REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y LA TECNOLOGÍA

Administración de Servidores y Analista de Sistemas

INFORME FINAL DE PASANTÍA DE EXTENSIÓN OCUPACIONAL PROFESIONAL EN EL DEPARTAMENTO DE INFORMÁTICA DEL MIDES

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIÓN CON ÉNFASIS EN SEGURIDAD

Asesor Académico: Elvis Araúz

Asesor Industrial: Norman Vellos

Autor: Diana Lisbeth Morcillo Salazar

Ciudad de Panamá, Abril de 2026

REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y LA TECNOLOGÍA

Administración de Servidores y Analista de Sistemas

INFORME FINAL DE PASANTÍA DE EXTENSIÓN OCUPACIONAL PROFESIONAL EN EL DEPARTAMENTO DE INFORMÁTICA DEL MIDES

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIÓN CON ÉNFASIS EN SEGURIDAD

Autor: Diana Lisbeth Morcillo Salazar

Ciudad de Panamá, Abril de 2026

Universidad Internacional de Ciencia y Tecnología

Ciudad de Panamá,

Profesor

Héctor José Mazurkiewicz

Coordinador Comité de Titulación de Estudios de Licenciatura.

Presente.

En mi carácter de Tutor del Trabajo de Grado (Informe Final de Pasantías de Extensión Ocupacional Profesional) presentado por la Bachiller, Diana L. Morcillo documento de identidad N.º 8-923-484, para optar al grado de, Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad, consideró que el trabajo: reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

Elvis Araúz

Documento de identidad Cédula No.

8-833-515

Línea de Investigación: Administración de servidores y Analista de Sistemas.

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN Y LA TECNOLOGÍA

INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN II

Estudiante: Diana L. Morcillo S. Cédula de identidad: No. 8-923-484

Tutor: Lic. Elvis Araúz, Cédula de identidad: No. 8-833-515

Correo electrónico del participante:diana.morcillo@unicyt.net

Celular No. 6487-9142

Título tentativo del trabajo de grado (TG) y de pasantía profesional (PEOP).

Línea de Investigación: Administración de servidores y Analista de Sistemas.

Sesión	Fecha	Hora Reunión.	Aspecto tratado	Observación
1.	6 de Febrero 2026.	1 hora	Propuesta del proyecto de grado.	
2.	20 de Febrero 2026.	1 hora	Revisión 1 del proyecto.	
3.	27 de Febrero 2026.	1 hora	Continuación de revisión 1 del proyecto.	
4.	6 de Marzo de 2026.	1 hora	Revisión 2 del proyecto.	
5.	13 de Marzo de 2026.	1 hora	Continuación de revisión 2 del proyecto.	
6.	20 de Marzo de 2026.	1 hora	Revisado completo del trabajo.	

Título definitivo: Administración de servidores y Analista de Sistemas.

Comentarios finales acerca de la investigación: Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

Firma

Diana L. Morcillo

Firma

Lic. Elvis Araúz

Dedicatoria

Este trabajo final de grado, quiero dedicárselo principalmente a mi mamá, quien ha sido mi mayor pilar, mi ejemplo de fortaleza y mi fuente constante de motivación. Su amor incondicional, su paciencia infinita y palabras de aliento han sido fundamentales para que hoy pueda culminar esta importante etapa de mi vida académica.

Gracias por creer en mí en todo momento, incluso cuando dudé de mis capacidades, por acompañarme en cada paso de este camino y por enseñarme el valor de la perseverancia, la responsabilidad y el esfuerzo. Cada logro alcanzado es reflejo de su dedicación, y entrega incondicional, esto representa el fruto de todos los sacrificios realizados a lo largo de los años.

Este logro también es suyo, porque sin su guía y confianza en mí, nada de esto habría sido posible.

Agradecimiento

Agradezco primeramente a Dios por concederme la salud, sabiduría y la perseverancia necesaria para culminar con éxito esta importante etapa de mi formación académica.

Al Departamento de Informática del Ministerio de Desarrollo Social, por su profesionalismo, apoyo y valiosa orientación durante el tiempo de práctica. Sus enseñanzas, consejos y acompañamiento contribuyeron de manera significativa a mi aprendizaje académico y profesional.

A la Universidad Internacional de Ciencia y Tecnología, por brindarme las herramientas, los recursos, el espacio necesario y los conocimientos brindados a lo largo de esta carrera.

Igualmente, extiendo también mi gratitud a todas las personas que, de manera directa o indirecta han podido contribuir de manera positiva en la realización de este trabajo, aportando su tiempo, conocimientos y apoyo desinteresado.

Resumen

El presente informe expone las actividades desarrolladas durante la pasantía de extensión profesional ocupacional en el departamento de Informática del Ministerio de Desarrollo Social. El objetivo principal fue analizar y dar respuesta a un problema identificado en la gestión, almacenamiento y acceso a los datos generados por los dispositivos de control de asistencia, específicamente relojes biométricos utilizados en la organización.

El estudio se enfoca en la estructuración de una solución basada en la optimización de la infraestructura de red existente, considerando la asignación y administración eficiente de direcciones IP para cada dispositivo, lo que permite su correcta identificación y comunicación dentro de la red. Asimismo, se plantea la configuración de un servidor dedicado al almacenamiento centralizado de la información, facilitando el acceso a los registros de entrada y salida del personal de manera organizada y segura.

Adicionalmente, se evalúa la implementación de mecanismos de seguridad, como el uso de redes privadas virtuales (VPN), con el fin de proteger la integridad, confidencialidad y disponibilidad de los datos transmitidos. También se analiza el papel del departamento de informática como eje fundamental en la interconexión de sistemas y en el soporte de los procesos operativos de la institución.

Los resultados obtenidos evidencian una mejora en la gestión de la información, así como en la eficiencia y confiabilidad en el acceso a los datos, contribuyendo al fortalecimiento de la infraestructura tecnológica de la organización.

Abstract

This report details the activities carried out during the professional development internship in the IT Department of the Ministerio de Desarrollo Social. The main objective was to analyze and address a problem identified in the management, storage, and access to data generated by attendance control devices, specifically biometric clocks used in the organization.

The study focuses on structuring a solution based on optimizing the existing network infrastructure, considering the efficient assignment and management of IP addresses for each device, which allows for their correct identification and communication within the network. It also proposes the configuration of a dedicated server for the centralized storage of information, facilitating organized and secure access to employee entry and exit records.

Additionally, the implementation of security mechanisms, such as the use of virtual private networks (VPNs), is evaluated to protect the integrity, confidentiality, and availability of transmitted data. The role of the IT Department as a fundamental axis for the interconnection of systems and the support of the institution's operational processes is also analyzed. The results obtained demonstrate an improvement in information management, as well as in the efficiency and reliability of data access, contributing to the strengthening of the organization's technological infrastructure.

Contenido

Contenido de figuras

Contenido de Tablas

Introducción

Hoy en día todas las organizaciones ya sean públicas o privadas dependen de la tecnología de la información y las comunicaciones para que sus operaciones se desarrollen de manera eficiente. En este caso la infraestructura de red se ha convertido en un componente primordial para garantizar la conectividad, el intercambio de información. La correcta planificación, administración e implementación de estos métodos debe ser fundamental para asegurar la protección de datos que circulan en ellas.

Dentro de las organizaciones la seguridad de la información busca garantizar la integridad y confidencialidad de los datos. Cuando se aumenta el número de dispositivos conectados a la red también crece el riesgo de vulnerabilidad, los accesos no autorizados y la perdida de información.

Por eso es indispensable aplicar buenas practicas al momento de diseñar la red, esto incluye esquemas adecuados de direccionamiento IP, segmentación de la red y los mecanismos de control de acceso.

El objetivo de este trabajo era identificar las diferentes deficiencias relacionadas con la gestión de estos dispositivos. Estas limitaciones afectan directamente la eficiencia operativa y aumenta el riesgo de vulneración de la información.

El poder desarrollar una propuesta basada en el diseño de una infraestructura de red orientada a optimizar la gestión, no solo busca resolver una necesidad especifica dentro del entorno institucional, sino también en contribuir al fortalecimiento de la infraestructura tecnológica, promoviendo un manejo seguro y confiable de la información.

CAPÍTULO I.

MARCO DE LA INSTITUCIÓN DONDE REALIZÓ LA PASANTÍA

1.1 Definición de la Carrera que Estudia.

Ingeniería en Redes de Comunicaciones con énfasis en Seguridad es una rama especializada de la informática que se enfoca en el diseño, planificación, implementación, administración, y optimización de infraestructuras de redes de datos, arquitecturas de red, protocolos de comunicación y servicios digitales.

Esta área de estudio abarca el análisis de arquitecturas de red, protocolos de comunicación y servicios digitales, así como la identificación, prevención y mitigación de vulnerabilidades y amenazas cibernéticas. Su enfoque permite desarrollar soluciones tecnológicas seguras y eficientes, capaces de responder a las crecientes demandas de conectividad y protección de datos en entornos organizacionales y globales.

1.2 Antecedentes de la Institución

El Ministerio de Desarrollo Social es el ente rector de las políticas, planes y programas en materia de equidad y/o desarrollo social, especialmente aquellas destinadas a erradicar la pobreza y brindar protección social a las personas, familias o grupos vulnerables en distintos momentos del ciclo vital, promoviendo la movilidad e integración social y la participación con igualdad de oportunidades en la vida nacional. Sus funciones como ente rector incluyen la formulación, coordinación, articulación, implementación, seguimiento y evaluación de dichas políticas.

La Ley 29 del 1 de agosto de 2005 creó el Ministerio de Desarrollo Social (MIDES)

El Ministerio de la Juventud, la Mujer, la Niñez y la Familia, creado por la Ley 42 de 1997, continuará existiendo y operando de acuerdo con las disposiciones de la presente Ley, bajo la denominación de Ministerio de Desarrollo Social.

En Panamá el Ministerio de Desarrollo Social será el ente rector de las políticas sociales, enfocado en la reducción de la pobreza y la protección de grupos vulnerables. Esta normativa base regula las transferencias monetarias condicionadas, la protección de la niñez, el voluntariado y el apoyo a personas mayores.

1.2.1 Misión de la Institución

Ejercer la rectoría de la política social integral, planes y programas en materia de equidad y/o desarrollo social, en beneficio de las familias y grupos vulnerables, en distintos momentos del ciclo vital, bajo el enfoque de derechos humanos y desarrollo sostenible que permitan la protección, erradicar la pobreza, la desigualdad e inequidad social.

1.2.2 Visión de la Institución

Una institución reconocida por su rectoría eficaz de la política social integral, moderna e innovadora que privilegia el conocimiento, la ética, eficiencia y eficacia en el uso de todos los recursos con transparencia y rendición de cuentas. Con profesionales altamente competitivos y comprometidos, que promueven un Panamá inclusivo, con bienestar y justicia social para todos y todas.

1.2.3 ¿A qué se Dedica la Institución?

El Ministerio de Desarrollo Social es el ente rector de las políticas sociales del Estado panameño. Esta institución lidera la inversión social para el fortalecimiento de las habilidades y capacidades del capital humano del país para lograr la sostenibilidad del desarrollo nacional, vela por la protección social y la regulación de la calidad de los servicios, tendientes a prevenir la exclusión social y compensar sus consecuencias.

Implementa programas de bienestar social, destacando las Transferencias Monetarias Condicionadas (PTMC) como el programa "120 a los 65" para adultos mayores, "Red de Oportunidades" para familias en pobreza, y "Ángel Guardián" para personas con discapacidad, cubriendo salud y educación.

Programas Principales (PTMC):

- 120 a los 65: Brinda B/.120 mensuales a adultos mayores de 65 años sin jubilación ni pensión, en riesgo social.

- Red de Oportunidades: Dirigido a familias en pobreza extrema, condicionando el apoyo a controles de salud y asistencia escolar.

- Ángel Guardián: Asistencia a personas con discapacidad severa en condiciones de vulnerabilidad.

Seguridad Alimentaria:

- SENAPAN (Bono Alimenticio): Entrega alimentos a áreas comarcales y de difícil acceso.
- Comedores Comunitarios: Combaten la desnutrición en comunidades vulnerables.

Desarrollo Social y Comunitario:

- CAIPI (Centros de Atención Integral a la Primera Infancia): Atención a la niñez.
- Redes de Familia: Capacitaciones y emprendimientos para mejorar la calidad de vida de amas de casa.
- CEFODEA: Programa educativo para jóvenes de 14 a 17 años que no asisten a la escuela.

Protección y Apoyo:

- Atención a personas en situación de calle: Censo y apoyo para mejorar sus condiciones.
- Línea 147: Servicio de atención para bienestar social y salud mental, reforzado vía WhatsApp.

El MIDES enfoca sus esfuerzos en la protección de la primera infancia, juventud, adultos mayores y personas con discapacidad para reducir la pobreza; generando un impacto social significativo al reducir la pobreza y la desigualdad, beneficiando a más de 186,000 personas mediante transferencias monetarias condicionadas. Estas acciones incluyen la protección de la primera infancia con CAIPIs, apoyo a la mujer rural, becas laborales para jóvenes y atención a adultos mayores.

Figura N°1

Estructura Organizativa de la Institución

1.3 Departamento Donde Realizó La Pasantía.

Departamento de Informática y Telecomunicaciones.

Es el encargado de gestionar, administrar y mantener la infraestructura tecnológica y de comunicaciones de la organización, garantizando el correcto funcionamiento de los sistemas informáticos, redes de datos y servicios de conectividad. Su labor se orienta a asegurar la disponibilidad, integridad y seguridad de la información, así como la continuidad operativa de los recursos tecnológicos utilizados por la institución.

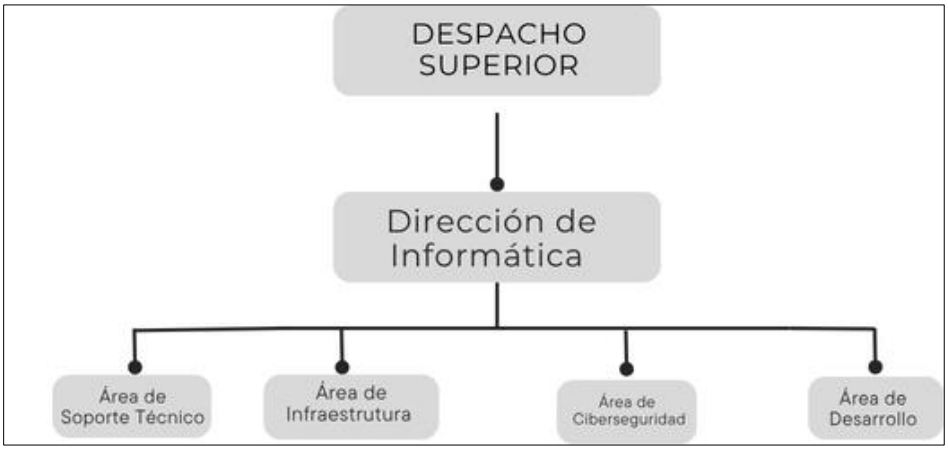
Además desempeña un papel fundamental en la integración de herramientas tecnológicas que permiten la comunicación y el intercambio seguro de información entre las distintas áreas de la organización, facilitando así la productividad, la toma de decisiones y la modernización de los servicios tecnológicos.

1.4 Función del Departamento.

El departamento es el encargado de la gestión de infraestructuras de red, asignación, administración y monitoreo de direcciones IP, la administración de servidores y sistemas operativos, el soporte técnico a usuarios, la implementación de políticas de seguridad informática, la protección contra amenazas cibernéticas y la supervisión del rendimiento de los sistemas.

Figura N°2

Estructura Organizativa del departamento de informática



Fuente Ministerio de Desarrollo Social

El departamento se divide en cuatro áreas fundamentales que trabajan de forma transversal:

- **Área de Soporte Técnico:** Encargada del mantenimiento correctivo y preventivo del hardware y la asistencia directa a los usuarios finales.

- **Área de Infraestructura:** Responsable de la gestión de servidores, redes de comunicación y la conectividad física/lógica de la institución.

- **Área de Ciberseguridad:** Encargada de la protección de los activos digitales, la integridad de los datos y la mitigación de vulnerabilidades en la red.

- **Área de Desarrollo:** Responsable de la creación, actualización y mantenimiento de software y sistemas institucionales.

1.5 Descripción del Cargo Ocupado.

Analista de Infraestructura de Red y Seguridad de Sistemas:

El cargo se encuentra adscrito a la Dirección de Informática y Comunicaciones, reportando funcionalmente al Área de Infraestructura bajo la supervisión del Ingeniero en ciberseguridad Norman Vellos.

Con una posición estratégica, ya que actuaba como enlace técnico entre el soporte de hardware y la administración de servicios de servidor, colaborando estrechamente con el área de Ciberseguridad para garantizar el cumplimiento de las políticas de protección de datos institucionales.

Funciones:

- Cambios de IP a diferentes equipos para su debido funcionamiento dentro de la red interna.
- Actualización de servidores que se utilizaran para llevar el control de IP asignadas a los relojes de marcación.
- Realizar diagramas de red para la aplicación de servicios de internet, telefonía y cámaras de vigilancia en los diferentes CAIPIS a nivel nacional.

1.6 Interacción Del Departamento De Informática Con Otras Áreas De La Institución.

Se garantiza la operatividad, seguridad y eficiencia de los sistemas tecnológicos, esta interacción permite alinear las necesidades tecnológicas con los objetivos estratégicos de cada departamento.

1.7 Importancia Del Departamento En El Engranaje De La Organización.

La importancia del departamento de informática constituye la columna vertebral tecnológica del Ministerio de Desarrollo Social. Su relevancia en el engranaje institucional se fundamenta en tres pilares estratégicos:

Garantía de Continuidad Operativa: Es el área responsable de que los servicios digitales y la infraestructura de red se mantengan activos. Sin una gestión eficiente de servidores y conectividad, los procesos administrativos y la atención se detendrían, afectando directamente la misión social de la organización.

Integridad y Custodia de la Información: La institución maneja datos sensibles de la población, el departamento actúa como el guardián de la seguridad lógica. A través de la administración de sistemas, asegura que la información sea veraz, esté disponible y protegida contra accesos no autorizados.

Transformación y Eficiencia Digital: El departamento no solo mantiene lo existente, sino que impulsa la modernización. Mediante el análisis de sistemas y la optimización de redes, permite automatizar procesos manuales —como el control de asistencia—, reduciendo el margen de error humano y optimizando los recursos del Estado.

CAPÍTULO II.

ANÁLISIS DE LA EXPERIENCIA

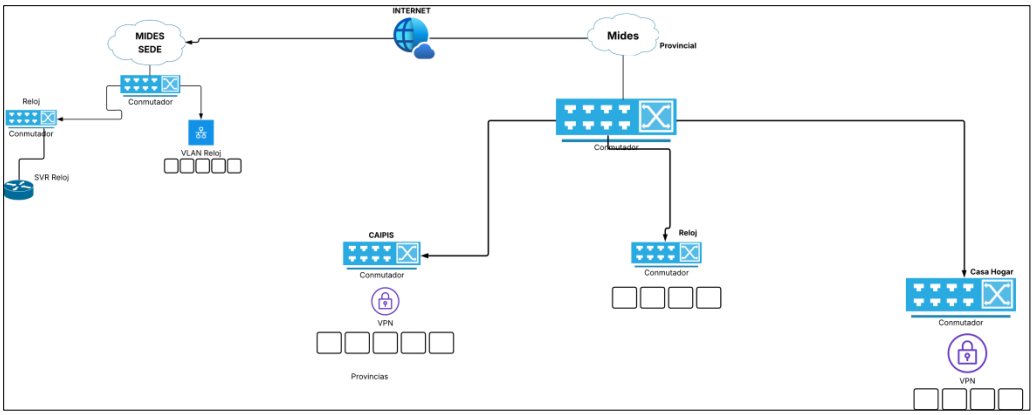
2.1 Funciones Realizadas Durante La Práctica.

En el Ministerio de Desarrollo Social me fueron asignadas diferentes funciones de la cuales puedo destacar:

2.1.1 Preparación de un sistema de red sencillo: que será implementado en los CAIPI (Centros de Atención Integral a la Primera Infancia). Este diagrama debería ser aplicado en la sede principal y en 90 centros distribuidos en las provincias y comarcas de Panamá.

Figura N°3

Diagrama de red



Fuente propia: primer borrador de cómo sería el diseño a implementar.

Tabla N°1

Cantidad de Centros en el país.

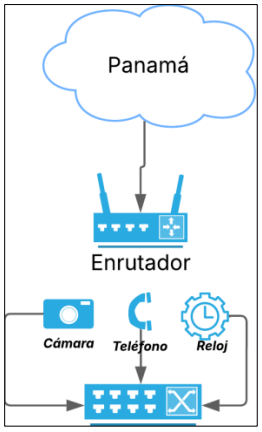
Región	Cantidad
Arraiján	2
Panamá Centro	4
Panamá Este	2
Panamá Norte	5
San Miguelito	11
Chorrera	3
Herrera	8
Los Santos	13
Colón	4
Coclé	13
Chiriquí	9
Comarca Ngäbe-Buglé	2
Veraguas	12
Guna Yala	1

2.1.2 Se hace un cambio en el diseño en el área provincial.

Por problemas de seguridad se decide cambiar el diseño

Figura N°4

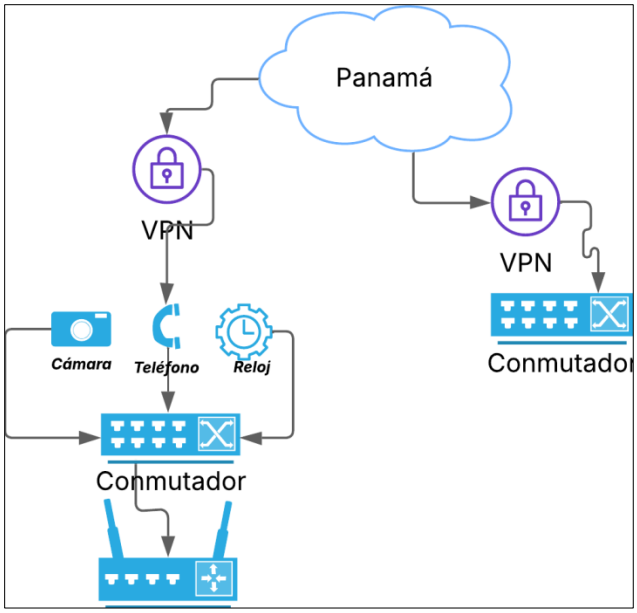
Diagrama de red antiguo



Fuente propia: diseño aplicado para todas las provincias.

Figura N°5

Nuevo diagrama de red



Se propuso la idea de agregar un VPN, ya que al generar tráfico fuera de la red local puede implicar riesgos.

Al configurar el VPN al enrutador principal se brinda seguridad adicional, garantizando la confidencialidad, integridad y autenticidad de los datos transmitidos a través de la red pública.

2.2 Configuración desde cero: de un servidor para almacenar los datos de los relojes de marcación, donde cada dispositivo se identifica por su dirección IP.

Figura N°6

Evaluación interna del equipo

Fuente Propia

Debido a que el equipo llevaba tiempo sin ser utilizado, se hizo una evaluación y mantenimiento, incluyendo el aumento de RAM.

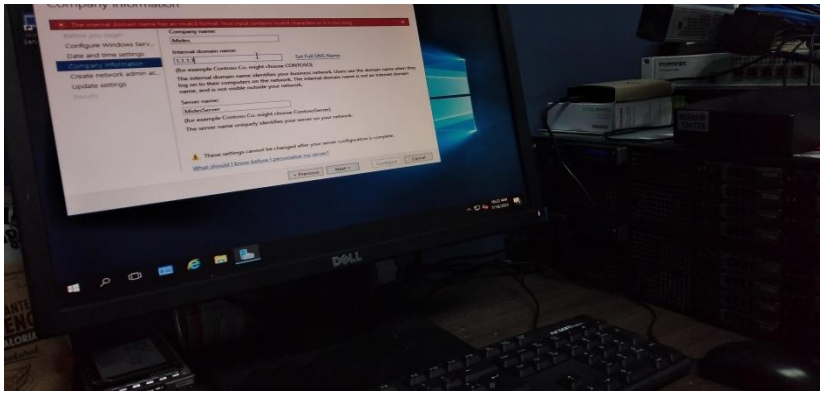
Figura N°7

Equipo listo para su configuración

Fuente propia

Figura N° 8

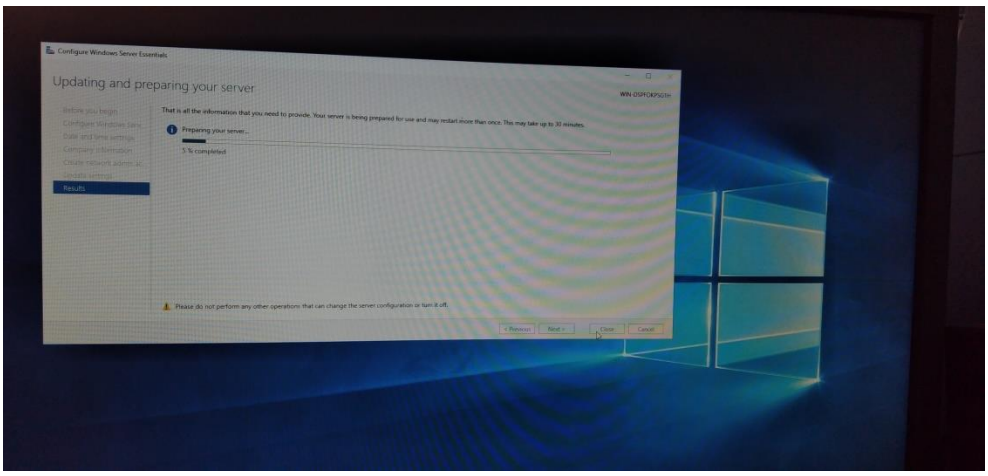
Configuración del servidor



Fuente propia

Figura N° 9

Configuración final del servidor



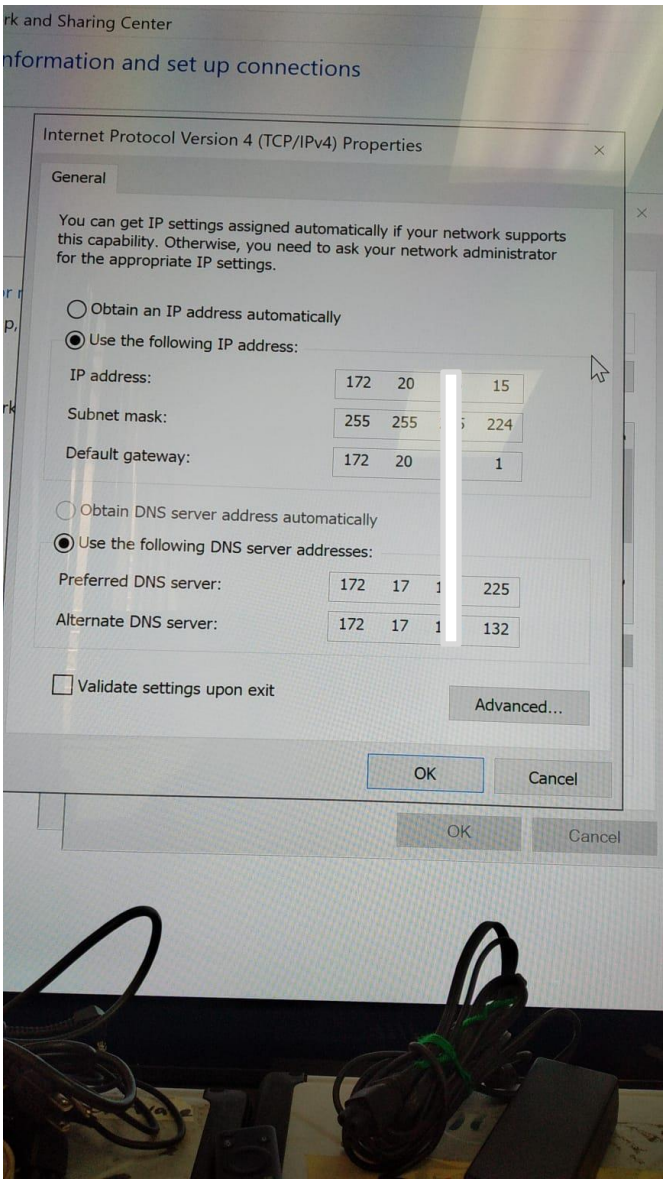
Fuente propia

Fase final de implementación del sistema operativo: configuración y preparación del servidor para su posterior integración al dominio institucional.

Después se le asigna la IP que recopila los registros de asistencia o eventos enviados por cada dispositivo.

Figura N°10

Asignación de IP, Gateway, Mascara y DNS



Fuente propia.

2.2.1 ¿Cómo funcionaría el servidor con los relojes de marcación?

La implementación de un sistema de control de asistencia, se requiere la configuración de una infraestructura de red que permita la interconexión eficiente entre los relojes de marcación y el servidor central. Para ello, cada dispositivo es incorporado a la red mediante la asignación de una dirección IP única, lo que posibilita su identificación individual y garantiza una comunicación organizada dentro del entorno.

Asignar y gestionar estas direcciones IP constituye un aspecto fundamental, ya que permite mantener un control preciso sobre cada reloj de marcación, evitando conflictos de direccionamiento y facilitando tareas de administración, monitoreo y mantenimiento. Cada dispositivo, al contar con su propia dirección IP, puede ser gestionado de manera independiente dentro de la red.

Este servidor se encarga de recibir los datos enviados por cada reloj, identificándolos a través de su dirección IP, lo que permite organizar y almacenar los registros de manera estructurada.

Se implementan mecanismos de comunicación que permiten la transferencia de datos entre múltiples dispositivos y el servidor de forma simultánea. Gracias a la identificación individual mediante direcciones IP, es posible gestionar múltiples conexiones sin interferencias, garantizando la integridad y disponibilidad de la información.

Desde el punto de vista de la seguridad, se recomienda la segmentación de la red mediante el uso de VLANs, con el fin de aislar el tráfico generado por los relojes de marcación del resto de la infraestructura. Asimismo, la implementación de firewalls permite controlar y filtrar el acceso al servidor, restringiendo únicamente a las direcciones IP autorizadas. En escenarios donde la comunicación se realiza a través de redes externas, el uso de VPNs contribuye a proteger la transmisión de datos mediante cifrado, evitando accesos no autorizados y garantizando la confidencialidad de la información.

Figura N°11

Estilo de los relojes de marcación

Fuente ZkTeco Panamá

Figura N°12

Modelo antiguo pero funcional

Fuente ZKTeco

2.2.2 Se procedió a la configuración de los relojes dentro de la institución

(Por temas de confidencialidad no se permitía tomar fotos)

2.3 Verificación del funcionamiento de los relojes.

Para este proceso generalmente se realiza utilizando software especializado proporcionado por el fabricante del dispositivo o mediante protocolos de comunicación configurados previamente y agregando la IP del reloj que queremos verificar, estos permiten la transferencia de datos de forma segura y estructurada.

La información descargada incluye registros de marcación con fecha, hora de entrada, hora de salida y, en algunos casos, identificación del usuario por huella, rostro o número de serie asignado al momento del registro.

Después de verificar el funcionamiento correcto, los datos son almacenados en el servidor central, donde pueden ser organizados, procesados y utilizados para la generación de reportes, control de asistencia.

Tabla N°2

Evaluación de descarga de información de los relojes de marcación

ID	Lugar	IP	Funcionamiento
2	Rrhh Sede	172.20.xx.xx	Si
15	Chiriquí	10.104.x.xxx	Si
16	Bocas Del Toro	10.104.x.xxx	Si
17	Veraguas	10.104.x.xxx	Si
19	Herrera	10.104.xx.xxx	Si
20	Coclé	10.104.xx.xxx	Si
21	Chorrera	10.104.xx.xxx	Si
22	San Miguelito	10.104.xx.xxx	Si
23	Chepo	10.104.xx.xxx	Si
24	Colón 1	10.104.xx.xxx	Si
25	Arraiján	10.104.xx.xxx	Si
26	Principal Planilla	172.20.xx.xx	Si
27	Cafetería	172.20.xx.xx	Si
28	R_ Informática	172.20.xx.xx	Si
30	Principal1	172.20.xx.xx	Si
31	Principal 2	172.20.xx.xx	Si
32	Administración 2	10.103.x.xxx	No
33	Administración1	10.103.x.xxx	No
35	Coai	10.104.xx.xxx	Si
39	Auditoria Padrino	10.104.xx.xxx	Si
41	Dids /120-Abajo	10.104.xx.xxx	Si
42	Panamá Este	10.105.xx.xxx	Si
43	Comarca_ Ngäbe-Buglé	10.104.xx.xxx	Si
45	Panamá Norte	10.105.xx.xxx	Si

48	Los Santos 2	10.104.x.xxx	Si
49	Meteti Darién	10.105.xx.xx	Si
50	Cefodea	10.105.xx.xxx	Si
55	Reloj Despacho	10.102.xx.xxx	Si
56	Gabinete_Social	10.104.xx.xxx	Si
57	Renab_Sede	10.104.x.xxx	Si
58	A. guardián Nuevo	172.20.xx.xxx	Si
60	Colón 2	10.104.xx.xxx	Si
61	Almacén	172.20.xx.xx	No
62	Transporte	10.104.xx.xxx	No
63	Dids/120-Arriba	10.104.xx.xxx	Si
66	Las Tablas	10.104.x.xxx	Si
67	Bocas Planta Baja	10.104.x.xxx	Si
78	Seguridad	172.20.xx.xxx	Si

Fuente Ministerio de Desarrollo Social

(IP censuradas por confidencialidad)

2.4 Análisis de Desempeño.

Durante el desarrollo de la pasantía, el desempeño de la misma se caracterizó por una evolución progresiva en la ejecución de las funciones asignadas dentro del departamento de informática. En una fase inicial, se enfocó en la observación y comprensión de la infraestructura de red existente, lo que permitió identificar la organización de los dispositivos, particularmente los relojes biométricos, así como su integración dentro del sistema.

A medida que avanzó la pasantía, se participó activamente en tareas relacionadas con la asignación y verificación de direcciones IP, la revisión de la conectividad entre dispositivos y la propuesta de mejoras orientadas a optimizar el almacenamiento de los datos generados. En este proceso, se evidenció la aplicación de conocimientos teóricos en redes, así como el desarrollo de habilidades prácticas en la gestión de sistemas.

Entre los principales aprendizajes se destacan la configuración básica de servidores para almacenamiento de información, la importancia de la segmentación y organización de la red, y la implementación de medidas de seguridad como el uso de VPN. No obstante, se enfrentaron dificultades iniciales relacionadas con la comprensión de configuraciones preexistentes y la adaptación a herramientas específicas de la institución.

En términos de logro, se alcanzó un nivel satisfactorio, evidenciado en la capacidad de analizar problemáticas reales, proponer soluciones viables y adaptarse al entorno laboral, cumpliendo con los objetivos establecidos por el tutor industrial.

2.5 Limitaciones o Dificultades Presentadas.

Durante la ejecución de la pasantía se identificaron diversas limitaciones de carácter técnico, organizacional y operativo. La falta de estandarización en los equipos biométricos fue el mayor reto técnico, ya que impidió una integración uniforme y complicó el flujo de información.

A nivel organizacional, se evidenció una limitada documentación de los procesos y configuraciones existentes, lo que dificultó la comprensión inicial del funcionamiento del sistema y requirió un mayor esfuerzo de análisis e investigación. Asimismo, el acceso restringido a ciertos recursos críticos, debido a políticas de seguridad, restringió la posibilidad de realizar configuraciones directas en algunos casos.

En cuanto a los recursos, se observaron ciertas deficiencias en la infraestructura tecnológica, como la falta de disparidad en la asignación de direcciones IP y la ausencia de un sistema centralizado completamente optimizado para la gestión de datos. A pesar de estas dificultades, se implementaron estrategias como la consulta constante con el personal del departamento, el aprendizaje autónomo y la aplicación de criterios técnicos, lo que permitió superar en gran medida las barreras identificadas.

2.6 Aportes y Conocimientos de la Experiencia a la Formación Profesional.

La pasantía profesional representó un aporte significativo a la formación académica, al permitir la integración de conocimientos teóricos con su aplicación en un entorno real. Esta experiencia facilitó la consolidación de conceptos fundamentales en redes de comunicación, tales como direccionamiento IP, interconectividad de dispositivos, gestión de servidores y principios de seguridad informática.

Se fortalecieron competencias prácticas en la resolución de problemas técnicos, el análisis de infraestructuras de red y la toma de decisiones orientadas a la optimización de procesos. La interacción directa con equipos y sistemas reales permitió comprender la complejidad de los entornos tecnológicos empresariales, más allá del enfoque teórico abordado en el aula. La experiencia contribuyó al desarrollo de habilidades transversales como el trabajo en equipo, la comunicación técnica, la organización del tiempo y la adaptación a entornos laborales. Estos elementos son fundamentales para el desempeño profesional en el área de redes y seguridad.

En este sentido, la pasantía no solo reforzó los conocimientos adquiridos durante la carrera, sino que también permitió identificar áreas de mejora y especialización futura dentro del campo de la tecnología.

2.7 Relación De La Pasantía Profesional Con La Carrera Estudiada.

La pasantía de extensión profesional ocupacional mantiene una relación directa y coherente con la Licenciatura en Ingeniería en Redes de Comunicaciones con énfasis en Seguridad, ya que las funciones desarrolladas se alinean con las competencias y áreas formativas de la carrera. Actividades como la asignación y administración de direcciones IP se vinculan con asignaturas relacionadas como Servicios Avanzados de Redes IP.

De igual forma, la participación en la configuración de un servidor para el almacenamiento de datos se relaciona con materias orientadas a la administración de sistemas y servicios de red. La evaluación e implementación de mecanismos de seguridad, como el uso de VPN, guarda estrecha relación con los contenidos de seguridad informática y protección de la información.

El análisis de la infraestructura tecnológica existente y la propuesta de mejoras evidencian la aplicación de competencias en diseño, gestión y optimización de redes, aspectos fundamentales en la formación del ingeniero/a en redes. Además, la experiencia permitió comprender el rol estratégico del departamento de TI dentro de la institución, reforzando la importancia de la carrera en el contexto empresarial. En conjunto, la realización de la pasantía constituye una experiencia integradora que articula los conocimientos teóricos adquiridos durante la formación académica con su aplicación práctica, contribuyendo al desarrollo de un perfil profesional acorde a las exigencias del campo laboral.

2.8 Cronograma de actividades.

Cronograma de Actividades		
Actividades	**Fecha**	**Resultado**
Inducción al departamento de TI y reconocimiento del entorno laboral.	Lunes 19/01 al Miércoles 21/01/2026	Comprensión de la estructura organizacional y funciones del área de TI, desarrollada con éxito.
Levantamiento de información de la infraestructura de red existente.	Jueves 22/01 al Lunes 26/01/2026	Identificación de dispositivos y topología de red, con resultados satisfactorios.
Inventario y verificación de dispositivos biométricos.	Martes 27/01 al Viernes 30/01/2026	Registro actualizado de equipos realizado de manera satisfactoria.
Revisión y organización de direcciones IP asignadas.	Lunes 02/02 al Jueves 05/02/2026	Control del direccionamiento IP desarrollado correctamente.
Diagnóstico de problemas de comunicación.	Viernes 06/02 al Martes 10/02/2026	Identificación de fallas de conectividad con resultados positivos.
Propuesta de mejora en la red.	Miércoles 11/02 al Viernes 13/02/2026	Diseño optimizado de red elaborado con éxito.
Configuración de servidor de almacenamiento.	Jueves 19/02 al Viernes 20/02/2026	Sistema centralizado implementado satisfactoriamente.
Pruebas de conectividad y transferencia de datos	Lunes 23/02 al Viernes 27/02/2026	Validación de funcionamiento realizada con éxito.
Implementación de VPN.	Lunes 02/03 al Viernes 06/03/2026	Acceso seguro a la red implementado satisfactoriamente.
Documentación de procesos.	Lunes 09/03 al Viernes 13/03/2026	Registros técnicos elaborados con resultados satisfactorios.
Optimización del acceso a datos.	Lunes 16/03 al Viernes 20/03/2026	Mejora en consulta de registros desarrollada exitosamente.
Evaluación y ajustes finales.	Lunes 23/03 al Miércoles 25/03/2026	Correcciones implementadas de manera satisfactoria.
Elaboración del informe final.	Jueves 26/03 al Viernes 27/03/2026	Documento final elaborado y organizado con éxito.

Capítulo III

Diagnóstico Observacional

3.1 Descripción De La Problemática Observada.

Durante los 2 meses que estuve realizando la pasantía en el Ministerio de Desarrollo Social, aplicando los conocimientos aprendidos en mi carrera, Ingeniería en Redes de Comunicaciones con énfasis en Seguridad, note varios inconvenientes, entre ellos puedo destacar:

La inexistencia de un esquema estructurado de direccionamiento IP, esto provocaba ciertas inconsistencias en la identificación de los dispositivos dentro de la red, que dificultaban su administración, monitoreo y escalabilidad.

Todos los equipos operaban sin una estandarización clara, lo que incrementaba la probabilidad de conflictos de red, errores en la conectividad y limitaciones en la trazabilidad de los datos.

Respecto a los relojes de marcación, la falta de un servidor centralizado que se dedicara al almacenamiento y gestión de la información, esto implicaba que los registros de entrada y salida del personal no se guardaran de manera eficiente y segura.

Al no contar o tener escasos mecanismos apropiados para el respaldo, control de acceso y recuperación de datos, esta situación representaba un riesgo operativo como la integridad de la información.

Basándose en el área de seguridad, la problemática estaba en la falta de implementación de medidas como segmentación de la red, el uso de VPN, esto dejaba la red expuesta a posibles vulnerabilidades, accesos no autorizados y la intercepción de la información.

3.2 Alternativas de solución a la problemática planteada, desde el área de formación.

Con el propósito de mejorar la gestión y administración de la infraestructura tecnológica observada durante la pasantía profesional, se plantearon diversas alternativas orientadas a optimizar el control, seguridad y disponibilidad de la información dentro del departamento de informática:

- Implementación de una correcta segmentación y asignación de direcciones IP para mejorar la organización y monitoreo de los dispositivos conectados a la red.

- Configuración de servidores destinados al almacenamiento centralizado de la información generada por los relojes biométricos, permitiendo un mejor control y respaldo de los registros de entrada y salida del personal.

- Aplicación de mecanismos de seguridad informática, como el uso de VPN y controles de acceso, con el fin de proteger la comunicación y transferencia de datos dentro de la red interna institucional.

- Desarrollo de procedimientos estandarizados para la descarga, administración y respaldo de la información almacenada en los equipos de control de asistencia.

- Fortalecimiento de las políticas de monitoreo y mantenimiento preventivo de la infraestructura tecnológica para garantizar la continuidad operativa de los servicios informáticos.

La aplicación de estas medidas permitirá mejorar la eficiencia operativa del departamento de informática, garantizando una administración más segura, organizada y confiable de los recursos tecnológicos.

Conclusiones

Cumplimiento de objetivos: Se ejecutaron satisfactoriamente las metas programadas en las áreas de Administración de Servidores y Análisis de Sistemas, logrando la transición de una infraestructura con deficiencias críticas hacia un modelo de red estructurado y seguro.

Análisis y Diagnóstico de Sistemas: Se realizó una evaluación profunda de la gestión de datos y el direccionamiento IP, identificando vulnerabilidades en la integridad y disponibilidad de la información de los sistemas de control de asistencia.

Optimización de Infraestructura: Se modificó la arquitectura física y lógica de la red, mejorando la interconexión de los dispositivos y garantizando un entorno de hardware robusto capaz de soportar la carga operativa institucional.

Producto Principal - Esquema de Seguridad y Red: el diseño e implementación de un nuevo esquema de direccionamiento IP bajo estándares de seguridad, lo que permitió segmentar la red, mitigar riesgos de intrusión y facilitar el monitoreo proactivo de los activos tecnológicos.

Gestión de Servidores: Se establecieron las bases para la centralización de la información, optimizando la administración de los servidores para asegurar que los procesos de automatización futura cuenten con una plataforma estable y escalable.

Enfoque en Seguridad: La implementación de medidas de control para asegurar la integridad de los datos generados por los sistemas de asistencia, reduciendo la superficie de exposición ante posibles fallos o accesos no autorizados.

Recomendaciones

Técnicas (Infraestructura): Se recomienda la transición hacia una segmentación de red mediante la configuración de VLANs y la implementación de un sistema de monitoreo de tráfico. Esto permitirá optimizar el rendimiento del servidor y asegurar que la carga de los dispositivos de asistencia no afecte los servicios críticos de la sede institucional.

Monitoreo Proactivo: Implementar herramientas de monitoreo de red que permitan alertar en tiempo real sobre caídas de dispositivos o saturación del ancho de banda dentro de la red local, pasando de una gestión reactiva a una preventiva.

Organizacionales: Es fundamental establecer un Protocolo de Mantenimiento Preventivo y una base de conocimientos (documentación técnica) actualizada. Esto garantiza que el personal administrativo pueda dar continuidad a la gestión del direccionamiento IP y la administración de sistemas sin depender de procesos reactivos ante fallos.

Documentación Continua: Mantener actualizado el inventario de hardware y el mapa de direccionamiento IP creado en esta pasantía, asegurando que cualquier cambio futuro en la infraestructura quede registrado para facilitar el soporte técnico.

Seguridad: Se debe implementar una política estricta de respaldos automatizados (Backups) bajo la regla 3-2-1 y reforzar el control de acceso al servidor mediante auditorías de registros (logs). Esto protege la integridad de los datos de asistencia frente a accesos no autorizados o pérdida de información crítica.

Actualización y Parches: Definir un cronograma estricto de actualizaciones de seguridad tanto para el sistema operativo del servidor, como para el firmware de los dispositivos de control de asistencia, mitigando vulnerabilidades conocidas.

Glosario

Autenticación: Proceso de verificación de identidad de un usuario o dispositivo antes de acceder a un sistema o red (Stallings, 2014).

DHCP (Dynamic Host Configuration Protocol): Protocolo que asigna automáticamente direcciones IP y otros parámetros de red a los dispositivos (Cisco, 2023).

Dirección IP: Identificador lógico único que permite la comunicación de un dispositivo dentro de una red (Tanenbaum & Wetherall, 2012).

Dirección MAC: Identificador físico único asignado a una interfaz de red por el fabricante (Cisco, 2023).

DNS (Domain Name System): Sistema que traduce nombres de dominio en direcciones IP (Microsoft, 2023).

Firewall: Sistema que controla y filtra el tráfico de red según políticas de seguridad establecidas (Stallings, 2014).

Gateway (Puerta de enlace): Dispositivo que permite la comunicación entre diferentes redes (Tanenbaum & Wetherall, 2012).

Integridad de datos: Garantía de que la información permanece exacta y sin alteraciones no autorizadas (ISO/IEC 27001, 2022).

Monitoreo de red: Supervisión continúa del estado y rendimiento de una red (Cisco, 2023).

Reloj biométrico: Dispositivo utilizado para registrar la asistencia mediante características físicas del usuario (ZKTeco, s.f.).

Router: Equipo encargado de dirigir el tráfico de datos entre distintas redes (Tanenbaum & Wetherall, 2012).

Servidor: Sistema que proporciona servicios o recursos a otros dispositivos en la red (Microsoft, 2023).

Switch: Dispositivo que interconecta equipos dentro de una red local (Cisco, 2023).

TCP/IP: Conjunto de protocolos que permiten la comunicación entre dispositivos en una red (Tanenbaum & Wetherall, 2012).

VLAN: Segmentación lógica de una red para mejorar su administración y seguridad (Cisco, 2023).

VPN: Tecnología que permite una conexión segura a través de redes públicas (Microsoft, 2023).

Bibliografía

Cisco Systems. (2020). *Design Zone for Campus Wired and Wireless LAN*. Cisco. cisco.com

Microsoft. (2023). Documentación de Windows Server. Microsoft Learn. microsoft.com

Stallings, W. (2014). Criptografía y seguridad de redes: Principios y práctica (5ta ed.). Pearson Education. pearson.com

Tanenbaum, A. S., & Wetherall, D. J. (2012). Redes de computadoras (5ta ed.). Pearson Educación. pearson.com

Ministerio de Desarrollo Social. (s.f.). *Historia del MIDES*. Gobierno de la República de Panamá. mides.gob.pa

Ministerio de Desarrollo Social. (s.f.). *Misión y Visión*. Gobierno de la República de Panamá. mides.gob.pa

Ministerio de Desarrollo Social. (s.f.). *Servicios*. Gobierno de la República de Panamá. mides.gob.pa

ZKTeco. (s.f.). *Sistemas de Control de Acceso y Relojes de Marcación*. ZKTeco Latinoamérica. zktecolatinoamerica.com

Cisco Systems. (2023). Networking Essentials Glossary. Cisco Networking Academy. Cisco.comISO/IEC. (2022).

ISO/IEC 27001: Information security, cybersecurity and privacy protection. International Organization for Standardization. iso.org

Anexos

Figura N°13

Explicación de cómo sería el diagrama de red dibujado.

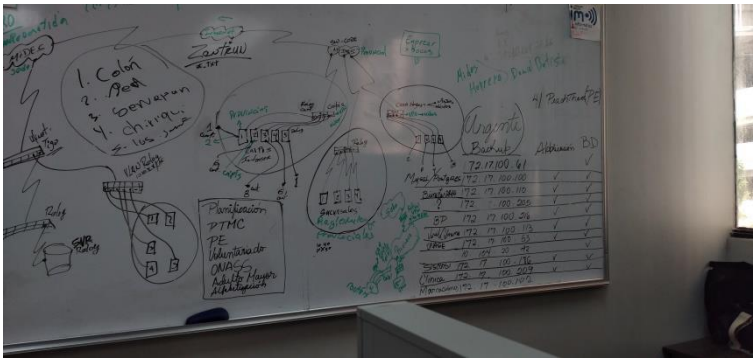


Figura N°14

Problemas de conectividad en la red.

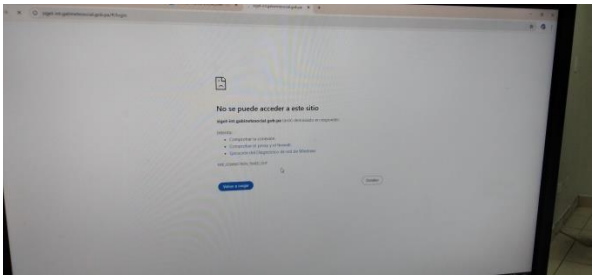
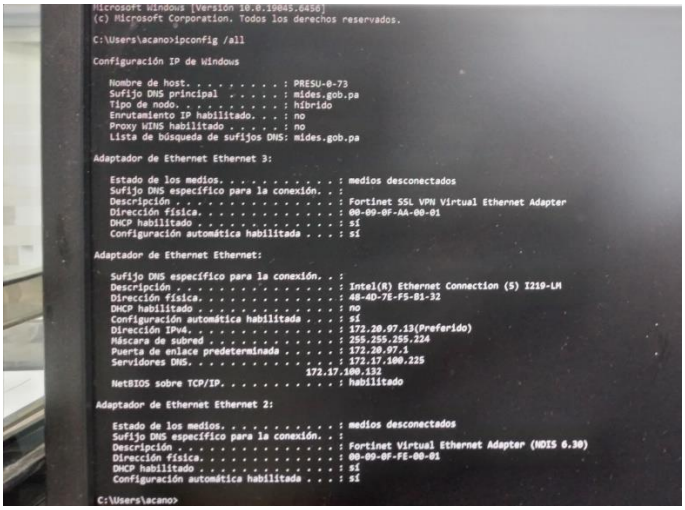


Figura N°15

Prueba de ping a equipos que presentaban problemas de conexión.



GOBIERNO NACIONAL
★ CON PASO FIRME ★

MINISTERIO DE DESARROLLO SOCIAL

Oficina Institucional de Recursos Humanos

Área de Capacitación y Desarrollo del Servidor Público

Panamá, 15 de diciembre de 2025
Nota No. 1322/OIRH-ACYDSP/2025

Licenciada
Alba Meta
Secretaría General
Universidad Internacional de Ciencia y Tecnología
E. S. D.

Licenciada Meta:

Por este medio, me dirijo a usted en respuesta de la Nota No. CARCE-RE-PA25-0012 de 21 de noviembre de 2025, a través de la cual solicita que la estudiante **DIANA LISBETH MORCILLO SALAZAR** con cédula de identidad personal **8-923-484,** quien cursa la Licenciatura en Ingeniería en redes de Comunicaciones con énfasis en Seguridad de la Universidad Internacional de Ciencia y Tecnología (UNICYT), realice su Práctica Profesional en nuestra institución.

Sobre el particular, hago de su conocimiento que cuenta con nuestra anuencia para que la estudiante, realice su Práctica Profesional de ocho (8) semanas, en el **Departamento de Informática** del Ministerio de Desarrollo Social, a partir del **5 de enero de 2026** hasta el **6 de marzo de 2026**, de **lunes de viernes** en horario de **8:00 a.m. a 4:00 p.m.,** bajo la supervisión del Licenciado Manuel Salgado, Director del Departamento de Informática.

Para mayor información, puede consultar a la Sección de Capacitación y Desarrollo del Servidor Público de la Oficina Institucional de Recursos Humanos, al teléfono 500-6045 o a los correos mmartez@mides.gob.pa, eurrutia@mides.gob.pa o mgutierrez@mides.gob.pa.

Atentamente,

MINISTERIO DE DESARROLLO SOCIAL
Oficina Institucional
RECURSOS HUMANOS
PANAMÁ

Licda. Jackeline Santos
Jefa de la Oficina Institucional de Recursos Humanos

JS/mm/mgp

SICA 2025 PANAMÁ

Dirección de Informática y Comunicaciones

Tel. 500-6033

Nota N°05/DIC/2026

Panamá. 27 de marzo de 2026

Universidad Internacional de Ciencia y Tecnología

Atención:
Licenciada: Mercedes N. Villanueva de Armentetos
Secretaría General

Reciba un cordial y respetuoso saludo, a través de la presente certificamos que la estudiante Diana Lisbeth Morcillo Salazar con cedula de identidad personal N°8-923-484, realizo labores en nuestro equipo de tecnología bajo la supervisión del Ingeniero Norman Vellos, desde el 19 de enero hasta el 27 de marzo del presente año 2026.

Durante estas 10 semanas la joven Diana demostró lo siguiente:

- Calidad de trabajo
- Eficiencia y efectividad en los proyectos asignados
- Desenvolvimiento práctico ante los problemas técnicos
- Asistencia y Puntualidad
- Iniciativa y creatividad

Esperando la misiva sea tomada en cuenta

Atentamente

Licdo. Manuel Salgado Sáenz
Director de Informática

MINISTERIO DE DESARROLLO SOCIAL
INFORMÁTICA Y COMUNICACIONES
PANAMÁ

GOBIERNO NACIONAL
★ CON PASO FIRME ★

MINISTERIO DE DESARROLLO SOCIAL
OFICINA INSTITUCIONAL DE RECURSOS HUMANOS

REGISTRO DE ASISTENCIA

[DAD ADMINISTRATIVA: _____ **MES** _____ **DE** 20_____.

FECHA	NOMBRE DEL FUNCIONARIO	FIRMA	HORA DE ENTRADA	ALMUERZO		HORA DE SALIDA
				HORA DE SALIDA	HORA DE LLEGADA	
19/1/2026	Diana Morcillo	Diana Morcillo	8:00 Am			5:00 p.m
20/01/2026	Diana Morcillo	Diana Morcillo	8:03 A M			5:00 pm.
21/01/2026	Diana Morcillo	Diana Morcillo	8:04 AM			5:07 p m.
22/01/2026	Diana Morcillo	Diana Morcillo	8:00 A m			5:00 PM
23/01/2026	Diana Morcillo	Diana Morcillo	8:06 Am.			5:00 p.M.
26/01/2026	Diana Morcillo	Diana Morcillo	8:03 Am			5:06 pm.
27/01/2026	Diana Morcillo	Diana Morcillo	7:59 A m.			5:03 PM
28/01/2026	Diana Morcillo	Diana Morcillo	8:05 a. m.			5:03 pm.
29/01/2026	Diana Morcillo	Diana Morcillo	7:58 a. m.			5:01 p.m.
30/01/2026	Diana Morcillo	Diana Morcillo	7:57 a. m.			5:04 pm.
2/02/2026	Diana Morcillo	Diana Morcillo	8:02 a m.			5:03 p m.
3/02/2026	Diana Morcillo	Diana Morcillo	7:58 a. m.			4:02 p. m.
4/02/2026	Diana Morcillo	Diana Morcillo	7:53 a. m.			4:02 p. m
5/02/2026	Diana Morcillo	Diana Morcillo	7:50 a m			4:01 p. m.
6/02/2026	Diana Morcillo	Diana Morcillo	7:57 a m.			4:02 p. m.
9/02/2026	Diana Morcillo	Diana Morcillo	7:56 a. m.			4:00 p. m.
10/02/2026	Diana Morcillo	Diana Morcillo	7:53 a. m			4:01 p. m.
11/02/2026	Diana Morcillo	Diana Morcillo	7:55 a. m.			4:01 p. m.
12/02/2026	Diana Morcillo	Diana Morcillo	7:56 a. m			4:02 p. m.
13/02/2026	Diana Morcillo	Diana Morcillo	7:57 a. m.			4:01 p. m.
19/02/2026	Diana Morcillo	Diana Morcillo	7:57 a. m.			4:02 pm.

obligatorio que cada Servidor Públicos firme con puño y letra y en orden de llegada. No debe saltarse ningún renglón. Debe utilizar otra hoja si es necesario.

DEL DIRECTOR (A): _____ **FECHA DE ENTREGA:** 27/3/2026

GOBIERNO NACIONAL
★ CON PASO FIRME ★

MINISTERIO DE DESARROLLO SOCIAL
OFICINA INSTITUCIONAL DE RECURSOS HUMANOS

REGISTRO DE ASISTENCIA

UNIDAD ADMINISTRATIVA: _____ **MES** _____ **DE** 20 _____.

FECHA	NOMBRE DEL FUNCIONARIO	FIRMA	HORA DE ENTRADA	ALMUERZO		HORA DE SALIDA
				HORA DE SALIDA	HORA DE LLEGADA	
20/2/2026	Diana Morcillo	Diana Morcillo	7:58 a.m.			4:02 p.m.
23/2/2026	Diana Morcillo	Diana Morcillo	8:30 a.m.			4:02 p.m.
24/2/2026	Diana Morcillo	Diana Morcillo	7:56 a.m.			4:02 p.m.
25/2/2026	Diana Morcillo	Diana Morcillo	8:30 a.m.			4:04 p.m.
26/2/2026	Diana Morcillo	Diana Morcillo	8:04 a.m.			4:04 p.m.
27/2/2026	Diana Morcillo	Diana Morcillo	7:52 a.m.			4:02 p.m.
2/3/2026	Diana Morcillo	Diana Morcillo	7:48 a.m.			4:05 p.m.
3/3/2026	Diana Morcillo	Diana Morcillo	7:57 a.m.			4:02 p.m.
4/3/2026	Diana Morcillo	Diana Morcillo	7:54 a.m.			4:02 p.m.
5/3/2026	Diana Morcillo	Diana Morcillo	7:50 a.m.			4:02 p.m.
6/3/2026	Diana Morcillo	Diana Morcillo	7:54 a.m.			4:02 p.m.
9/3/2026	Diana Morcillo	Diana Morcillo	8:15 a.m.			4:02 p.m.
10/3/2026	Diana Morcillo	Diana Morcillo	7:56 a.m.			4:03 p.m.
11/3/2026	Diana Morcillo	Diana Morcillo	7:52 a.m.			4:04 p.m.
12/3/2026	Diana Morcillo	Diana Morcillo	7:50 a.m.			4:02 p.m.
13/3/2026	Diana Morcillo	Diana Morcillo	8:00 a.m.			4:02 p.m.
16/3/2026	Diana Morcillo	Diana Morcillo	7:49 a.m.			4:01 p.m.
17/3/2026	Diana Morcillo	Diana Morcillo	7:55 a.m.			4:04 p.m.
18/3/2026	Diana Morcillo	Diana Morcillo	8:00 a.m.			4:02 p.m.
19/3/2026	Diana Morcillo	Diana Morcillo	7:50 a.m.			4:02 p.m.
20/3/2026	Diana Morcillo	Diana Morcillo	7:47 a.m.			4:02 p.m.

obligatorio que cada Servidor Públicos firme con puño y letra y en orden de llegada. No debe saltarse ningún renglón. Debe utilizar otra hoja si es necesario.

DEL DIRECTOR (A): _____ **FECHA DE ENTREGA:** 27/3/2026

GOBIERNO NACIONAL
★ CON PASO FIRME ★

MINISTERIO DE DESARROLLO SOCIAL
OFICINA INSTITUCIONAL DE RECURSOS HUMANOS

REGISTRO DE ASISTENCIA

)AD ADMINISTRATIVA: _____ **MES** _____ **DE** 20_____.

FECHA	NOMBRE DEL FUNCIONARIO	FIRMA	HORA DE ENTRADA	ALMUERZO		HORA DE SALIDA
				HORA DE SALIDA	HORA DE LLEGADA	
3/3/2026	Diana Morcilla	Diana Morcilla	7:53 a.m.			4:02 p.m.
4/3/2026	Diana Morcilla	Diana Morcilla	8:15 a.m.			4:03 p.m.
5/3/2026	Diana Morcilla	Diana Morcilla	7:55 a.m.			4:01 p.m.
6/3/2026	Diana Morcilla	Diana Morcilla	7:47 a.m.			4:01 p.m.
7/3/2026	Diana Morcilla	Diana Morcilla.	7:45 a.m.			4:04 p.m.

gatorio que cada Servidor Públicos firme con puño y letra y en orden de llegada. No debe saltarse ningún renglón. Debe utilizar otra hoja si es necesario.

L DIRECTOR (A): _____ **FECHA DE ENTREGA:** 27/3/2026