niveles moderados, permitiendo una transmisión de datos relativamente estable dentro de la red inalámbrica.*

Finalmente, el análisis de los tres casos permite evidenciar que el período de la señal tiene una influencia directa sobre la velocidad de transmisión y la calidad de la comunicación en la red inalámbrica. A menor período de señal se obtiene una mayor velocidad de transmisión y un mejor desempeño del canal, mientras que períodos mayores reducen la eficiencia de la comunicación y pueden afectar el rendimiento general de la red.

Conclusión:

*El desarrollo de la evidencia **GA8-220501107-AA1-EV01** permitió analizar diferentes aspectos relacionados con el funcionamiento y la evaluación de la red inalámbrica implementada en la infraestructura de la empresa Enter Ltda. A través de las actividades realizadas fue posible comprender la importancia de validar los parámetros que influyen directamente en el rendimiento y la calidad del servicio de una red WiFi, tales como el ancho de banda, la frecuencia de operación, el período de la señal, la velocidad de transmisión y el uso de los canales de comunicación.*

*En primer lugar, mediante la generación del **reporte Wlan-Report-Latest** desde uno de los equipos de la red se pudo obtener información detallada sobre el comportamiento de la conexión inalámbrica. Este reporte permitió identificar eventos relevantes como los momentos de conexión y desconexión de la red, cambios en el estado del adaptador inalámbrico, disponibilidad de acceso a Internet y posibles errores o limitaciones en la conectividad. Esta información resulta fundamental para el monitoreo de la red, ya que proporciona datos que facilitan la identificación de fallas y el análisis del desempeño de la conexión inalámbrica.*

*Posteriormente, se elaboró la **lista de verificación para validar parámetros de calidad, velocidad de transmisión, ancho de banda, uso de canales y frecuencias de transmisión**, lo cual permitió evaluar diferentes escenarios de funcionamiento de la red mediante tres casos de análisis. A partir de estos casos fue posible evidenciar la relación existente entre el período de la señal y la velocidad de transmisión de los datos, demostrando que un menor período de señal permite una mayor velocidad de transmisión y una mejor calidad en la comunicación. De igual forma, se pudo observar cómo el uso del canal y la ocupación del ancho de banda pueden influir en el rendimiento general de la red, generando condiciones de funcionamiento estables o, por el contrario, situaciones de congestión o interferencia que afectan la calidad del servicio.*

*Adicionalmente, el **registro fotográfico del proceso de pruebas** permitió documentar las diferentes etapas del procedimiento realizado para la verificación de la red inalámbrica. Estas evidencias visuales contribuyen a respaldar el trabajo desarrollado y demuestran la ejecución de las pruebas necesarias para la evaluación de los parámetros de transmisión y el análisis del comportamiento de la red en diferentes condiciones.*

Finalmente, el desarrollo de esta evidencia permitió fortalecer los conocimientos relacionados con la evaluación y monitoreo de redes inalámbricas, así como la interpretación de parámetros técnicos que influyen en el desempeño de la comunicación de datos. La aplicación de herramientas de análisis, listas de verificación y registros de pruebas constituye una estrategia fundamental para garantizar el correcto funcionamiento de las redes, permitiendo a los administradores identificar posibles problemas, optimizar la configuración de los dispositivos y mejorar la calidad del servicio ofrecido a los usuarios dentro de la infraestructura de red de la organización.

Bibliografía:

https://zajuna.sena.edu.co/Repositorio/Titulada/institution/SENA/CienciasNaturales/228183/Contenido/OVA/CF9/index.html#/

https://zajuna.sena.edu.co/Repositorio/Titulada/institution/SENA/CienciasNaturales/228183/Contenido/OVA/CF14/index.html#/

https://www.youtube.com/watch?v=-laahU9HtqQ&t=837s

https://vamosarema.com/

https://netwgeeks.com/introduccion-a-gns3/

https://www.youtube.com/watch?v=fOC0w553iTQ

Evidencia GA9-220501106-AA1-EV01. Informe sobre detección de fallos en el rendimiento y operación de la solución.

Introducción:

En las infraestructuras de red actuales, el correcto funcionamiento de los sistemas de comunicación depende en gran medida de la capacidad de detectar, analizar y solucionar oportunamente las fallas que puedan presentarse durante la operación normal de la red. En organizaciones que cuentan con múltiples dispositivos interconectados, la administración eficiente de la red es fundamental para garantizar la disponibilidad de los servicios, la continuidad de las operaciones y la adecuada transmisión de la información entre los diferentes usuarios y sistemas.

*En el caso de la empresa **Enter Ltda.**, la infraestructura de red se encuentra distribuida en dos sedes: una sede principal ubicada en un edificio de tres pisos y una sede remota ubicada en un edificio de dos pisos. Esta estructura requiere una correcta interconexión entre los dispositivos de red, tales como routers, switches, servidores, puntos de acceso inalámbricos y equipos de usuario, con el fin de permitir la comunicación y el intercambio de información dentro de la organización. Debido a la complejidad de esta infraestructura, es necesario implementar mecanismos de monitoreo y procedimientos de diagnóstico que permitan identificar posibles fallas que puedan afectar el rendimiento y la operación de la red.*

*Para el desarrollo de esta actividad se utilizó la herramienta **GNS3**, la cual permite simular entornos de red de forma realista y evaluar el comportamiento de los dispositivos y enlaces de comunicación en diferentes escenarios. A través de esta herramienta fue posible recrear la topología de red correspondiente a las dos sedes de la empresa Enter Ltda., facilitando la realización de pruebas orientadas a la detección de fallas, el análisis del rendimiento de la red y la identificación de posibles problemas en su funcionamiento.*

*En este contexto, el presente informe tiene como propósito describir el proceso de **detección, aislamiento y corrección de fallas en el rendimiento y operación de la solución de red**, aplicando diferentes procedimientos de diagnóstico dentro del entorno de simulación. Para ello se abordan aspectos como la localización de fallas, la identificación de problemas en los componentes de la red, el análisis de síntomas que permitan determinar las causas de los inconvenientes y la aplicación de soluciones que permitan restablecer el funcionamiento adecuado de la red.*

Finalmente, el desarrollo de esta evidencia permite fortalecer los conocimientos relacionados con la administración y mantenimiento de redes, así como comprender la importancia de implementar procesos de monitoreo y diagnóstico que contribuyan a garantizar la estabilidad, el rendimiento y la disponibilidad de los servicios de red dentro de una organización.

Solución de los 5 puntos sugeridos para detección de fallas:

- ***Localización de fallas:*** *El proceso de localización de fallas constituye una de las primeras etapas dentro de la administración y mantenimiento de redes, ya que permite identificar el punto específico donde se presenta un problema que afecta el rendimiento o la operación de la infraestructura de red. Este proceso es fundamental para garantizar la continuidad de los servicios y minimizar el impacto que puedan generar las fallas en el funcionamiento normal de la red.*

  En el caso de la infraestructura de red de la empresa ***Enter Ltda.****, la cual se encuentra distribuida entre una sede principal ubicada en un edificio de tres pisos y una sede remota en un edificio de dos pisos, fue necesario realizar un proceso de análisis inicial para determinar posibles puntos de falla dentro de la topología implementada. Para ello se tuvo en cuenta la interconexión entre los diferentes dispositivos que conforman la red, tales como routers, switches, puntos de acceso inalámbricos, servidores y equipos de usuario.*

  La localización de fallas se realizó a través del entorno de simulación proporcionado por la herramienta ***GNS3****, la cual permitió observar el comportamiento de los dispositivos de red y analizar el estado de las conexiones establecidas entre ellos. Mediante esta herramienta fue posible verificar la conectividad entre los diferentes segmentos de la red, identificar posibles problemas en la comunicación entre dispositivos y evaluar el estado de los enlaces que permiten la transmisión de datos entre las dos sedes de la empresa.*

  Durante este proceso también se revisaron aspectos relacionados con la configuración de los dispositivos de red, tales como direcciones IP, tablas de enrutamiento, estado de las interfaces y configuración de los servicios de red. Esta verificación permitió detectar posibles inconsistencias o configuraciones incorrectas que podrían generar problemas de conectividad o afectar el rendimiento general de la red.

  De igual manera, se realizó un monitoreo del tráfico y del comportamiento de los dispositivos dentro de la simulación, lo cual permitió identificar situaciones en las que la red podría presentar fallas, como pérdida de conectividad entre equipos, retrasos en la transmisión de datos o interrupciones en la comunicación entre las sedes. A partir de este análisis fue posible establecer una base para continuar con las etapas posteriores del proceso de detección de fallas, las cuales incluyen la identificación de los problemas específicos, el diagnóstico de sus posibles causas y la aplicación de soluciones que permitan restablecer el funcionamiento adecuado de la red.

  Finalmente, la localización de fallas permitió identificar los posibles puntos críticos dentro de la infraestructura de red de la empresa Enter Ltda., facilitando el análisis de los problemas que pueden presentarse durante la operación normal del sistema. Este proceso constituye una etapa fundamental dentro de la administración de redes, ya que permite actuar de manera oportuna para mantener la estabilidad, disponibilidad y rendimiento de los servicios de comunicación dentro de la organización.

- ***Identificación:*** *La etapa de identificación de fallas dentro de una red de datos consiste en reconocer, registrar y analizar los posibles problemas que pueden afectar el funcionamiento normal de la infraestructura de comunicaciones. Este proceso es fundamental para garantizar la disponibilidad de los servicios de red, ya que permite detectar oportunamente cualquier irregularidad en el comportamiento de los dispositivos o en la transmisión de la información.*

  Para realizar una adecuada identificación de los posibles problemas presentes en la red, fue necesario desarrollar un proceso de ***documentación de problemas****, el cual consiste en registrar información relevante sobre la configuración de los dispositivos y sobre las condiciones en las que se presentan las fallas. Esta documentación permite facilitar el análisis posterior de los problemas y agilizar el proceso de diagnóstico y solución. Dentro de esta documentación se incluyeron los siguientes aspectos:*

  Configuración de cada computador: *Se revisó la configuración de los equipos finales conectados a la red, tales como computadores de usuario, equipos de monitoreo y clientes de prueba. En este proceso se verificaron parámetros como la dirección IP asignada, la máscara de subred, la puerta de enlace predeterminada y la conectividad con otros dispositivos dentro de la red. Esta revisión permitió comprobar que los equipos contaran con una configuración adecuada para poder comunicarse correctamente con el resto de la infraestructura.*

  Configuración general de la red: *También se analizó la configuración general de la topología de red implementada en la simulación. En este caso se verificó el estado de los enlaces entre los dispositivos, la conectividad entre la sede principal y la sede remota, así como la correcta comunicación entre los diferentes segmentos de la red. Este análisis permitió identificar posibles problemas relacionados con la conectividad, la configuración de los dispositivos de red o el funcionamiento de los enlaces de comunicación.*

  Información sobre problemas en la red: *Durante el proceso de simulación se registraron los diferentes comportamientos observados en la red, especialmente aquellos que podían indicar la presencia de fallas o inconsistencias en el funcionamiento del sistema. Entre los problemas identificados se consideraron situaciones como pérdida de conectividad entre dispositivos, demoras en la transmisión de datos, interrupciones en la comunicación entre sedes o dificultades en el acceso a determinados servicios dentro de la red.*

  Es importante tener en cuenta que los problemas en una red de datos pueden presentarse en diferentes momentos del ciclo de vida de la infraestructura. En algunos casos, las fallas pueden ocurrir durante el proceso de ***instalación o configuración inicial de los dispositivos****, mientras que en otros casos pueden aparecer durante la* ***operación normal de la red****, debido a cambios en la configuración, sobrecarga de tráfico o fallas en los equipos.*

Por esta razón, el proceso de detección de fallas debe seguir una metodología estructurada que permita analizar de manera ordenada los posibles problemas que se presenten en la red. En este sentido, el proceso de detección de fallas se basa en tres pasos fundamentales:

Identificación de la falla: *En esta etapa se detecta la existencia de un problema en la red mediante la observación de síntomas como pérdida de conectividad, interrupción en los servicios, lentitud en la transmisión de datos o fallos en la comunicación entre dispositivos.*

Diagnóstico de la falla: *Una vez identificada la falla, se procede a analizar sus posibles causas. Para ello se revisan las configuraciones de los dispositivos, el estado de los enlaces de red y el comportamiento general del sistema, con el objetivo de determinar el origen del problema.*

Aplicación de soluciones: *cuando se ha determinado la causa de la falla, se aplican las acciones necesarias para corregir el problema y restablecer el funcionamiento normal de la red. Posteriormente se realizan pruebas adicionales para verificar que la solución implementada haya resuelto completamente la situación.*

Finalmente, la etapa de identificación de fallas permitió recopilar información detallada sobre el estado de los dispositivos, la configuración de la red y los posibles problemas presentes dentro de la infraestructura simulada de la empresa Enter Ltda. Este proceso constituye una base fundamental para las siguientes etapas del análisis de fallas, ya que facilita la realización de diagnósticos más precisos y la implementación de soluciones adecuadas que permitan garantizar el correcto funcionamiento de la red.

- ***Preguntas para la elaboración de síntomas:*** *Durante el proceso de detección de fallas en una red de datos es fundamental identificar los síntomas que permiten reconocer la existencia de un problema en la infraestructura. Para ello, se utilizan una serie de preguntas orientadas a recopilar información sobre el momento en que ocurre la falla, las condiciones en las que se presenta y los cambios que se hayan realizado en la red antes de que el problema aparezca.*

  Estas preguntas permiten obtener información clave para comprender el comportamiento de la red y facilitar el proceso de diagnóstico. En el caso de la red implementada para la empresa ***Enter Ltda.****, las preguntas fueron analizadas teniendo en cuenta el funcionamiento de la topología de red simulada en* ***GNS3****, la cual conecta la sede principal y la sede remota mediante diferentes dispositivos y enlaces de comunicación.*

  A continuación, se presentan las preguntas utilizadas para la elaboración de los síntomas y el análisis correspondiente de cada una de ellas.

¿Qué se estaba haciendo cuando ocurrió la falla?

Durante las pruebas realizadas en el entorno de simulación, se observó que algunas fallas se presentaban mientras se realizaban pruebas de conectividad entre los diferentes dispositivos de la red. Por ejemplo, al intentar establecer comunicación entre equipos ubicados en la sede principal y equipos de la sede remota, en algunos casos se presentaron interrupciones en la transmisión de datos o pérdida temporal de conectividad.

Este tipo de situaciones permitió identificar que ciertos problemas podían estar relacionados con el estado de los enlaces de comunicación o con la configuración de los dispositivos que permiten la interconexión entre ambas sedes. Asimismo, durante el proceso de monitoreo de la red se analizaron diferentes escenarios en los cuales se generaban cambios en el tráfico o se realizaban pruebas de acceso a servicios dentro de la red, lo cual permitió observar el comportamiento de los dispositivos bajo distintas condiciones de funcionamiento.

¿Se había ejecutado antes este proceso?

Sí, las pruebas de conectividad y funcionamiento de la red se habían realizado previamente durante las fases de configuración y validación de la infraestructura. Estas pruebas permitieron verificar que los dispositivos se encontraban correctamente configurados y que la comunicación entre los diferentes segmentos de la red se realizaba de manera adecuada.

La repetición de estos procesos dentro del entorno de simulación permitió comparar los resultados obtenidos en diferentes momentos y detectar posibles variaciones en el comportamiento de la red. De esta forma, fue posible identificar si los problemas observados correspondían a fallas recientes o si se trataba de situaciones que ya se habían presentado anteriormente.

Si es afirmativo, ¿se ejecutó con éxito?

En la mayoría de los casos, las pruebas realizadas anteriormente se ejecutaron con éxito, lo que permitió confirmar que la infraestructura de red se encontraba funcionando correctamente bajo condiciones normales de operación. Sin embargo, durante la ejecución de nuevas pruebas dentro del entorno de simulación, se presentaron algunos comportamientos anómalos que permitieron identificar posibles fallas en determinados momentos del funcionamiento de la red.

Estas situaciones permitieron evidenciar que, aunque la red puede operar correctamente en condiciones normales, es posible que bajo ciertas circunstancias se presenten fallas relacionadas con la configuración de los dispositivos, la congestión de tráfico o el estado de los enlaces de comunicación.

¿Qué ha cambiado desde ese momento?

*Uno de los aspectos más importantes en el proceso de detección de fallas consiste en identificar los cambios que se hayan realizado en la red antes de que se presente el problema. En el caso de la red simulada en **GNS3**, se analizaron diferentes cambios que pudieron haber influido en el comportamiento de la infraestructura, tales como modificaciones en la configuración de los dispositivos, ajustes en los parámetros de comunicación o la incorporación de nuevos equipos dentro de la topología.*

También se consideraron posibles variaciones en el tráfico de la red, especialmente durante las pruebas en las que se simulaban condiciones de funcionamiento anormal con mayores cantidades de tráfico en determinados segmentos de la infraestructura. Estas situaciones permitieron observar cómo el incremento del tráfico puede afectar el rendimiento de la red y generar síntomas como retrasos en la transmisión de datos o interrupciones en la conectividad.

Finalmente, El análisis de estos cambios permitió comprender mejor las posibles causas de las fallas identificadas durante el proceso de monitoreo y facilitó la identificación de los elementos de la red que requerían una revisión más detallada.

- ***Diagnóstico de problemas:** El diagnóstico de problemas constituye una de las etapas más importantes dentro del proceso de administración y mantenimiento de redes, ya que permite analizar en profundidad las posibles causas de las fallas identificadas durante las etapas anteriores. Este proceso consiste en evaluar la información recopilada durante la identificación de síntomas, revisar la configuración de los dispositivos de red y analizar el comportamiento general de la infraestructura con el fin de determinar el origen de los problemas que afectan el rendimiento y la operación de la red.*

  Durante esta etapa fue necesario realizar un análisis detallado de la información obtenida previamente en el proceso de identificación de fallas, evaluando todos los aspectos que pudieran influir en el funcionamiento de la red. Entre los principales elementos analizados se encuentran la configuración de los dispositivos de red, el estado de los enlaces de comunicación, el comportamiento del tráfico de datos y la interacción entre los diferentes componentes que conforman la infraestructura.

  *Uno de los primeros pasos en el diagnóstico de problemas consistió en **evaluar la información disponible sobre el problema**, revisando los registros obtenidos durante las pruebas realizadas en la simulación. Esta información permitió identificar los momentos en los cuales se presentaban fallas de conectividad o interrupciones en la comunicación entre dispositivos, así como determinar si estos problemas se presentaban de manera constante o intermitente.*

*Posteriormente, se realizó un análisis de la **configuración de los dispositivos de red**, verificando parámetros fundamentales como direcciones IP, máscaras de subred, puertas de enlace, estado de las interfaces de red y configuración de los enlaces que permiten la comunicación entre la sede principal y la sede remota. Este proceso permitió detectar posibles inconsistencias en la configuración que podrían generar problemas de conectividad o afectar el flujo normal de la información dentro de la red.*

*Otro aspecto importante dentro del diagnóstico fue el análisis del **estado de los enlaces de comunicación** entre los dispositivos. En una infraestructura de red, los enlaces representan el medio a través del cual se transmiten los datos entre los diferentes equipos, por lo que cualquier problema en estos enlaces puede generar fallas en la comunicación. Mediante el uso de las herramientas disponibles en **GNS3**, fue posible verificar el estado de las conexiones entre routers, switches y dispositivos finales, permitiendo identificar posibles interrupciones o configuraciones incorrectas que pudieran afectar el funcionamiento de la red.*

*Asimismo, se evaluó el **comportamiento del tráfico de datos** dentro de la red, especialmente durante las pruebas en las que se simulaban diferentes condiciones de funcionamiento. En algunos casos se generaron escenarios de mayor carga de tráfico con el objetivo de observar cómo respondía la infraestructura ante situaciones que podrían afectar el rendimiento del sistema. Este análisis permitió identificar posibles puntos de congestión o retrasos en la transmisión de la información.*

*Un aspecto fundamental del diagnóstico de problemas consiste en **descartar las causas que no son probables**, con el fin de concentrar el análisis en aquellos elementos que realmente pueden estar generando la falla. Este proceso implica revisar cada componente de la red de manera sistemática, eliminando gradualmente las posibles causas hasta encontrar el origen del problema.*

*En el caso de la red de **Enter Ltda.**, este procedimiento permitió descartar problemas relacionados con algunos dispositivos que se encontraban correctamente configurados y operando de manera adecuada. De esta forma, el análisis se concentró en los elementos de la infraestructura que presentaban comportamientos anómalos o inconsistencias en su funcionamiento.*

*Finalmente, el diagnóstico de problemas permitió realizar un análisis detallado del comportamiento de la red simulada en **GNS3**, evaluando la configuración de los dispositivos, el estado de los enlaces de comunicación y el flujo de tráfico dentro de la infraestructura. Este proceso facilitó la identificación de las posibles causas de las fallas detectadas durante las pruebas y permitió establecer las bases necesarias para la aplicación de soluciones correctivas que garanticen el funcionamiento adecuado de la red de la empresa **Enter Ltda.***

- ***Aplicar soluciones:*** *La aplicación de soluciones constituye la fase final dentro del proceso de detección y diagnóstico de fallas en una red de datos. En esta etapa se implementan las acciones correctivas necesarias para restablecer el funcionamiento adecuado de la infraestructura de red y garantizar que los servicios operen de manera estable y eficiente.*

  En el caso de la red diseñada para la empresa ***Enter Ltda.****, que conecta la sede principal y la sede remota mediante una topología de red tipo estrella extendida, el proceso de aplicación de soluciones se llevó a cabo dentro del entorno de simulación proporcionado por la herramienta* ***GNS3****. Este entorno permitió realizar diferentes pruebas de conectividad, verificar configuraciones y simular condiciones tanto normales como anormales de funcionamiento con el fin de validar la efectividad de las soluciones implementadas.*

  Antes de aplicar cualquier solución fue necesario ***intentar repetir el problema detectado****, con el objetivo de confirmar que la falla realmente existía y que no se trataba de un error ocasionado por el operador o por una ejecución incorrecta de las pruebas. En muchas ocasiones, dentro de los procesos de administración de redes, los problemas pueden estar asociados a errores humanos durante la configuración de dispositivos o durante la ejecución de comandos de diagnóstico.*

  Para realizar esta verificación se ejecutaron nuevamente diferentes pruebas de conectividad entre los dispositivos de la red, tales como pruebas de comunicación entre equipos ubicados en la sede principal y dispositivos de la sede remota. También se realizaron pruebas de acceso a servicios dentro de la red y se revisó el estado de las interfaces de los dispositivos con el fin de comprobar si la falla se presentaba de manera constante.

  Una vez confirmado el problema, se procedió a realizar el ***análisis de las posibles soluciones****, teniendo en cuenta los resultados obtenidos durante el proceso de diagnóstico. Entre las acciones correctivas aplicadas dentro del entorno de simulación se incluyeron la revisión y corrección de configuraciones de red, la verificación del estado de los enlaces de comunicación y la comprobación de los parámetros de funcionamiento de los dispositivos involucrados.*
  En algunos casos fue necesario ajustar configuraciones relacionadas con la conectividad entre dispositivos, revisar la correcta asignación de direcciones IP, verificar la configuración de las interfaces de red y confirmar que los enlaces entre routers, switches y dispositivos finales se encontraban activos y correctamente configurados. Estas acciones permitieron restablecer la comunicación entre los diferentes segmentos de la red.

  Después de aplicar cada una de las soluciones propuestas, se procedió nuevamente a ***intentar repetir el problema****, con el objetivo de verificar si la falla continuaba presentándose o si la solución implementada había logrado corregir el inconveniente detectado. Este procedimiento es fundamental dentro del proceso de administración de redes, ya que permite validar de manera objetiva la efectividad de las acciones correctivas aplicadas.*

*En aquellos casos en los que, después de aplicar la solución, **el problema no pudo ser repetido**, se concluyó que la solución implementada fue correcta y que el funcionamiento de la red se había restablecido adecuadamente. Esto se confirmó mediante la ejecución de nuevas pruebas de conectividad, análisis del comportamiento del tráfico de datos y verificación del estado de los dispositivos dentro de la topología de red.*

*Sin embargo, en algunos escenarios se identificó que ciertos problemas podían presentarse de manera **intermitente**, es decir, no ocurrían de forma constante sino únicamente bajo determinadas condiciones de funcionamiento, como por ejemplo cuando se generaban mayores cantidades de tráfico dentro de la red. En estos casos fue necesario continuar con el proceso de análisis y plantear **nuevas soluciones**, con el fin de encontrar alternativas que permitieran mejorar el rendimiento de la red y evitar que estas fallas afectaran el funcionamiento normal de la infraestructura.*

*Por consiguiente, Gracias a este proceso sistemático de verificación, corrección y validación, fue posible garantizar que la red implementada en el entorno de simulación funcionara de manera adecuada y que los dispositivos pudieran comunicarse correctamente entre sí. Asimismo, este procedimiento permitió fortalecer las prácticas de administración y mantenimiento de redes, contribuyendo a mejorar la estabilidad, confiabilidad y eficiencia de la infraestructura tecnológica de la empresa **Enter Ltda.***

*Finalmente, la aplicación de soluciones dentro del proceso de detección de fallas permitió corregir los problemas identificados durante las pruebas realizadas en **GNS3**, validando la efectividad de las configuraciones implementadas y asegurando el correcto funcionamiento de la red entre la sede principal y la sede remota.*

- ***Punto importante a tener en cuenta - Administración de fallas:** La administración de fallas es un proceso fundamental dentro de la gestión de redes, ya que permite supervisar el funcionamiento de la infraestructura, detectar posibles problemas en el sistema de comunicaciones y garantizar que la red opere de manera estable y eficiente. Este proceso tiene como objetivo principal identificar, registrar, notificar y solucionar las fallas que puedan presentarse en los diferentes componentes de la red, con el fin de minimizar el impacto que estos problemas puedan generar en el funcionamiento de los servicios y en las actividades de los usuarios.*

  *En el caso de la red implementada para la empresa **Enter Ltda.**, la administración de fallas se enfocó en el monitoreo del comportamiento de los dispositivos y enlaces de comunicación que conforman la infraestructura de red entre la sede principal y la sede remota. Para ello se utilizó el entorno de simulación proporcionado por la herramienta **GNS3**, el cual permitió observar el funcionamiento de la topología de red y analizar el estado de los diferentes dispositivos que participan en la transmisión de datos.*

Uno de los aspectos más importantes dentro de la administración de fallas es la ***detección oportuna de los problemas*** *que puedan afectar el rendimiento de la red. En este sentido, se realizaron diferentes pruebas de conectividad y monitoreo del estado de los dispositivos con el objetivo de identificar posibles interrupciones en la comunicación, pérdida de conectividad entre equipos o comportamientos anómalos en la transmisión de datos. Estas pruebas permitieron detectar fallas potenciales y evaluar el impacto que podrían tener en el funcionamiento general de la infraestructura.*

Una vez identificadas las fallas, es necesario realizar un proceso de ***registro de los problemas detectados****, el cual consiste en documentar la información relacionada con el evento ocurrido. Este registro incluye datos como el momento en que se presentó la falla, los dispositivos involucrados, las condiciones bajo las cuales se generó el problema y las acciones realizadas para su solución. La documentación de esta información resulta fundamental para facilitar la gestión de la red y para disponer de un historial que permita analizar el comportamiento del sistema a lo largo del tiempo.*

Otro elemento importante dentro de la administración de fallas es la ***notificación a los usuarios o administradores de la red*** *cuando se detecta algún problema que pueda afectar la disponibilidad de los servicios. Aunque en este caso se trata de una red simulada dentro del entorno de* ***GNS3****, en un entorno real este proceso permitiría informar a los responsables de la administración de la red sobre la existencia de una falla para que puedan tomar las medidas necesarias para su corrección.*

Adicionalmente, la administración de fallas busca implementar mecanismos que permitan ***solucionar automáticamente ciertos problemas cuando sea posible****, reduciendo así el tiempo de interrupción de los servicios y mejorando la eficiencia en la operación de la red. En muchos casos, esto puede lograrse mediante configuraciones adecuadas de los dispositivos de red, monitoreo constante del estado de los equipos y la implementación de procedimientos que permitan detectar rápidamente las anomalías en el funcionamiento del sistema.*

Dentro del entorno de simulación utilizado en este proyecto, la administración de fallas permitió analizar el comportamiento de la red bajo diferentes condiciones de funcionamiento, evaluar la capacidad de respuesta de los dispositivos ante posibles problemas y aplicar las acciones correctivas necesarias para restablecer el funcionamiento adecuado de la infraestructura.

Finalmente, la administración de fallas constituye un proceso esencial para garantizar la estabilidad, disponibilidad y eficiencia de una red de datos. A través del monitoreo constante, el registro de eventos, la notificación de problemas y la aplicación de soluciones oportunas, es posible mantener un control adecuado sobre el funcionamiento de la infraestructura de red y asegurar que los servicios de comunicación operen de manera confiable dentro de la organización. En el caso de la red simulada de la empresa ***Enter Ltda.****, este proceso permitió fortalecer la gestión de la infraestructura y mejorar la capacidad de respuesta ante posibles fallas que puedan presentarse durante la operación del sistema.*

Conclusiones:

El desarrollo de la evidencia permitió comprender la importancia que tiene el proceso de detección, diagnóstico y solución de fallas dentro de la administración de redes de datos. A través del análisis del funcionamiento de la infraestructura de red implementada para la empresa Enter Ltda., fue posible identificar cómo los diferentes componentes de hardware y software deben operar de manera coordinada para garantizar un servicio de comunicación estable y eficiente entre la sede principal y la sede remota.

Mediante la utilización de la herramienta de simulación GNS3 se logró recrear un entorno de red que permitió realizar pruebas de conectividad, monitorear el comportamiento de los dispositivos y analizar diferentes escenarios en los que podían presentarse fallas dentro de la red. Esto facilitó el proceso de localización de problemas, ya que se pudieron identificar situaciones que afectaban el rendimiento de la infraestructura, como interrupciones en la comunicación, errores de configuración o fallas en los enlaces entre dispositivos.

Durante el proceso de identificación de fallas se evidenció la importancia de mantener una adecuada documentación de la red, incluyendo la configuración de cada equipo, la configuración general de la infraestructura y el registro de los problemas detectados. Esta información resulta fundamental para facilitar el análisis de los inconvenientes que puedan presentarse durante la operación de la red, permitiendo a los administradores actuar de manera más rápida y eficiente frente a cualquier situación que afecte el funcionamiento del sistema.

Asimismo, el proceso de diagnóstico permitió analizar las posibles causas de los problemas detectados, descartando aquellas que no eran probables y enfocándose en los elementos que realmente podían estar generando la falla. Este análisis permitió comprender que muchas veces los problemas de red pueden originarse tanto en configuraciones incorrectas de los dispositivos como en condiciones de funcionamiento que afectan el rendimiento de la infraestructura, especialmente cuando se presentan altos niveles de tráfico en determinados puntos de la red.

La aplicación de soluciones constituyó una etapa clave dentro del proceso de administración de fallas, ya que permitió implementar acciones correctivas orientadas a restablecer el funcionamiento adecuado de la red. En este proceso se verificó la importancia de repetir las pruebas antes y después de aplicar una solución, con el fin de confirmar que el problema había sido realmente corregido y que no se trataba de un error ocasionado por el operador o por condiciones temporales del sistema.

De igual manera, la administración de fallas permitió comprender la necesidad de realizar un monitoreo constante del estado de la red, registrando los eventos que puedan afectar su funcionamiento y estableciendo procedimientos que permitan detectar y solucionar los problemas de manera oportuna. Este proceso contribuye significativamente a mejorar la confiabilidad, disponibilidad y eficiencia de los servicios de comunicación dentro de una organización.

Finalmente, el desarrollo de esta actividad permitió fortalecer los conocimientos relacionados con la gestión y administración de redes, así como con el uso de herramientas de simulación como GNS3 para la evaluación del rendimiento y la detección de fallas en infraestructuras de red. Este tipo de prácticas resulta fundamental para la formación en el área de gestión de redes de datos, ya que permite aplicar los conceptos teóricos en escenarios prácticos que simulan situaciones reales dentro de una organización.

Registro fotográfico del proceso de pruebas: (para los 3 informes)

***Nota:** Se trabajo con la herramienta GNS3 la cual nos presentó una serie de errores, impidiendo terminar el proceso de capturas de pantalla de los procesos de pruebas. A la hora de tomar las capturas de pantalla GNS3 presento un error grave el cual daño el archivo de la topología realizada. Se informo la problemática a la instructora y para completar la evidencia se deja claridad de lo sucedido para poder responder este punto del informe:*

Durante el proceso de instalación, configuración y uso de la herramienta GNS3 se presentaron múltiples problemáticas de carácter técnico que afectaron significativamente el desarrollo de las prácticas de simulación de red.

En primera instancia, se evidenciaron fallas durante la descarga e instalación del software. El instalador presentó interrupciones constantes, deteniéndose a mitad del proceso o generando errores inesperados, lo que obligó a repetir la instalación en varias ocasiones. Este comportamiento puede estar asociado a problemas de conectividad, incompatibilidad del sistema operativo o conflictos con dependencias necesarias como WinPcap/Npcap o componentes de virtualización.

Posteriormente, al crear una topología de red dentro del entorno de GNS3, se logró guardar el archivo correctamente; sin embargo, al intentar abrirlo nuevamente, el proyecto no mostraba ningún dispositivo ni configuración previamente realizada. Esto sugiere posibles fallos en la persistencia de datos, corrupción del archivo de proyecto (.gns3) o errores en la ruta de almacenamiento.

Adicionalmente, la herramienta comenzó a presentar inestabilidad general, afectando su rendimiento. Uno de los problemas más relevantes fue la imposibilidad de integrar dispositivos inalámbricos dentro de la topología, limitando así la simulación de escenarios más completos. Esto puede deberse a la falta de soporte nativo de GNS3 para dispositivos wireless o a la ausencia de imágenes compatibles.

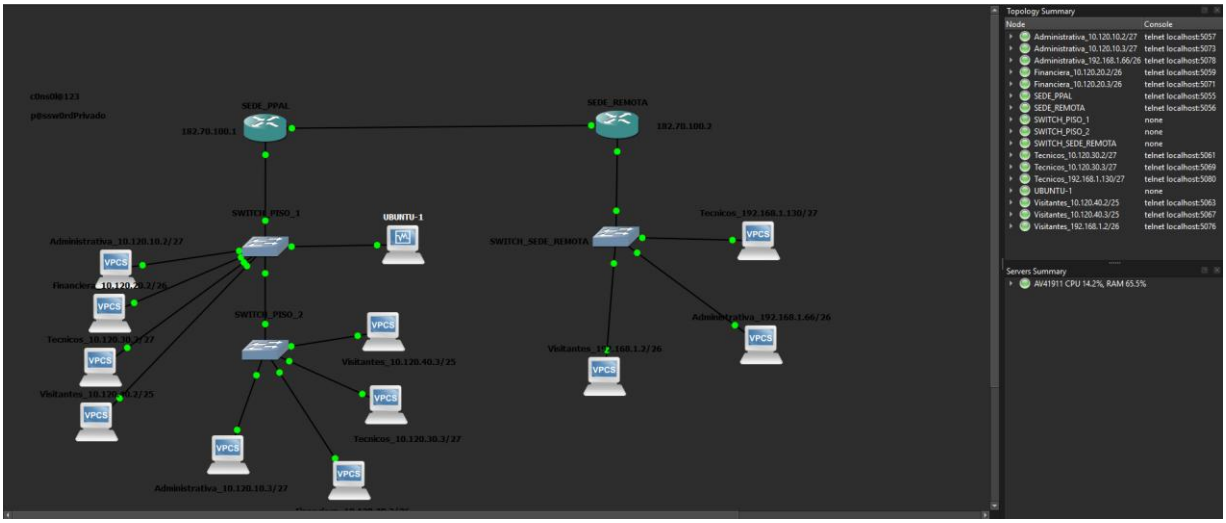
Se intentó mejorar el rendimiento mediante el uso de máquinas virtuales (GNS3 VM); sin embargo, surgieron errores de comunicación entre la aplicación principal y la máquina virtual. En varios casos, la VM no respondía correctamente, lo cual puede estar relacionado con una mala configuración de hipervisores como VMware o VirtualBox, problemas de recursos (RAM/CPU) o errores en la integración de red (adaptadores virtuales).

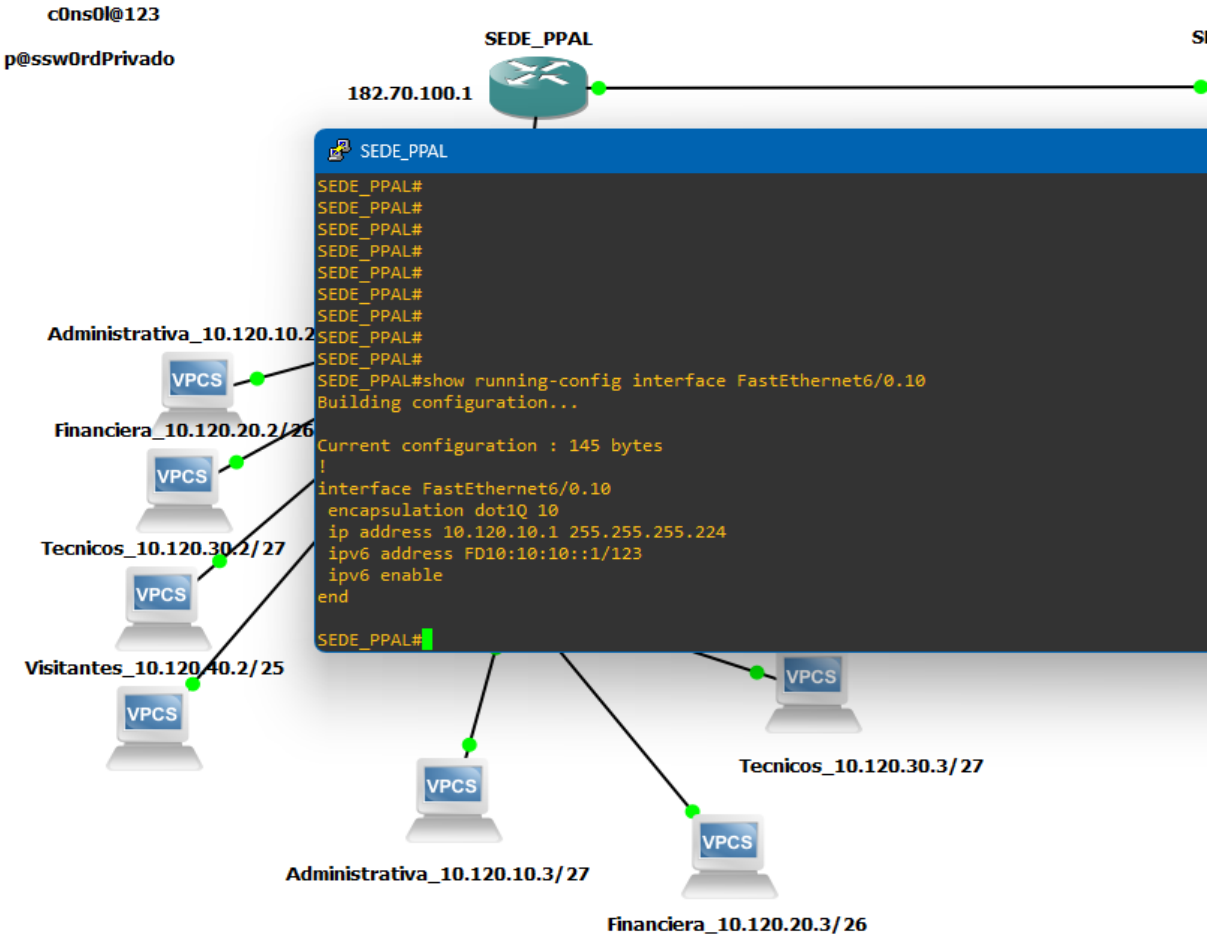
En cuanto a la configuración de dispositivos, específicamente routers, se presentaron fallos en la asignación y verificación de direcciones IP. A pesar de ingresar correctamente los parámetros de configuración, no se obtenía respuesta en pruebas de conectividad, lo que indica posibles errores en la configuración de interfaces, falta de activación de las mismas (shutdown/no shutdown), o problemas en la topología lógica.

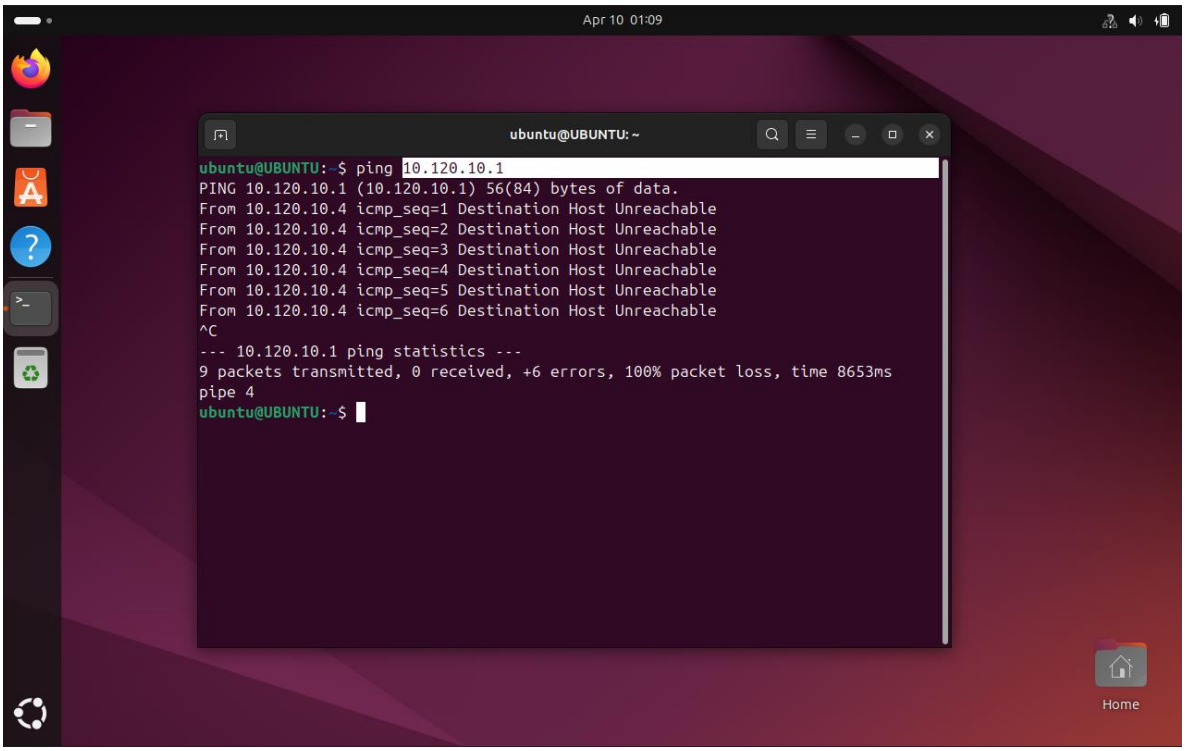
Debido a la acumulación de errores, se procedió a desinstalar la herramienta. No obstante, al intentar realizar una nueva instalación, GNS3 no lograba ejecutarse correctamente, lo que sugiere que quedaron residuos de instalaciones anteriores en el sistema, conflictos en el registro o problemas con componentes previamente instalados.

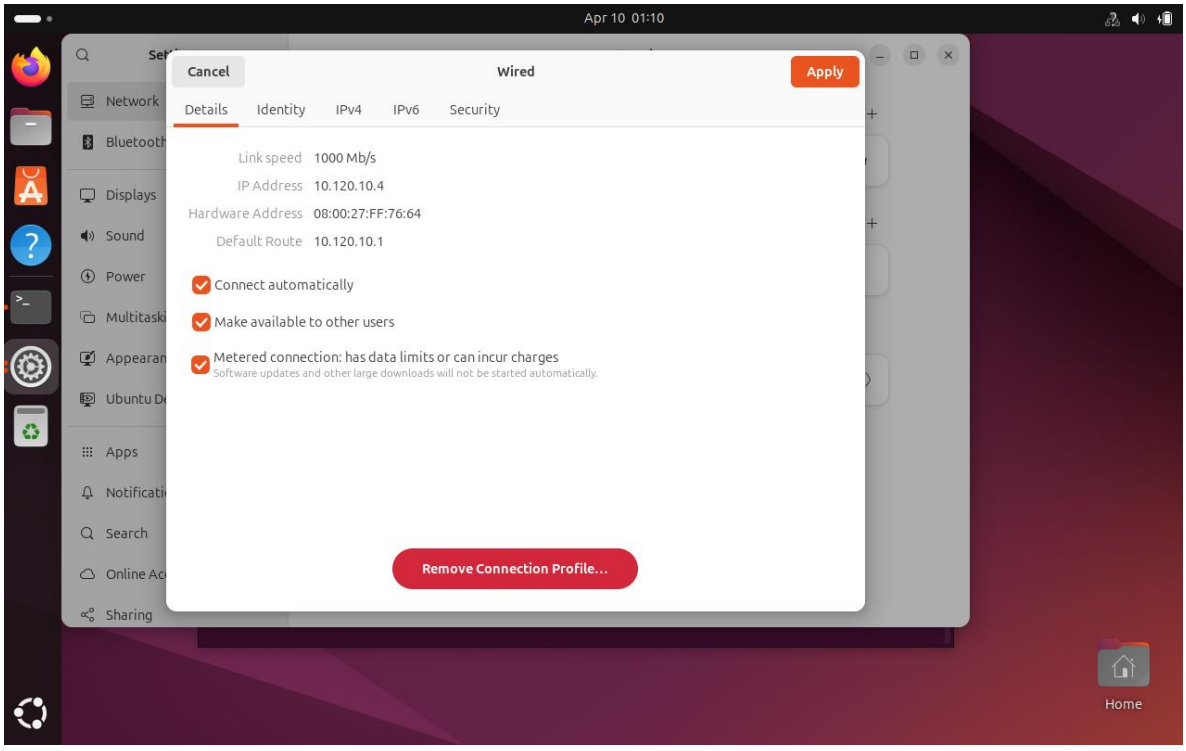
Finalmente, las problemáticas presentadas abarcan desde errores en la instalación, fallos en la gestión de proyectos, limitaciones funcionales, problemas de virtualización y errores en la configuración de red, lo que impidió el correcto desarrollo de las actividades planteadas en la herramienta GNS3.



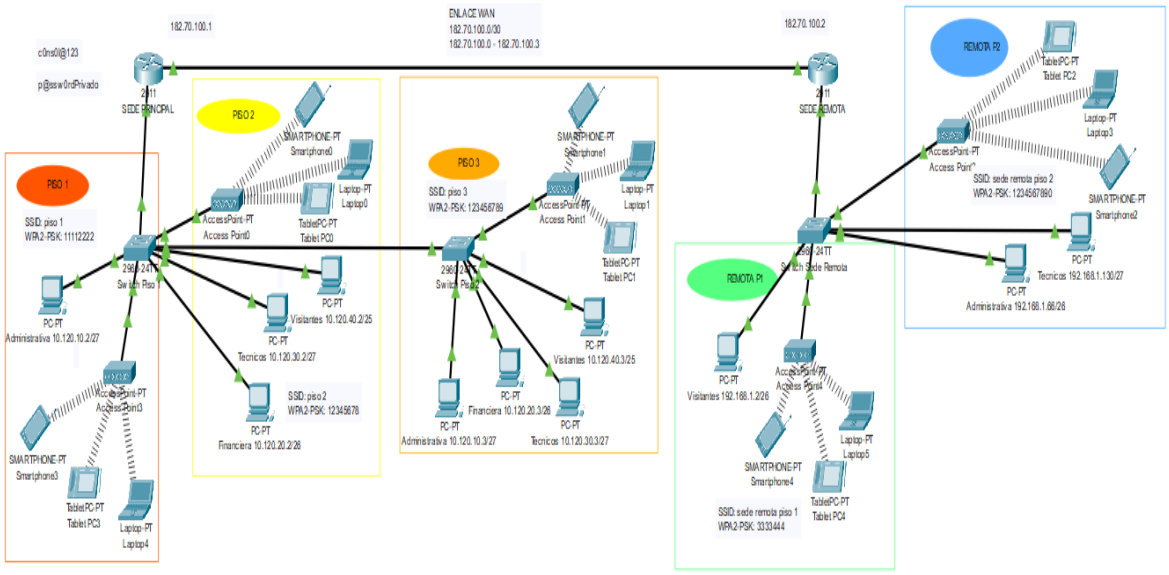

c0ns0l@123
p@ssw0rdPrivado
SEDE_PPAL
182.70.100.1
SEDE_REMOTA
182.70.100.2
SWITCH_PISO_1
UBUNTU-1
SWITCH_SEDE_REMOTA
SWITCH_PISO_2
Administrativa_10.120.10.2/27
Tecnicos_192.168.1.130/27
Visitantes_10.120.40.3/25
Tecnicos_10.120.30.3/27
Administrativa_10.120.10.3/27
Topology Summary
Node
Console
Servers Summary

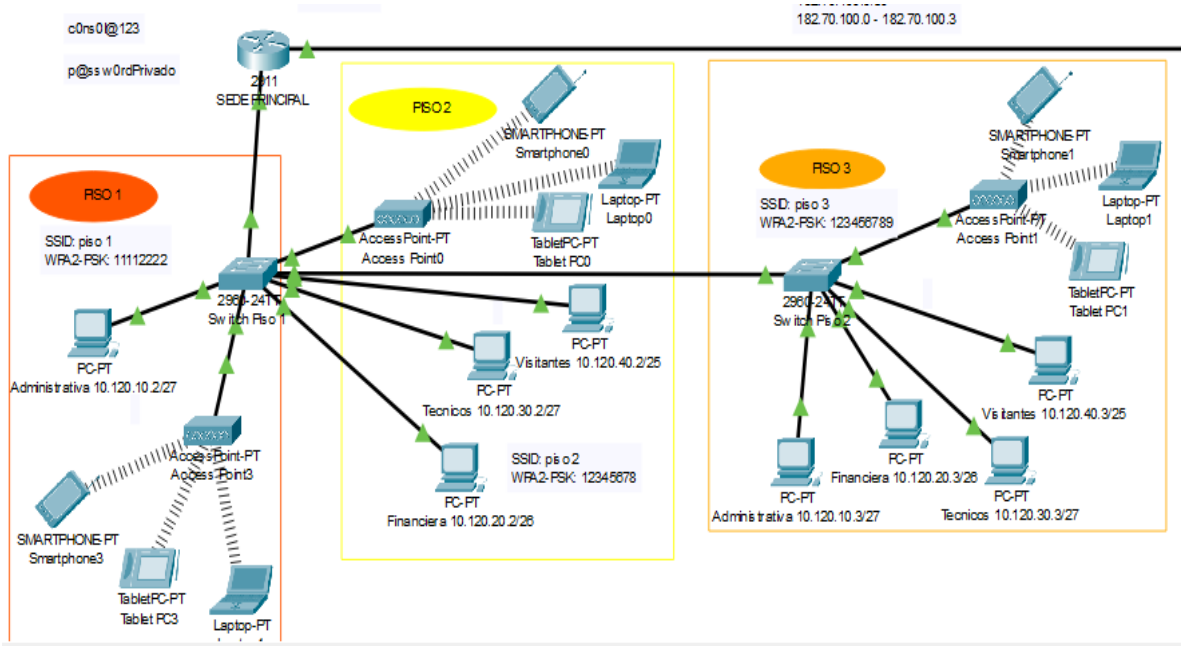

c0ns0l@123
p@ssw0rdPrivado
SEDE_PPAL
182.70.100.1
SEDE_PPAL
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#
SEDE_PPAL#show running-config interface FastEthernet6/0.10
Building configuration...
Current configuration : 145 bytes
!
interface FastEthernet6/0.10
encapsulation dot1Q 10
ip address 10.120.10.1 255.255.255.224
ipv6 address FD10:10:10::1/123
ipv6 enable
end
SEDE_PPAL#
Administrativa_10.120.10.2
Financiera_10.120.20.2/26
Tecnicos_10.120.30.2/27
Visitantes_10.120.40.2/25
Tecnicos_10.120.30.3/27
Administrativa_10.120.10.3/27
Financiera_10.120.20.3/26
VPCS

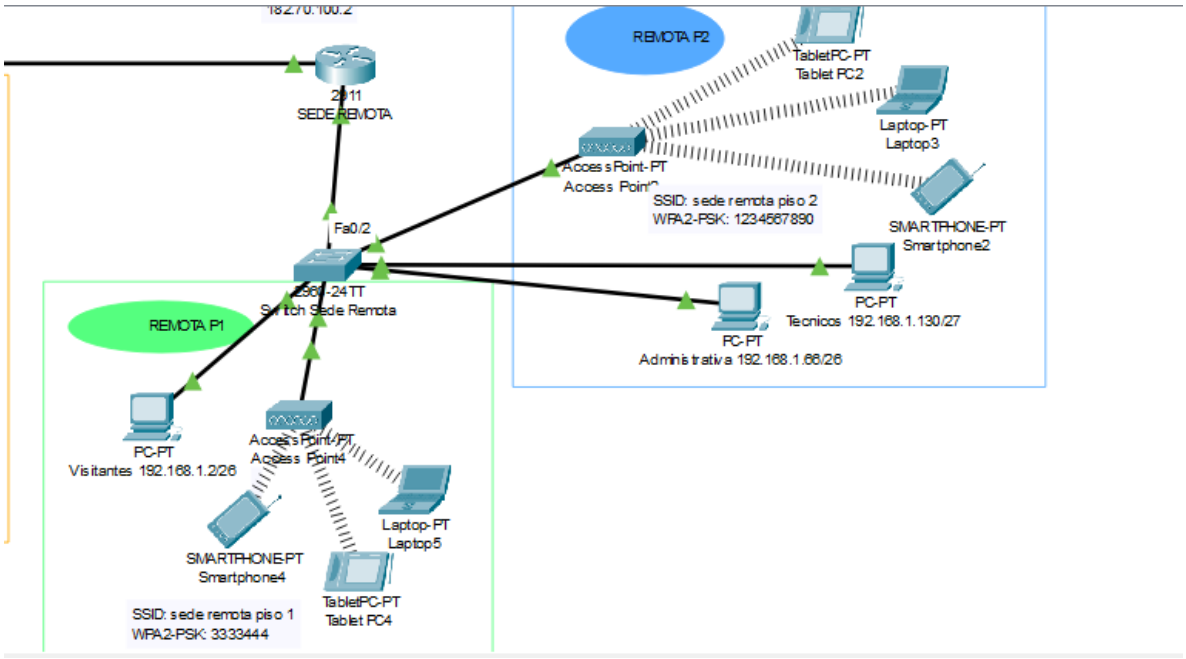

Apr 10 01:09
ubuntu@UBUNTU: ~
ubuntu@UBUNTU:~$ ping 10.120.10.1
PING 10.120.10.1 (10.120.10.1) 56(84) bytes of data.
From 10.120.10.4 icmp_seq=1 Destination Host Unreachable
From 10.120.10.4 icmp_seq=2 Destination Host Unreachable
From 10.120.10.4 icmp_seq=3 Destination Host Unreachable
From 10.120.10.4 icmp_seq=4 Destination Host Unreachable
From 10.120.10.4 icmp_seq=5 Destination Host Unreachable
From 10.120.10.4 icmp_seq=6 Destination Host Unreachable
^C
--- 10.120.10.1 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 8653ms
pipe 4
ubuntu@UBUNTU:~$
Home


Apr 10 01:10
Cancel
Wired
Apply
Details
Identity
IPv4
IPv6
Security
Link speed 1000 Mb/s
IP Address 10.120.10.4
Hardware Address 08:00:27:FF:76:64
Default Route 10.120.10.1
Connect automatically
Make available to other users
Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.
Remove Connection Profile...
Network
Displays
Sound
Power
Apps
Search
Sharing
Home

Dato: *Para complementar la información la topología realizada en GNS3 se basó en la topología realizada en cisco packet tracer por ende se muestra captura de pantalla de la topología realizada con esa herramienta que fue lo que se planteo con la instructora. La topología de red cuenta con todos los equipos de la empresa Enter Ltda, la cual cuenta con una sede principal y una sede remota.*







Bibliografía:

https://zajuna.sena.edu.co/Repositorio/Titulada/institution/SENA/CienciasNaturales/228183/Contenido/OVA/CF10/index.html#/

https://www.plc-hmi-scadas.com/blog/redes-gns3-tormenta-de-broadcast-y-protocolo-stp/

https://eaglepubs.erau.edu/masteringenterprisenetworkslabs2edition/chapter/setting-up-gns3/

https://www.ninjaone.com/es/blog/que-es-deteccion-de-redes/

https://www.manageengine.com/latam/netflow/deteccion-de-anomalias-de-red.html

https://netwgeeks.com/introduccion-a-gns3/

INSTRUMENTO DE EVALUACIÓN

1. DATOS GENERALES

Programa de formación	Gestión de redes de datos
Proyecto formativo	Planeación, implementación y gestión de infraestructura informática en el sector Mipyme para la mejora de la productividad, desarrollo e innovación.
Fase proyecto	Evaluación
Resultado de aprendizaje	**220501106-04** - Gestionar los dispositivos de cómputo y servicios de red para garantizar el funcionamiento de la plataforma tecnológica.
Actividad de aprendizaje	**GA9-220501106-AA2** - Declarar e implementar políticas que ofrezcan alta disponibilidad y de acceso a los diferentes servicios existentes en la red, de acuerdo con protocolos técnicos.
Evidencia de producto	Informe de actualización de componentes de *hardware* y *software* de los equipos de cómputo. **GA9-220501106-AA2-EV02.**

Criterios de evaluación

- Elabora la documentación técnica de los dispositivos de cómputo y sistemas operativos según políticas y recomendaciones.
- Establece estrategias de mejora continua del servicio para garantizar y optimizar los niveles de operatividad acordados en la solución.
- Documenta la bitácora de eventos de la infraestructura y las plataformas de acuerdo a las políticas establecidas.
- Realiza la actualización de componentes de *hardware* y *software* de los equipos de cómputo según especificaciones del proveedor.
- Administra las plataformas de gestión y supervisión de los componentes y servicios en ambientes *on-premise* y/o en la nube según buenas prácticas y recomendaciones.

INSTRUMENTO DE EVALUACIÓN

2. RÚBRICA

Criterios	Excelente	Bueno	Deficiente	Total
Estructura del informe	El documento contiene una excelente presentación, se entrega en el formato adecuado con todo lo solicitado.	Aunque el documento presenta una estructura base, la misma carece de algunos elementos del cuerpo solicitado.	No tuvo en cuenta las normas básicas para la presentación del trabajo.	
Máximo 5 puntos	**5 puntos**	**2 puntos**	**0 puntos**	
Fines de la actividad	El documento da respuesta a todos los requerimientos de las actividades propuestas de acuerdo a lo solicitado en la guía. Los aportes por parte del aprendiz son significativos.	El documento da respuesta a la mayoría de los requerimientos de las actividades propuestas de acuerdo a lo solicitado en la guía. Los aportes por parte del aprendiz son importantes, pero podría mejorar su proceso de apropiación.	El documento no da respuesta a los requerimientos de las actividades propuestas.	
Máximo 60 puntos	**60 puntos**	**30 puntos**	**0 puntos**	
Aprendizajes obtenidos	Se identifica una reflexión acerca de los aprendizajes	Se identifican ideas vagas que permiten ver algunos de los	En ningún apartado o momento se	

INSTRUMENTO DE EVALUACIÓN

Criterios	Excelente	Bueno	Deficiente	Total
	obtenidos durante la sesión de trabajo.	aprendizajes que se obtuvo durante la sesión de trabajo.	identifican los aprendizajes dentro del proceso de las actividades durante la sesión de trabajo.	
Máximo 20 puntos	**20 puntos**	**10 puntos.**	**0 puntos.**	
Ortografía, puntuación y gramática	La redacción es excelente, las ideas están correlacionadas, el texto es coherente en su totalidad. Su ortografía es adecuada.	La redacción del documento articula medianamente las ideas y no se usa conectores apropiadamente. Además, presenta: de cuatro a seis errores ortográficos o de puntuación o de cuatro a seis errores gramaticales.	El documento presenta deficiencias en redacción y errores ortográficos.	
Máximo 10 puntos	**10 puntos**	**5 puntos.**	**2 puntos.**	
Bibliografía / webgrafía	Incluye más de dos fuentes de información y las cita según las normas APA.	Incluye solo una fuente de información y la cita según las normas APA.	No cita ni utiliza fuentes de información.	
Máximo 5 puntos	**5 puntos**	**2 puntos.**	**0 puntos**	

INSTRUMENTO DE EVALUACIÓN

3. EVALUACIÓN

Observaciones: _____

Juicio de valor: _____

***Nombre**: Jhojan stiven jaramillo.*

***Nombre:** Yuri cuervo.*

***Programa:** Gestión de Redes de Datos.*

***Ficha de caracterización:** 3118456.*

***Instructora:** Sandra Zapata.*

Evidencia GA9-220501106-AA2-EV02. Informe de actualización de componentes de hardware y software de los equipos de cómputo.

Para esta actividad se sigue con la estrategia del aprendizaje basado en proyectos, en el cual se resolverá el problema de aplicación de la actividad correspondiente a la sede principal en el edificio de 3 pisos y la sede remota en un edificio de 2 pisos.

Con base en los listados de los dispositivos de cómputo necesarios en cada una de las dos sedes de la empresa Enter Ltda., el aprendiz debe elaborar la documentación técnica de los dispositivos de cómputo y sistemas operativos según políticas y recomendaciones, realizar la actualización de componentes de hardware y software de los equipos de cómputo, según especificaciones del proveedor, y con esta información presentar un informe de actualización de componentes de hardware y software de los equipos de cómputo.

Se toma información de evidencias anteriores, las cuales se plantearon en la grabación sincrónica para complementar la información del informe propuesto.

Contenido:

- *Documentación técnica de los equipos de cómputo y sistemas operativos de las 2 sedes - Listado de equipos de cómputo, sistemas operativos a instalar y su importancia.*
- *Listado de verificación para canales de comunicación inalámbrica.*
- *Listado sobre el análisis de riesgo y matriz de riesgo.*
- *Evidencia de actualización de componentes de hardware y software de los equipos de cómputo, según especificaciones del proveedor.*
- *Listado de los equipos existentes con sus especificaciones actuales.*
- *Propuesta de actualización de Hardware.*
- *Propuesta de actualización de Software.*
- *Ventajas de la solución propuesta.*
- *Cronograma y presupuesto.*
- *Registro fotográfico del proceso de actualización de los equipos.*
- *Recomendaciones y Conclusiones.*
- *Bibliografía.*



Introducción:

En la actualidad, el correcto funcionamiento de las infraestructuras tecnológicas depende en gran medida de la adecuada gestión y actualización de los componentes de hardware y software de los equipos de cómputo. Mantener los sistemas actualizados no solo permite mejorar el rendimiento y la eficiencia operativa, sino que también contribuye significativamente a fortalecer la seguridad de la información, reducir vulnerabilidades y garantizar la continuidad de los servicios dentro de una organización.

En el desarrollo de esta evidencia, se abordó el proceso de documentación técnica y actualización de los equipos de cómputo pertenecientes a la empresa Enter Ltda., la cual cuenta con una sede principal distribuida en tres pisos y una sede remota de dos pisos. Este proceso incluyó la identificación de los dispositivos existentes, la verificación de sus características técnicas y la aplicación de mejoras tanto a nivel de hardware como de software, siguiendo las recomendaciones de los fabricantes y las buenas prácticas en administración de redes.

Para la validación de los procedimientos y el análisis del comportamiento de la red, se emplearon herramientas tecnológicas como GNS3, cisco packet tracer, que permitieron simular un entorno real de red, dentro de los cuales facilitaron la configuración, gestión y actualización de los equipos de red. Estas herramientas fueron fundamentales para recrear escenarios de operación, evaluar el impacto de las actualizaciones y garantizar que los cambios realizados no afectaran la estabilidad del sistema.

Asimismo, este informe presenta de manera estructurada la información correspondiente a las actualizaciones realizadas, evidenciando los cambios aplicados, las versiones de software implementadas y las mejoras en los componentes de hardware. De esta forma, se busca demostrar la importancia de llevar un control adecuado de los procesos de actualización como parte fundamental de la administración de redes, contribuyendo a una infraestructura más eficiente, segura y alineada con las necesidades organizacionales.

Documentación técnica de los equipos de cómputo y sistemas operativos de las 2 sedes:

- ***Descripción general de la infraestructura:*** *La infraestructura tecnológica de la empresa Enter Ltda. está compuesta por dos sedes: una sede principal distribuida en tres pisos y una sede remota de dos pisos. Ambas sedes cuentan con equipos de cómputo, dispositivos de red y sistemas operativos que permiten la comunicación, el acceso a servicios y la correcta operación de las actividades empresariales.*
  Para el diseño, configuración y validación de esta infraestructura, se utilizaron herramientas de simulación como ***GNS3*** *y* ***Cisco Packet Tracer****, las cuales permitieron recrear un entorno de red realista, implementar configuraciones en dispositivos Cisco y evaluar el comportamiento de la red ante diferentes escenarios.*

- ***Listado de equipos de cómputo para las dos sedes:***

SEDE	*AREA/PISO*	*TIPO DE EQUIPO: MESA*	*TIPO DE EQUIPO: PORTATIL*	*CARACTERISTICAS*
Principal	*Sala de internet (piso 1)*	*20*	*N/A*	*Intel i5, 8GB RAM, 512GB SSD, Windows 10 Pro*
Principal	*Sala de espera (piso2)*	*2*	*2*	*Intel i3/i5, 4–8GB RAM, Windows 10 Pro*
Principal	*Recepción (piso 2)*	*1*	*N/A*	*Intel i3, 4GB RAM, Windows 10 Home*
Principal	*Gerencia administrativa (piso 2)*	*1*	*N/A*	*Intel i5, 8GB RAM, Windows 11 Pro*
Principal	*Sala de conferencias (piso 2)*	*1*	*1*	*Intel i5, 8GB RAM, Windows 10 Pro*
Principal	*Empleado temporal (piso 2)*	*1*	*N/A*	*Intel i3, 4GB RAM, Ubuntu 22.04*
Principal	*Área central para usuarias (piso 1)*	*N/A*	*2*	*Intel i5, 8GB RAM, Windows 11 Pro*
Principal	*Contabilidad (piso 3)*	*1*	*N/A*	*Intel i5, 8GB RAM, Windows 11 Pro*
Principal	*Tesorería (piso 3)*	*1*	*N/A*	*Intel i5, 8GB RAM, Windows 10 Pro*
Principal	*Recursos humanos (Piso 3)*	*2*	*N/A*	*Intel i3, 4GB RAM, Windows 10 Home*
Principal	*Bodega (piso 3)*	*1*	*N/A*	*Intel i3, 4GB RAM, Ubuntu 20.04*
Principal	*Sala de conferencias (piso 3)*	*1*	*1*	*Intel i5, 8GB RAM, Windows 10 Pro*
Principal	*Cuarto de telecomunicaciones (piso 1,2,3)*	*N/A*	*2*	*Windows Server / Linux Server*
Remota	*Sala de espera (piso 1)*	*1*	*N/A*	*Intel i5, 8GB RAM, Windows 10 Pro*
Remota	*Recepción (piso 1)*	*1*	*N/A*	*Intel i3, 4GB RAM, Windows 10 Home*
Remota	*Sala de conferencias (piso 1)*	*1*	*1*	*Intel i5, 8GB RAM, Windows 10 Pro*
Remota	*Sala de conferencias (piso 2)*	*1*	*1*	*Intel i5, 8GB RAM, Windows 10 Pro*
Remota	*Administrativos (piso 2)*	*2*	*2*	*Intel i3, 4GB RAM, Windows 10 Home*
Remota	*Técnicos (piso 2)*	*1*	*2*	*Intel i5, 8GB RAM, 512GB SSD, Windows 10 Pro*
Remota	*Visitantes (piso 1)*	*2*	*N/A*	*Intel i3, 4GB RAM, Ubuntu 20.04*
Remota	*Cuarto de telecomunicaciones (piso 1,2)*	*N/A*	*2*	*Windows Server / Linux Server*

- ***Otros dispositivos:***

SEDE	*AREA/PISO*	*DISPOSITIVO*	*CANTIDAD*	*OBSERVACIONES*
Principal	*Sala de internet (piso 1)*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Sala de internet (piso 1)*	*Smart TV 52 pulgadas*	*1*	*Servicio cableado, uso para presentaciones compatibles con dispositivos movibles.*
Principal	*Área central (piso 1)*	*Tablets*	*2*	*Conexión WIFI corporativa, uso en actividades administrativas.*
Principal	*Área central (piso 1)*	*Smartphones*	*2*	*Conexión WIFI y datos móviles.*
Principal	*Todas las áreas (piso 1,2,3)*	*Teléfonos IP*	*Extensiones en todas las áreas*	*Comunicaciones internas y extensiones en todas las áreas.*
Principal	*Gerencia administrativa (piso 2)*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Sala de conferencia (piso 2)*	*Proyector*	*1*	*Para presentaciones y capacitaciones.*
Principal	*Sala de conferencia (piso 2)*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Recursos humanos (piso 3)*	*Smartphones*	*4*	*Conexión WIFI y datos móviles.*
Principal	*Recursos humanos (piso 3)*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Recursos humanos (piso 3)*	*Tablets*	*4*	*Conexión WIFI corporativa, uso en actividades administrativas.*
Principal	*Bodega*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Sala de conferencia (piso 3)*	*Proyector*	*1*	*Para presentaciones y capacitaciones.*
Principal	*Sala de conferencia (piso 3)*	*Impresora multifuncional*	*1*	*Conexiones LAN compartidas en red, uso administrativo y de soporte.*
Principal	*Todas las áreas (piso 1,2,3)*	*Cámaras de vigilancia*	*extensiones en todas las áreas.*	*Monitoreo de seguridad en todas las áreas.*
Principal	*General*	*Access point*	*Según cobertura.*	*Para uso corporativo y para visitantes.*

SEDE	AREA/PISO	DISPOSITIVO	CANTIDAD	OBSERVACIONES
Remota	Sala de espera (piso 1)	Smart TV	1	Conexiones LAN compartidas en red, uso administrativo y de soporte.
Remota	Recepción (piso 1)	Impresora multifuncional	1	Conexiones LAN compartidas en red, uso administrativo y de soporte.
Remota	Recepción (piso 1)	Tablets	2	Conexión WIFI corporativa, uso en actividades administrativas.
Remota	Sala de conferencias (piso 1)	Proyector	1	Para presentaciones y capacitaciones.
Remota	Sala de conferencias (piso 2)	Impresora multifuncional	1	Conexiones LAN compartidas en red, uso administrativo y de soporte.
Remota	Sala de conferencias (piso 2)	Tablets	6	Conexión WIFI corporativa, uso en actividades administrativas.
Remota	Sala de conferencias (piso 1)	Impresora multifuncional	1	Conexiones LAN compartidas en red, uso administrativo y de soporte.

- ***Importancia del listado de los equipos de cómputo:***

El listado de equipos de cómputo dentro de una organización cumple un papel fundamental en la gestión de la infraestructura tecnología. Este tipo de inventario no solo permite conocer la cantidad de dispositivos disponibles, sino también las características técnicas de cada uno, lo cual facilita la planeación, el mantenimiento y la actualización de la red corporativa. Contar con un registro detallado de los equipos de escritorio, portátiles y servidores instalados en las diferentes áreas de la empresa ayuda a identificar con claridad los recursos asignados a cada dependencia. Esto permite garantizar que los trabajadores cuenten con herramientas de acuerdo con sus funciones, evitando la sobrecarga de algunos equipos o la falta de disponibilidad en otros casos.

Además, el listado se convierte en un insumo clave para el área de soporte técnico, ya que con base en él es posible realizar diagnósticos más agiles, planificar mantenimientos preventivos y corregir fallas de manera oportuna. Así mismo, contribuye a prever necesidades de renovación tecnológica, ya que permite detectar equipos obsoletos o que no cumplen con los requerimientos de los sistemas operativos y aplicaciones actuales.

Otro aspecto relevante es la seguridad informática. Conocer exactamente que dispositivos hacen parte de la red ayuda a controlar los accesos, aplicar políticas de seguridad, mantener actualizados los parches del sistema y reducir riesgos asociados a vulnerabilidades. Un inventario actualizado es también un apoyo en auditorias y procesos de certificación, donde se exige la evidencia de control sobre los recursos tecnológicos.

Finalmente, el listado de los equipos de cómputo respalda la toma de decisiones administrativas y financieras, ya que facilita la elaboración de presupuestos, la adquisición de licencias de software acordes al número de dispositivos y la proyección de inversiones en tecnología. En este sentido, no solo es un documento técnico, sino una herramienta estratégica que aporta al crecimiento, continuidad y eficiencia de la empresa.

Nota: para completar la información de los dispositivos:

ELEMENTO/DISPOSITIVO	*CARACTERISTICAS*	*DISPOSITIVO QUE GESTIONA*
Router VoIP	Facilita la comunicación telefónica a través de Internet, mejorando la calidad de las llamadas y la funcionalidad de las redes VoIP.	Gestiona conexión a internet, seguridad en la red, calidad de servicio QoS. configuración y monitoreo.
Modem ips	Dispositivo de seguridad de red que monitorea el tráfico de datos y detecta actividades maliciosas, como ataques, para bloquearlas y prevenir que ingresen a la red.	Gestiona conexión a internet, gestión del tráfico, asignación de direcciones ip y seguridad.
Switch PoE de 24 pines	Interconecta dispositivos en una red local (LAN), permitiendo la comunicación entre ellos.	Gestiona conectividad de red, alimentacion PoE, gestión de tráfico, priorización de tráfico y seguridad.
Softphones	Software que simulan un teléfono tradicional, permitiendo realizar y recibir llamadas a través de la computadora o dispositivo móvil, utilizando la conexión a internet. Ofrecen funcionalidades como desvío de llamadas, buzón de voz, grabación de llamadas, mensajería instantánea, videoconferencias y más.	Gestiona las llamadas de voz, transferencia de llamadas, conferencia de llamadas, directorio de contactos historial de llamadas y configuración del perfil.
Router inalámbrico	Es un dispositivo que permite la conexión a Internet de manera inalámbrica a través de ondas de radio, eliminando la necesidad de cables. Además de ofrecer conexión Wi-Fi, también actúa como un enrutador, distribuyendo la señal de Internet a dispositivos conectados a sus puertos Ethernet.	Gestiona la conexión de los dispositivos inalámbricos, seguridad en la red, configuración y monitoreo.
Emisores WI-FI	Sus características principales incluyen la capacidad de transmitir datos a diferentes velocidades, y la implementación de diferentes protocolos de seguridad para proteger la red.	Gestiona la transmisión WI-FI, gestiona el tráfico y la seguridad.
Access point	Es un dispositivo que crea una red de área local inalámbrica (WLAN), generalmente en una oficina o edificio grande, conectándose a un router cableado mediante Ethernet para extender la señal Wi-Fi.	Gestiona el WI-FI para dispositivos inalámbricos.

- ***Listado de sistemas operativos a instalar:***

SEDE	*SISTEMA OPERATIVO*	*AREA/PISO*	*TIPO EQUIPO: MESA*	*TIPO EQUIPO: PORTATIL*	*CARACTERISTICAS*
Principal	*Windows 10 Pro*	*Sala de internet (piso1)*	*20*	*N/A*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Principal	*Windows 10 Pro*	*Sala de espera (piso2)*	*2*	*2*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Principal	*Windows 10 Home*	*Recepción (piso 2)*	*1*	*N/A*	Versión básica enfocada en el uso doméstico y de oficina ligera, con interfaz sencilla y soporte general.
Principal	*Windows 11 Pro*	*Gerencia administrativa (piso2)*	*1*	*N/A*	Incorpora una interfaz moderna, mayor integración con la nube y herramientas de productividad empresarial.
Principal	*Windows 10 Pro*	*Sala de conferencias (piso 2)*	*1*	*1*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Principal	*Ubuntu 22.04*	*Empleado temporal (piso2)*	*1*	*N/A*	Sistema operativo Linux confiable, abierto, estable, ligero, versátil y seguro con soporte a largo plazo (LTS), buen rendimiento, ideal para equipos de escrito como para servidores.
Principal	*Windows 11 Pro*	*Área central (piso1)*	*N/A*	*2*	Incorpora una interfaz moderna, mayor integración con la nube y herramientas de productividad empresarial.
Principal	*Windows 11 Pro*	*Contabilidad (piso3)*	*1*	*N/A*	Incorpora una interfaz moderna, mayor integración con la nube y herramientas de productividad empresarial.
Principal	*Windows 10 Pro*	*Tesorería (piso3)*	*1*	*N/A*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Principal	*Windows 10 Home*	*Recursos humanos (piso3)*	*2*	*N/A*	Versión básica enfocada en el uso doméstico y de oficina ligera, con interfaz sencilla y soporte general.
Principal	*Ubuntu 20.04*	*Bodega (piso3)*	*1*	*N/A*	Sistema operativo Linux confiable, abierto, estable, ligero, versátil y seguro con soporte a largo plazo (LTS), buen rendimiento, ideal para equipos de escrito como para servidores.
Principal	*Windows 10 Pro*	*Sala de conferencias (piso3)*	*1*	*1*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Principal	*Windows server / Linux server.*	*Cuarto de telecomunicaciones (piso 1,2,3)*	*N/A*	*2*	Diseñados para la gestión de redes, usuarios, almacenamiento y servicios críticos de infraestructura.

SEDE	*SISTEMA OPERATIVO*	*AREA/PISO*	*TIPO EQUIPO: MESA*	*TIPO EQUIPO: PORTATIL*	*CARACTERISTICAS*
Remota	*Windows 10 Pro*	*Sala de espera (piso1)*	*1*	*N/A*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Remota	*Windows 10 Home*	*Recepción (piso1)*	*1*	*N/A*	Versión básica enfocada en el uso doméstico y de oficina ligera, con interfaz sencilla y soporte general.
Remota	*Windows 10 Pro*	*Sala de conferencias (piso1)*	*1*	*1*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Remota	*Windows 10 Pro*	*Sala de conferencias (piso2)*	*1*	*1*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Remota	*Windows 10 Home*	*Administrativos (piso2)*	*2*	*2*	Versión básica enfocada en el uso doméstico y de oficina ligera, con interfaz sencilla y soporte general.
Remota	*Windows 10 Pro*	*Técnicos (piso2)*	*1*	*2*	Ofrece seguridad avanzada, control de dispositivos y administración de redes, ideal para entornos empresariales.
Remota	*Ubuntu 20.04*	*Visitantes (piso1)*	*2*	*N/A*	Sistema operativo Linux confiable, abierto, estable, ligero, versátil y seguro con soporte a largo plazo (LTS), buen rendimiento, ideal para equipos de escrito como para servidores.
Remota	*Windows server/Linux server*	*Cuarto de telecomunicaciones (piso 1,2)*	*N/A*	*2*	Diseñados para la gestión de redes, usuarios, almacenamiento y servicios críticos de infraestructura.

- ***Importancia del Listado de sistemas operativos a instalar:***

Es un elemento fundamental dentro de la planeación tecnológica y la gestión de recursos informáticos. Este documento no solo organiza y detalla que software se implementara en cada equipo, sino que también garantiza la homogeneidad, compatibilidad y eficiencia en los procesos internos. Tener claridad sobre los sistemas operativos permite asegurar que cada área de la organización cuente con la plataforma adecuada según sus necesidades, ya sea para tareas administrativas, de gestión financiera, de atención al cliente o de soporte técnico.

Además, un listado bien estructurado facilita el control y mantenimiento de los equipos, evitando confusiones o errores al momento de actualizaciones, instalación de programas o resolución de fallas. Esto también contribuye a la seguridad informática, ya que permite identificar que versiones están en uso y planificar oportunamente las actualizaciones y parches de seguridad.

En términos de productividad, disponer de un inventario de los sistemas operativos ayuda a reducir tiempos de soporte, estandarizar configuraciones y mejorar la capacitación de los usuarios, pues se trabaja con entornos conocidos y unificados. En conclusión, contar con este listado no solo es un requisito organizativo, sino una herramienta estratégica que apoya el buen funcionamiento, seguridad y crecimiento tecnológico de la empresa.

Listado de verificación para canales de comunicación inalámbrica:

Access point (ubicación)	***ssid de red***	***No. canal***	***Sí cumple***	***No cumple***	***Observaciones***
piso 1	piso 1	Canal #6	✓	*N/A*	*SSID configurado correctamente, se configuro WPA2-PSK con contraseña segura (11112222), conexión DHCP IPV4 asignada correctamente al dispositivo inalámbrico. Conexión inalámbrica funcional y segura. En los ACCESS POINT se configuraron los canales de forma alternada para evitar interferencias entre redes inalámbricas cercanas. (para un entorno real).*
piso 2	piso 2	Canal #1	✓	*N/A*	*SSID configurado correctamente, se configuro WPA2-PSK con contraseña segura (12345678), conexión DHCP IPV4 asignada correctamente al dispositivo inalámbrico. Conexión inalámbrica funcional y segura. En los ACCESS POINT se configuraron los canales de forma alternada para evitar interferencias entre redes inalámbricas cercanas. (para un entorno real).*
piso 3	piso 3	Canal # 11	✓	*N/A*	*SSID configurado correctamente, se configuro WPA2-PSK con contraseña segura (123456789), conexión DHCP IPV4 asignada correctamente al dispositivo inalámbrico. Conexión inalámbrica funcional y segura. En los ACCESS POINT se configuraron los canales de forma alternada para evitar interferencias entre redes inalámbricas cercanas. (para un entorno real).*
sede remota piso 1	sede remota piso 1	Canal #6	✓	*N/A*	*SSID configurado correctamente, se configuro WPA2-PSK con contraseña segura (33334444), conexión DHCP IPV4 asignada correctamente al dispositivo inalámbrico. Conexión inalámbrica funcional y segura. En los ACCESS POINT se configuraron los canales de forma alternada para evitar interferencias entre redes inalámbricas cercanas. (para un entorno real).*
sede remota piso 2	sede remota piso 2	Canal #1	✓	*N/A*	*SSID configurado correctamente, se configuro WPA2-PSK con contraseña segura (1234567890), conexión DHCP IPV4 asignada correctamente al dispositivo inalámbrico. Conexión inalámbrica funcional y segura. En los ACCESS POINT se configuraron los canales de forma alternada para evitar interferencias entre redes inalámbricas cercanas. (para un entorno real).*

Listado sobre el análisis de riesgo (4 tablas):

Riesgo / valoración	***Probabilidad***				***Impacto***			
Seguridad física	***MA***	***A***	***M***	***B***	***L***	***M***	***A***	***C***
R1- Daños en el hardware por uso inadecuado del personal interno.	***X***						***X***	
R2- Robos de equipos por permitir ingresar personal no autorizado.		***X***						***X***
R3- Conflictos sociales.				***X***		***X***		
R4- Zonas peligrosas.			***X***			***X***		
R5 -Desastres naturales.				***X***				***X***

Riesgo / valoración	***Probabilidad***				***Impacto***			
Sistemas de información	***MA***	***A***	***M***	***B***	***L***	***M***	***A***	***C***
R6- Ciberataques (malware, ransomware, phishing).		***X***						***X***
R7- Acceso no autorizado.		***X***					***X***	
R8- Falta de copias de seguridad.			***X***			***X***		
R9- Fallas de hardware o software.	***X***							***X***
R10- Pedida de datos.	***X***							***X***
R11- Subestimar los imperativos cambiantes.			***X***			***X***		

Riesgo / valoración	***Probabilidad***				***Impacto***			
Manejo y control de personal	***MA***	***A***	***M***	***B***	***L***	***M***	***A***	***C***
R12- Personal no capacitado para la manipulación de equipos	***X***							***X***
R13- No se lleva un listado del personal que manipula los equipos.		***X***					***X***	
R14- No hay cámaras para monitorear robos.		***X***						***X***

Riesgo / valoración	*Probabilidad*				*Impacto*			
Eléctricos e Infraestructura	***MA***	***A***	***M***	***B***	***L***	***M***	***A***	***C***
R15- Mala infraestructura para inundaciones o terremotos.		***X***						***X***
R16- Fallos eléctricos por mala manipulación al equipo.			***X***				***X***	
R17- Incendios malintencionados.				***X***				***X***
R18- Caídas de energía.		***X***					***X***	
R19- No tener un sistema eléctrico Regulado.		***X***					***X***	
R20- No existe sistema contra incendios.	***X***							***X***

- ***Matriz de riesgos:***

Convención:

Riesgo catastrófico (12-16), Riesgo Alto (8-11), Riesgo Medio (4-7), Riesgo bajo (1-3).

Probabilidad de amenaza.	Impacto o magnitud del daño leve.	Impacto o magnitud del daño moderado.	Impacto o magnitud del daño alto.	Impacto o magnitud del daño catastrófico.
Muy alta.			R1	R9, R10, R12, R20
Alta.			R7, R13, R18, R19	R2, R6, R14, R15
Mediana.		R4, R8, R11	R16	
Baja.		R3		R5, R17

Evidencia de actualización de componentes de hardware y software de los equipos de cómputo, según especificaciones del proveedor:

El proceso de actualización de los equipos de cómputo de la empresa Enter Ltda. se llevó a cabo teniendo en cuenta las recomendaciones de los fabricantes y las buenas prácticas en administración de redes. Este proceso incluyó tanto equipos de escritorio, portátiles, servidores y dispositivos de red, como también dispositivos móviles tales como smartphones y tablets, los cuales forman parte activa de la infraestructura tecnológica.

Las pruebas y validaciones se realizaron en un entorno simulado mediante el uso de herramientas como GNS3 y Cisco Packet Tracer, permitiendo verificar el comportamiento de la red después de cada actualización aplicada.

- ✓ ***Actualización de componentes de hardware:*** *Las actualizaciones de hardware se enfocaron en mejorar el rendimiento de los equipos de cómputo, teniendo en cuenta las especificaciones recomendadas por los fabricantes:*

Ampliación de memoria RAM: *Se incrementó la capacidad de memoria en equipos de escritorio y portátiles (de 8 GB a 16 GB), con el fin de mejorar la ejecución de aplicaciones y el rendimiento general del sistema.*

Cambio de discos duros (HDD a SSD): *Se sustituyeron discos duros mecánicos por unidades de estado sólido (SSD), lo cual permitió reducir los tiempos de arranque del sistema y mejorar la velocidad de acceso a la información.*

Mantenimiento: *Se realiza mantenimiento a todos los equipos para evitar fallas de los mismo.*

Actualización de interfaces de red: *En dispositivos de red (routers y switches Cisco), se verificó el correcto funcionamiento de interfaces y módulos, asegurando compatibilidad con las configuraciones implementadas.*

*En el caso de **smartphones y tablets**, aunque no se realizan modificaciones internas de hardware como en un PC, se verificaron aspectos como: Estado de batería, Correcto funcionamiento del adaptador WiFi, Compatibilidad con redes inalámbricas configuradas.*

- ➢ ***Actualización de software:*** *Las actualizaciones de software fueron realizadas conforme a las versiones recomendadas por los proveedores:*

Equipos de cómputo: *Actualización de sistemas operativos (Windows 10 / 11), Actualización de Linux (Ubuntu Server), Instalación de parches de seguridad, Actualización de drivers de red.*

Dispositivos de red Cisco y GNS3: *Actualización del sistema operativo **Cisco IOS-GNS3**, Validación de configuraciones en routers y switches, Implementación de servicios de red (DHCP, VLANs, ruteo).*

Smartphones y tablets: *Actualización del sistema operativo (Android / iOS) a versiones más recientes, Actualización de aplicaciones utilizadas para acceso a la red corporativa, Configuración de red WiFi (SSID, autenticación y seguridad), Verificación de conectividad con la red interna.*

Validación de las actualizaciones: *Después de aplicar las actualizaciones, se realizaron pruebas para verificar el correcto funcionamiento de todos los dispositivos: Pruebas de conectividad desde*

PCs, laptops, smartphones y tablets, Verificación de asignación de direcciones IP mediante DHCP, Acceso a servicios de red desde dispositivos móviles, Pruebas de comunicación entre sedes.

En GNS3 y Cisco Packet Tracer, se comprobó que todos los dispositivos, incluyendo los móviles, podían conectarse correctamente a la red.

Listado de los equipos existentes con sus especificaciones actuales:

Equipo No.	*Sede*	*Piso*	*Componente hardware*	*Componente Software*	*Fecha*	*Actualización*	*Versión*
Pc-01	*Principal*	*1*	*CPU: Intel i5 / RAM: 8GB / Ato: 500GB HDD*	*Windows 10 Pro, Antivirus, Drivers de red*	*05/03/2026*	*Ampliación de RAM a 16GB y cambio a SSD*	*Windows 10*
Lap-01	*Principal*	*1*	*CPU: Intel i5 / RAM: 8GB / Ato: 1TB HDD*	*Windows 10, Drivers actualizados, firewalls*	*05/03/2026*	*Cambio de HDD a SSD y actualización de sistema*	*Windows 11*
Mob-01	*Principal*	*1*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps corporativas*	*05/03/2026*	*Actualización del sistema operativo*	*Android 15*
Tab-01	*Principal*	*1*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps básicas*	*05/03/2026*	*Actualización del sistema operativo*	*Android 15*
Pc-02	*Principal*	*2*	*CPU: Intel i3 /RAM: 4GB /Ato: 500G BHDD*	*Windows 10 Home, Drivers, firewalls*	*06/03/2026*	*Ampliación de RAM a 8GB*	*Windows 10 Actualizado*
Pc-03	*Principal*	*2*	CPU: Intel i5 / RAM: 8GB / Ato: 1TB HDD	*Windows 10 Pro, Antivirus, firewalls*	*06/03/2026*	*Cambio de HDD a SSD*	*Windows 10 Actualizado*
Pc-04	*Principal*	*2*	*CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD*	*Windows 10, Drivers, firewalls*	*06/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Lap-02	*Principal*	*2*	*CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD*	*Windows 10, Drivers actualizados*	*06/03/2026*	*Actualización de sistema y drivers*	*Windows 11*
Mob-02	*Principal*	*2*	*CPU: Octa-core / RAM: 4GB /Ato: 64GB*	*Android, Apps corporativas*	*06/03/2026*	*Actualización del sistema operativo*	*Android 15*
Tab-03	*Principal*	*2*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps básicas*	*06/03/2026*	*Actualización del sistema operativo*	*Android 15*
Pc-05	*Principal*	*3*	*CPU: Ryzen 5 / RAM: 8GB / Ato: 1TB HDD*	*Windows 10, Antivirus activo, firewalls*	*07/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Pc-06	*Principal*	*3*	*CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD*	*Windows 10, Drivers, firewalls*	*07/03/2026*	*Cambio de HDD a SSD*	*Windows 10 Actualizado*
Pc-07	*Principal*	*3*	*CPU: Intel i3 / RAM: 4GB /Ato: 500GB HDD*	*Windows 10, Software básico, firewalls*	*07/03/2026*	*Ampliación de RAM a 8GB*	*Windows 10 Actualizado*
Pc-08	*Principal*	*3*	*CPU: Intel i5 / RAM: 8GB / Ato: 1TB HDD*	*Windows 10, Antivirus, firewalls*	*07/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Lap-03	*Principal*	*3*	CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD	*Windows 10, Drivers, firewalls*	*07/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Mob-03	*Principal*	*3*	*CPU: Octa-core / RAM: 4GB /Ato: 64GB*	*Android, Apps corporativas*	*07/03/2026*	*Actualización del sistema operativo*	*Android 15*
Tab-03	*Principal*	*3*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps básicas*	*07/03/2026*	*Actualización del sistema operativo*	*Android 15*

Equipo No.	*Sede*	*Piso*	*Componente hardware*	*Componente Software*	*Fecha*	*Actualización*	*Versión*
Pc-09	*Remota*	*1*	*CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD*	*Windows 10, Antivirus activo, firewalls*	*08/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Lab-04	*Remota*	*1*	*CPU: Intel i5 / RAM: 8GB /Ato: 500GB HDD*	*Windows 10, Drivers actualizados*	*08/03/2026*	*Actualización de sistema y drivers*	*Windows 11*
Mob-04	*Remota*	*1*	*CPU: Octa-core / RAM: 4GB /Ato: 64GB*	*Android, Apps corporativas*	*08/03/2026*	*Actualización del sistema operativo*	*Android 15*
Tab-03	*Remota*	*1*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps básicas*	*08/03/2026*	*Actualización del sistema operativo*	*Android 15*
Pc-10	*Remota*	*2*	*CPU: Intel i3 / RAM: 4GB /Ato: 500GB HDD*	*Windows 10, Software básico, firewalls*	*09/03/2026*	*Ampliación de RAM a 8GB*	*Windows 10 Actualizado*
Pc-11	*Remota*	*2*	*CPU: Ryzen 5 / RAM: 8GB / Ato: 1TB HDD*	*Windows 10, Antivirus activo, firewalls*	*09/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Lap-05	*Remota*	*2*	*CPU: Intel i5 / RAM: 8GB / Ato: 1TB HDD*	*Windows 10, Antivirus*	*09/03/2026*	*Actualización del sistema operativo*	*Windows 11*
Mob-05	*Remota*	*2*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps corporativas*	*09/03/2026*	*Actualización del sistema operativo*	*Android 15*
Tab-04	*Remota*	*2*	*CPU: Octa-core /RAM: 4GB / Ato: 64GB*	*Android, Apps básicas*	*09/03/2026*	*Actualización del sistema operativo*	*Android 15*

Propuesta de actualización de Hardware:

A partir del análisis técnico realizado al inventario de equipos de cómputo de la sede principal y la sede remota, se identificaron limitaciones en el rendimiento asociadas principalmente a la capacidad de almacenamiento y memoria de los dispositivos. En este sentido, se plantean las siguientes acciones de actualización de hardware, orientadas a optimizar la eficiencia operativa de la infraestructura tecnológica.

En primer lugar, se propone la sustitución de unidades de almacenamiento tipo HDD por unidades de estado sólido (SSD) en los equipos que aún operan con tecnología mecánica. Esta actualización permite incrementar significativamente la velocidad de acceso a datos, reducir los tiempos de arranque del sistema operativo y mejorar la ejecución de aplicaciones. La implementación de esta mejora se llevó a cabo en equipos como PC-01, PC-03, PC-06, PC-11 y varios equipos portátiles, evidenciando una mejora sustancial en el desempeño general del sistema.

Adicionalmente, se determinó la necesidad de ampliar la capacidad de memoria RAM en aquellos equipos que presentaban configuraciones inferiores a los requerimientos actuales (4 GB). La ampliación a 8 GB o 16 GB se realizó en equipos críticos como PC-02, PC-07 y PC-10, con el fin de optimizar la gestión de procesos simultáneos, reducir la latencia en la ejecución de tareas y mejorar la estabilidad del sistema bajo condiciones de carga.

Adicionalmente, se determinó la necesidad de ampliar la capacidad de memoria RAM en aquellos equipos que presentaban configuraciones inferiores a los requerimientos actuales (4 GB). La ampliación a 8 GB o 16 GB se realizó en equipos críticos como PC-02, PC-07 y PC-10, con el fin de

optimizar la gestión de procesos simultáneos, reducir la latencia en la ejecución de tareas y mejorar la estabilidad del sistema bajo condiciones de carga.

Por otra parte, en los dispositivos móviles (smartphones y tablets), debido a sus características de diseño, no se contemplan actualizaciones de hardware. No obstante, se establece como medida técnica la optimización de recursos mediante la gestión eficiente del almacenamiento y el mantenimiento del sistema operativo actualizado, con el fin de asegurar su correcto funcionamiento dentro de la red corporativa.

Finalmente, las actualizaciones de hardware propuestas e implementadas permiten fortalecer la infraestructura tecnológica de la organización, incrementando el rendimiento de los equipos, reduciendo tiempos de respuesta y mejorando la experiencia del usuario. Estas acciones contribuyen directamente a la estabilidad, disponibilidad y eficiencia de los servicios de red en ambas sedes.

Ventajas de la solución propuesta – Hardware:

- ✓ ***Mejora del rendimiento general:*** *Incremento en la velocidad de procesamiento y ejecución de aplicaciones en los equipos de cómputo.*
- ✓ ***Reducción de tiempos de respuesta:*** *Disminución en los tiempos de arranque del sistema operativo, carga de programas y acceso a la información.*
- ✓ ***Mayor capacidad de multitarea:*** *Posibilidad de ejecutar múltiples aplicaciones de manera simultánea sin afectar el desempeño del sistema.*
- ✓ ***Incremento de la estabilidad del sistema:*** *Reducción de fallos, bloqueos y errores asociados a limitaciones de hardware.*
- ✓ ***Optimización de recursos tecnológicos:*** *Mejor aprovechamiento de la capacidad instalada en los equipos sin necesidad de reemplazarlos completamente.*
- ✓ ***Prolongación de la vida útil de los equipos:*** *Las actualizaciones permiten extender el tiempo de uso de los dispositivos existentes.*
- ✓ ***Reducción de costos operativos:*** *Disminución de la inversión en nuevos equipos mediante la actualización de componentes específicos.*
- ✓ ***Mejora en la productividad del usuario:*** *Mayor eficiencia en las actividades diarias debido a un mejor desempeño del sistema.*
- ✓ ***Mayor disponibilidad del servicio:*** *Disminución de interrupciones en la operación de la red y los servicios tecnológicos.*
- ✓ ***Adaptación a requerimientos actuales:*** *Los equipos quedan alineados con las necesidades tecnológicas actuales de la organización.*

Propuesta de actualización de Software:

A partir del análisis realizado a los equipos de cómputo de la sede principal y la sede remota, se evidenció que varios dispositivos operan con versiones desactualizadas de sistemas operativos,

controladores y aplicaciones, lo cual impacta negativamente en el rendimiento, la seguridad y la estabilidad de la infraestructura tecnológica. Asimismo, se identificaron posibles vulnerabilidades asociadas a la falta de parches de seguridad y a la ausencia de políticas de actualización automatizada.

Con el fin de optimizar el funcionamiento de los equipos y garantizar la continuidad de los servicios de red, se plantea la implementación de un proceso de actualización de software que contemple la instalación de las últimas versiones de los sistemas operativos compatibles con cada dispositivo. Esta acción permitirá mejorar la seguridad del sistema, optimizar el uso de los recursos y asegurar la compatibilidad con aplicaciones modernas.

De igual manera, se propone la aplicación periódica de parches de seguridad, con el objetivo de corregir vulnerabilidades detectadas por los fabricantes y prevenir posibles ataques informáticos. Este proceso debe ser gestionado de manera centralizada, asegurando que todos los equipos de la red se mantengan actualizados.

Adicionalmente, se contempla la actualización de los controladores (drivers) de los dispositivos, especialmente aquellos relacionados con la conectividad de red, video y periféricos, con el fin de garantizar un funcionamiento óptimo del hardware y evitar fallos en la operación.

En cuanto al software de seguridad, se propone la implementación y actualización constante de herramientas como antivirus y firewalls, que permitan proteger los equipos frente a amenazas externas, así como la configuración de políticas de seguridad que regulen el acceso y uso de los recursos tecnológicos.

Asimismo, se recomienda la optimización del software instalado mediante la eliminación de aplicaciones innecesarias y la configuración adecuada de los programas utilizados en el entorno laboral, lo cual contribuirá a mejorar el rendimiento de los equipos.

En el caso de los dispositivos móviles, como smartphones y tablets, se plantea la actualización de los sistemas operativos y aplicaciones, garantizando su compatibilidad con la red corporativa y asegurando un nivel adecuado de seguridad en el acceso a la información.

Finalmente, se propone la implementación de políticas de actualización automática, que permitan mantener los sistemas actualizados de forma continua, reduciendo la intervención manual y minimizando los riesgos asociados a software obsoleto.

Ventajas de la solución propuesta – Software:

- **Mejora en la seguridad de la información:** La actualización de sistemas operativos y aplicación de parches reduce vulnerabilidades y protege frente a amenazas informáticas.
- **Mayor estabilidad del sistema:** Disminución de errores, fallos y cierres inesperados gracias a versiones de software más optimizadas.
- **Optimización del rendimiento:** Mejora en la velocidad de respuesta y ejecución de aplicaciones mediante software actualizado y depurado.
- **Compatibilidad con nuevas tecnologías:** Permite que los equipos trabajen correctamente con aplicaciones modernas y servicios actuales de red.

- **Reducción de riesgos operativos:** Disminuye la probabilidad de fallos críticos o interrupciones del servicio causados por software obsoleto.
- **Mejor gestión de recursos del sistema:** Uso más eficiente de CPU, memoria y almacenamiento mediante sistemas optimizados.
- **Protección contra malware y ciberataques:** Actualización de antivirus y firewalls fortalece la defensa frente a amenazas externas.
- **Automatización de actualizaciones:** Reduce la intervención manual y asegura que los sistemas se mantengan actualizados de forma continua.
- **Mejora en la productividad del usuario:** Los sistemas más rápidos y estables permiten realizar tareas de manera más eficiente.
- **Mayor continuidad del servicio:** Disminución de caídas del sistema, garantizando disponibilidad en la red y plataformas tecnológicas.

Cronograma y presupuesto:

- ***Análisis económico:*** *A partir de las actualizaciones de hardware y software propuestas para los equipos de la sede principal y la sede remota, se realizó una estimación de los costos asociados a la adquisición de componentes físicos y licencias de software.*

  En el caso del hardware, los principales costos corresponden a la compra de unidades de estado sólido (SSD) y módulos de memoria RAM, necesarios para mejorar el rendimiento de los equipos. Por otro lado, en el componente de software, se consideran licencias de sistemas operativos, herramientas de seguridad (antivirus) y posibles aplicaciones corporativas.

Análisis económico					
ítem	***Concepto***	***Descripción***	***Cantidad***	***Costo unitario (COP)***	***Costo total (COP)***
1	*Disco SSD*	*Para PCs y laptops con HDD*	*4*	*$350.000*	*$1.400.000*
2	*Memoria RAM*	*Equipos con bajo rendimiento*	*4*	*$170.000*	*$680.000*
3	*Licencias SO*	*Equipos que requieren actualización*	*20*	*$500.000*	*$10.000.000*
4	*Antivirus*	*PCs y laptops*	*15*	*$80.000*	*$1.200.000*
5	*Mano de obra*	*Instalación y configuración*	*20*	*$50.000*	*$1.000.000*
TOTAL					*$14.280.000 COP*

- ***Tiempo estimado:*** El tiempo estimado para la implementación de las actualizaciones es de **3 a 5 días hábiles**, distribuidos de la siguiente manera:

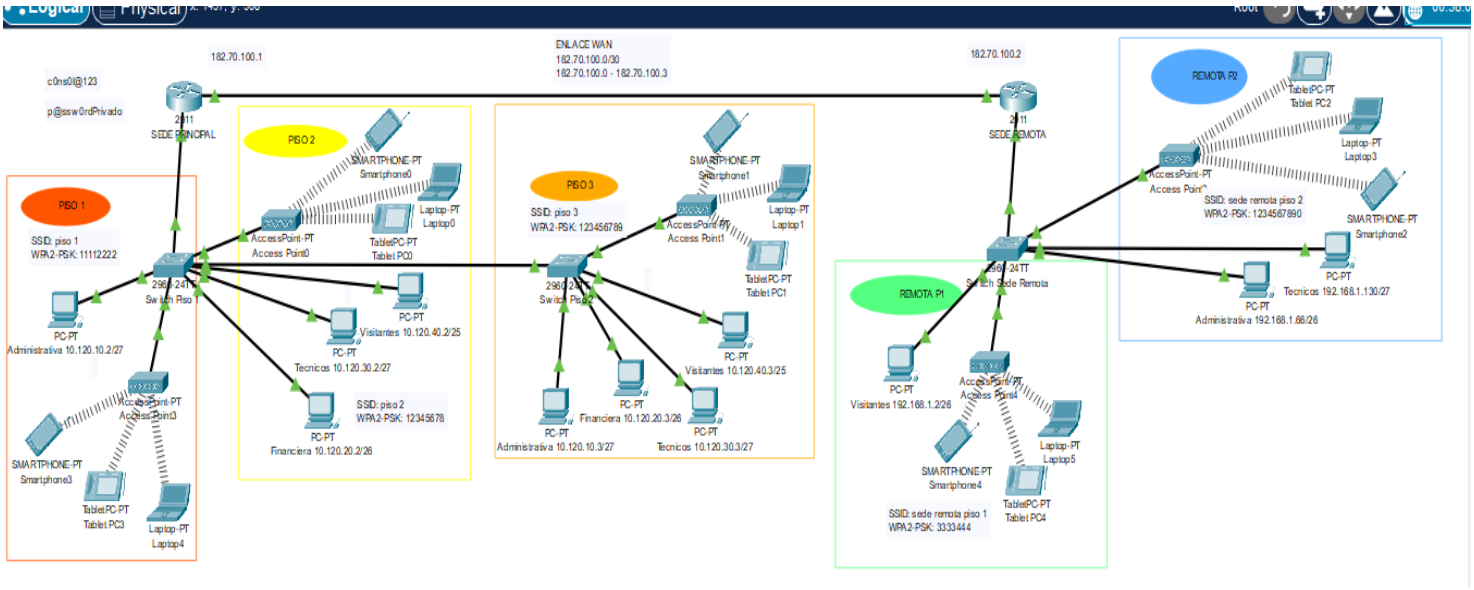
Tiempo estimado			
Día	***Actividad***	***Descripción***	***Equipos involucrados***
Día 1	Diagnóstico y respaldo	Revisión general y copia de seguridad	Todos los equipos
Día 2	Actualización de hardware	Instalación de SSD y ampliación de RAM	PCs y laptops seleccionados
Día 3	Instalación de software	Instalación de sistemas operativos	Equipos que lo requieren
Día 4	Configuración	Drivers, antivirus y programas	Todos los equipos
Día 5	Pruebas y validación	Verificación de funcionamiento	Todos los equipos

- ***Costo aproximado:*** *Dependiendo del número de equipos actualizados:*

Costo aproximado		
Concepto	***Descripción***	***Valor***
Inversión total estimada	*Hardware + Software + Mano de obra*	*$14.280.000 COP*
Tipo de inversión	*Actualización tecnológica*	*Media*
Alcance	*Sede principal y sede remota*	*Completo*
Beneficio esperado	*Mejora de rendimiento, seguridad y estabilidad*	*Alto*

Registro fotográfico del proceso de actualización de los equipos:

Se esta trabajando por medio de simulaciones con las herramientas Cisco packet tracer y GNS3, por ende, se toma captura de la simulación realizada en Cisco, en la cual cuenta con todos los equipos trabajados en este informe.



Recomendaciones:

- ✓ ***Implementar un plan de mantenimiento preventivo y correctivo:*** *Establecer cronogramas periódicos para la revisión de equipos, actualización de software y verificación del estado de la red, con el fin de prevenir fallos y garantizar la continuidad del servicio.*
- ✓ ***Mantener actualizado el software de todos los dispositivos:*** *Aplicar de manera constante actualizaciones de sistemas operativos, parches de seguridad, drivers y aplicaciones, reduciendo vulnerabilidades y mejorando el rendimiento.*
- ✓ ***Optimizar el uso de los recursos de hardware:*** *Continuar con la implementación de mejoras como ampliación de memoria RAM y uso de unidades SSD, especialmente en equipos que presenten bajo desempeño.*
- ✓ ***Implementar políticas de seguridad informática:*** *Definir controles de acceso, uso adecuado de contraseñas, instalación de antivirus y configuración de firewalls para proteger la información y los recursos de la red.*
- ✓ ***Realizar monitoreo constante de la red:*** *Utilizar herramientas de supervisión en entornos como GNS3 y dispositivos Cisco para identificar fallas, congestión o degradación del servicio en tiempo real.*
- ✓ ***Capacitar al personal técnico y usuarios finales:*** *Brindar formación sobre el uso adecuado de los equipos, buenas prácticas de seguridad y procedimientos básicos ante fallas, con el fin de reducir errores operativos.*
- ✓ ***Llevar registro y documentación de eventos:*** *Mantener actualizada la bitácora de eventos de infraestructura y plataformas, permitiendo un mejor control y seguimiento de incidentes en la red.*
- ✓ ***Realizar pruebas periódicas de conectividad y rendimiento:***
  Verificar parámetros como ancho de banda, latencia y estabilidad de la red para asegurar un funcionamiento óptimo.
- ✓ ***Planificar futuras actualizaciones tecnológicas:***
  Evaluar continuamente el estado de la infraestructura para anticipar necesidades de renovación de equipos o implementación de nuevas tecnologías.
- ✓ ***Garantizar la continuidad del servicio:***
  Implementar mecanismos de respaldo y recuperación de información, así como estrategias que minimicen el impacto ante posibles fallos.

Conclusiones:

El desarrollo de la evidencia permitió realizar la identificación, análisis y actualización de los componentes de hardware y software de los equipos de cómputo pertenecientes a la sede principal y la sede remota de la organización. A partir del diagnóstico inicial, se evidenciaron limitaciones en el rendimiento de algunos dispositivos, así como la presencia de sistemas operativos y aplicaciones desactualizadas, lo cual representaba riesgos para la seguridad y la eficiencia operativa.

Con base en esta información, se plantearon e implementaron acciones de mejora orientadas a optimizar el funcionamiento de los equipos, tales como la ampliación de memoria RAM en dispositivos con bajo desempeño, la sustitución de discos duros tradicionales por unidades de estado sólido (SSD) y la actualización de sistemas operativos, controladores y herramientas de seguridad. Estas acciones permitieron mejorar significativamente la velocidad de procesamiento, la estabilidad del sistema y la protección frente a vulnerabilidades.

Asimismo, la elaboración de la documentación técnica y el registro de las actualizaciones realizadas contribuyeron a establecer un control más organizado sobre la infraestructura tecnológica, facilitando futuras intervenciones y procesos de mantenimiento. Esto resulta fundamental para la gestión adecuada de los recursos tecnológicos y la toma de decisiones en la organización.

Finalmente, las actualizaciones de hardware y software implementadas permiten optimizar el rendimiento, mejorar la seguridad y prolongar la vida útil de los equipos de cómputo, garantizando una operación más eficiente y confiable de los servicios tecnológicos en ambas sedes, alineando la infraestructura con las necesidades actuales de la empresa.

Bibliografías:

https://www.welivesecurity.com/es/cibercrimen/incidentes-ciberseguridad-2024-america-latina/

https://www.channelpartner.es/seguridad/principales-ciberataques-en-espana-en-2024/

https://www.qualoom.es/ataques-informaticos/

https://www.piranirisk.com/es/blog/8-consejos-para-prevenir-ataques-informaticos

https://tech.gobetech.com/18188/por-que-es-importante-la-seguridad-de-la-red.html

https://winempresas.pe/blog/ataques-informaticos-causas-y-12-tipos-de-ciberataques

https://concepto.de/sistema-operativo/

https://www.universitatcarlemany.com/actualidad/blog/tipos-de-sistemas-operativos/

https://www.officedepot.com.mx/officedepot/en/blog/que-es-un-equipo-de-computo-esto-es-todo-lo-que-debes-saber?srsltid=AfmBOopqdl1M57oR1DFivCKBOSRiAweRNAoF7s3cR6ynsrIoCKy7Ah6v

https://coverix.mx/equipo-de-computo-para-empresas

https://youtu.be/uQzLvkUpIts

https://youtu.be/hvGnCLlVi1o

http://repositorio.utn.edu.ec/bitstream/123456789/3768/3/04%20RED%20041%20Informe%20T%C3%A9cnico-%20Espa%C3%B1ol.pdf

https://red.uao.edu.co/bitstream/handle/10614/10248/T07892.pdf;sequence=4

SERVICIO NACIONAL DE APRENDIZAJE SENA

PLAN DE TRABAJO CONCERTADO CON EL APRENDIZ PARA EL DESARROLLO DE LA RUTA DE APRENDIZAJE

Programa de Formación:	Gestión de redes de datos	**Centro:**	CENTRO DE LA INNOVACIÓN AGROINSDUSTRIAL Y DE SERVICIOS	**I.D**	**Nombr**
Proyecto (s):	Planeación, implementación y gestión de infraestructura informática en el sector Mipyme para la mejora de la productividad, desarrollo e innovación.				**Código**

Resultado (S) de Aprendizaje

R1.	**220501106-03 - Verificar el funcionamiento de dispositivos de cómputo y servicios de red de acuerdo a políticas de la organización.**	R2.	
R2.	**plataforma tecnológica**		
R3.		R4.	

RAP	EVIDENCIA	DESCRIPCIÓN DE LAS EVIDENCIAS DE APRENDIZAJE	FECHA CONCERTACIÓN	TIPO DE EVIDENCIA	FORMA DE ENTREGA	RAP	EVIDENCIA	DESCRIPCIÓN DE LAS EVIDENCIAS DE APRENDIZAJE
R1.	E1	Informe sobre detección de fallos en el rendimiento y operación de la solución. GA9-220501106-AA1-EV01. .	30/4/2026	**P:Producto**	Digital	R2	E5	
	E2	Informe de actualización de componentes de hardware y software de los equipos de cómputo. GA9-220501106-AA2-EV02.	30/4/2026	**P:Producto**	Digital		E6	
	E3						E7	
	E4						E8	

NOMBRE DEL APRENDIZ	FECHA DE ENTREGA REAL								JUICIO DE EVALUACION							
	E1	E2	E3	E4	E5	E6	E7	E8	E1	E2	E3	E4	E5	E6	E7	E8
JHOJAN STIVEN JARAMILLO CORREA	A	A														
LUIS ALBERTO SANCHEZ LOPEZ	30/4/2026	30/4/2026														
VERONICA VIVIANA QUIROSQUIROS	30/4/2026	30/4/2026														
WIANNYS ALEJANDRA HERNANDEZ CERVANTES	30/4/2026	30/4/2026														
YURY TATIANA CUERVO FALLA	A	A														
SEBASTIAN CHAVERRA RUIZ	30/4/2026	30/4/2026														
JAIBER CAMILO ANAYA ANAYA	30/4/2026	30/4/2026														
HAYMAR AGUALIMPIA RENTERIA	30/4/2026	30/4/2026														
CESAR DARIO OSORIO ULLOA	30/4/2026	30/4/2026														
WILMER GALEANO ARIAS	30/4/2026	30/4/2026														
CRISTIAN CAMILO RUIZ GALEANO	30/4/2026	30/4/2026														

Juicio de Evaluación A : Aprobado D: Desaprobado

Evidencia P: Producto D:Desempeño C:Conocimiento

Forma de Entrega: F: Física - D: Digital

Reporte de Juicios de Evaluación

Fecha del Reporte: 14/04/2026
Ficha de Caracterización: 3118456
Cógigo: 228183
Versión: 2
Denominación: GESTION DE REDES DE DATOS
Estado de la Ficha de Caracterización: EN EJECUCION
Fecha Inicio: 18/11/2024
Fecha Fin: 17/02/2027
Modalidad de Formación: VIRTUAL
Regional: 15 - REGIONAL BOYACÁ
Centro de Formación: 9551 - CENTRO DE LA INNOVACIÓN AGROINDUSTRIAL Y DE SERVICIOS

Tipo de Documento	Número de Documento	Nombre	Apellidos	Estado	Competencia	Resultado de Aprendizaje	Juicio de Evaluación	Fecha y Hora del Juicio Evaluativo	Funcionario que registro el juicio evaluativo
CC	1006182195	JHOJAN STIVEN	JARAMILLO CORREA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	APROBADO	06/12/2025 12.11 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1006182195	JHOJAN STIVEN	JARAMILLO CORREA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1006182195	JHOJAN STIVEN	JARAMILLO CORREA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1006182195	JHOJAN STIVEN	JARAMILLO CORREA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	APROBADO	06/12/2025 12.22 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1012358891	CRISTIAN CAMILO	RUIZ GALEANO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE LOS SERVICIOS DE RED	POR EVALUAR		-
CC	1012358891	CRISTIAN CAMILO	RUIZ GALEANO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1012358891	CRISTIAN CAMILO	RUIZ GALEANO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1012358891	CRISTIAN CAMILO	RUIZ GALEANO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	POR EVALUAR		-
CC	1014205816	YURY TATIANA	CUERVO FALLA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	APROBADO	06/12/2025 12.11 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1014205816	YURY TATIANA	CUERVO FALLA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1014205816	YURY TATIANA	CUERVO FALLA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1014205816	YURY TATIANA	CUERVO FALLA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	APROBADO	06/12/2025 12.29 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1017174142	JAIBER CAMILO	ANAYA ANAYA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	APROBADO	22/12/2025 8.45 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1017174142	JAIBER CAMILO	ANAYA ANAYA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1017174142	JAIBER CAMILO	ANAYA ANAYA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1017174142	JAIBER CAMILO	ANAYA ANAYA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	APROBADO	22/12/2025 8.46 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1017230607	HAYMAR	AGUALIMPIA RENTERIA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	POR EVALUAR		-
CC	1017230607	HAYMAR	AGUALIMPIA RENTERIA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1017230607	HAYMAR	AGUALIMPIA RENTERIA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1017230607	HAYMAR	AGUALIMPIA RENTERIA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE	POR EVALUAR		-
CC	1019110452	ANA BELEN	RAMIREZ SANCHEZ	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	POR EVALUAR		-
CC	1019110452	ANA BELEN	RAMIREZ SANCHEZ	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1019110452	ANA BELEN	RAMIREZ SANCHEZ	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1019110452	ANA BELEN	RAMIREZ SANCHEZ	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	POR EVALUAR		-
CC	1073327029	CESAR DARIO	OSORIO ULLOA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	APROBADO	03/02/2026 9.48 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1073327029	CESAR DARIO	OSORIO ULLOA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1073327029	CESAR DARIO	OSORIO ULLOA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1073327029	CESAR DARIO	OSORIO ULLOA	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	APROBADO	03/02/2026 9.48 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1079936837	WIANNYS ALEJANDRA	HERNANDEZ CERVANTES	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	POR EVALUAR		-
CC	1079936837	WIANNYS ALEJANDRA	HERNANDEZ CERVANTES	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1079936837	WIANNYS ALEJANDRA	HERNANDEZ CERVANTES	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1079936837	WIANNYS ALEJANDRA	HERNANDEZ CERVANTES	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE	POR EVALUAR		-
CC	1110508474	WILMER	GALEANO ARIAS	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	APROBADO	06/12/2025 12.11 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	1110508474	WILMER	GALEANO ARIAS	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	1110508474	WILMER	GALEANO ARIAS	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	1110508474	WILMER	GALEANO ARIAS	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	APROBADO	06/12/2025 15.26 a	CC 25290314 - SANDRA XIMENA ZAPATA ANGULO
CC	71335651	ELMER DIDIER	OSORIO MARIN	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	POR EVALUAR		-
CC	71335651	ELMER DIDIER	OSORIO MARIN	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	71335651	ELMER DIDIER	OSORIO MARIN	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	71335651	ELMER DIDIER	OSORIO MARIN	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	POR EVALUAR		-
CC	7917706	LUIS ALBERTO	MOLINARES POLO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531302 - CONFIGURAR EL HARDWARE, DISPOSITIVOS DE CÓMPUTO Y SISTEMAS OPERATIVOS NECESARIOS PARA LA IMPLEMENTACIÓN DE	POR EVALUAR		-

CC	7917706	LUIS ALBERTO	MOLINARES POLO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531303 - VERIFICAR EL FUNCIONAMIENTO DE DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED DE ACUERDO A POLÍTICAS DE LA ORGANIZACIÓN.	POR EVALUAR		-
CC	7917706	LUIS ALBERTO	MOLINARES POLO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531304 - GESTIONAR LOS DISPOSITIVOS DE CÓMPUTO Y SERVICIOS DE RED PARA GARANTIZAR EL FUNCIONAMIENTO DE LA PLATAFORMA	POR EVALUAR		-
CC	7917706	LUIS ALBERTO	MOLINARES POLO	EN FORMACION	38500 - CONFIGURAR DISPOSITIVOS DE CÓMPUTO DE ACUERDO CON ESPECIFICACIONES DEL DISEÑO Y PROTOCOLOS TÉCNICOS	531305 - IMPLEMENTAR LOS SERVICIOS RED NECESARIOS PARA CUMPLIR LOS REQUERIMIENTOS DEL PORTAFOLIO DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN	POR EVALUAR		-