



UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ  
EXTENSIÓN EN EL CARMEN  
CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN  
Creada Ley No. 10 – Registro Oficial 313 de noviembre 13 de 1985

## **PROYECTO INTEGRADOR**

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN  
TECNOLOGÍAS DE LA INFORMACIÓN

**SISTEMA DE SEGURIDAD DE REDES CON CABLEADO  
ESTRUCTURADO BASADO EN LA NORMA TIA/EIA 568 PARA EL  
SISTEMA CANTONAL DE IGUALDAD Y PROTECCIÓN INTEGRAL  
DE DERECHOS DE LOS GRUPOS DE ATENCIÓN PRIORITARIA DEL  
CANTÓN EL CARMEN.**

DE LA A BRIONES LUIS MARIO

**AUTOR**

MINAYA MACÍAS RENELMO WLADIMIR

**TUTOR**

EL CARMEN, JULIO 2024

**Uleam**



	NOMBRE DEL DOCUMENTO: CERTIFICADO DE TUTOR(A)	CÓDIGO: PAT-04-F-004
	PROCEDIMIENTO: TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR	REVISIÓN: 1
		Página 1 de 1

## CERTIFICACIÓN

En calidad de docente tutor de la Extensión El Carmen, de la Universidad Laica "Eloy Alfaro" de Manabí, CERTIFICO:

Haber dirigido y revisado el trabajo de investigación, bajo la autoría del estudiante **DE LA A BRIONES LUIS MARIO**, legalmente matriculado en la carrera de Tecnologías de la Información, período académico 2023(2)-2024(1), cumpliendo el total de 384 horas, bajo la opción de titulación de trabajo de Investigación, cuyo tema del proyecto es "Sistema de Seguridad de Redes con Cableado Estructurado Basado en la norma TIA/EIA 568 para el sistema cantonal de igualdad y Protección Integral de Derechos de los Grupos de Atención Prioritaria del cantón El Carmen".

La presente investigación ha sido desarrollada en apego al cumplimiento de los requisitos académicos exigidos por el Reglamento de Régimen Académico y en concordancia con los lineamientos internos de la opción de titulación en mención, reuniendo y cumpliendo con los méritos académicos, científicos y formales, suficientes para ser sometida a la evaluación del tribunal de titulación que designe la autoridad competente.

Particular que certifico para los fines consiguientes, salvo disposición de Ley en contrario.

El Carmen, 26 de Julio del 2024.

Lo certifico,

  
**Wladimir Minaya Macías, Mg.**  
**Docente Tutor**  
**Área: Sistemas**





**Uleam**  
*Extensión El Carmen*

**UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABÍ**

**EXTENSIÓN EL CARMEN**

**APROBACIÓN DEL TRABAJO DE TITULACIÓN**

Los miembros del Tribunal Examinador aprueban el Trabajo de Titulación con modalidad Proyecto Integrador, titulado "SISTEMA DE SEGURIDAD DE REDES CON CABLEADO ESTRUCTURADO BASADO EN LA NORMA TIA/EIA 568 PARA EL SISTEMA CANTONAL DE IGUALDAD Y PROTECCIÓN INTEGRAL DE DERECHOS DE LOS GRUPOS DE ATENCIÓN PRIORITARIA DEL CANTÓN EL CARMEN", cuyo autor es De La A Briones Luis Mario, de la Carrera de Ingeniería en Tecnologías de la Información y como Tutor de Trabajo de Titulación el Ing. Renelmo Wladimir Minaya Macías, Mg.

El Carmen, agosto de 2024

Ing. Mora Marcillo Alex Bladimir, Mg.  
Presidente del tribunal de titulación

Ing. Quiroz Valencia Arturo Patricio, Mg.  
Miembro del tribunal de titulación

Ing. Sinchiguano Chiriboga César Augusto, Mg.  
Miembro del tribunal de titulación

**Uleam**

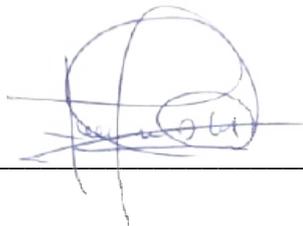
**UNIVERSIDAD LAICA “ELOY ALFARO” DE MANABÍ**

**EXTENSIÓN EN EL CARMEN**



**DECLARACIÓN DE AUTORÍA**

La responsabilidad del contenido de este Trabajo de titulación, cuyo tema es: Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, corresponde exclusivamente a: De La A Briones Luis Mario con CI. 0918021999, y los derechos patrimoniales de la misma corresponden a la Universidad Laica “Eloy Alfaro” de Manabí.



---

De La A Briones Luis Mario

C.I. 0918021999

## **DEDICATORIA**

Este trabajo va dedicado con mucho amor a mi Sra. Madre Hortensia De La A, a mi compañera de vida Shirley Pinela y a mis queridos hijos, Luis, Jean y Marelisa, quienes durante todo este proceso creyeron en mí, siendo ese apoyo fundamental día a día brindándome cada una de las herramientas para alcanzar mis sueños. Gracias a cada palabra de aliento y de su paciencia durante este largo proceso.

Este trabajo va dedicado a ustedes por su comprensión, su apoyo y por cada uno de los momentos de distracción que me ayudaron a seguir adelante.

## **AGRADECIMIENTO**

En primer lugar, quiero agradecer a Dios, primero por cada oportunidad brindada y segundo por darme la fortaleza y sabiduría para poder superar cada desafío a lo largo de este camino

Segundo, tengo un agradecimiento especial para cada uno de mis profesores y mentores durante esta larga trayectoria, grandes maestros que, gracias a sus enseñanzas y dedicación para formar profesionales comprometidos y capaces, lograron saciar cada una de mis dudas y fueron partícipes de este logro alcanzado. Gracias, Ingenieros, Wladimir, Saed, Clarita, Bladimir, Cristhian, César, Soraida, Alexandra, Tatiana, Víctor, Patricio, Rocío, Danilo, César, Ángel, y otros más por cada consejo impartido y por la confianza otorgada.

A cada uno de mis compañeros de estudio, por el apoyo mutuo y las discusiones grupales que teníamos a la hora de entregar un trabajo, Este logro es el resultado de nuestro esfuerzo continuo y en conjunto, de igual forma a las autoridades del sistema cantonal, por facilitarme el acceso a la información y recursos necesarios para llevar a cabo este proyecto.

Finalmente, a todos aquellos que de alguna manera contribuyeron al desarrollo de este proyecto de tesis, mis más sinceros agradecimientos. Su apoyo y colaboración fueron esenciales para alcanzar esta gran meta.

# ÍNDICE GENERAL

<i>PORTADA</i>	<i>I</i>
<i>CERTIFICACIÓN DEL TUTOR</i>	<i>III</i>
<i>TRIBUNAL DE SUSTENTACIÓN</i>	<i>IV</i>
<i>DECLARACIÓN DE AUTORÍA</i>	<i>V</i>
<i>DEDICATORIA</i>	<i>VI</i>
<i>AGRADECIMIENTO</i>	<i>VII</i>
<i>ÍNDICE GENERAL</i>	<i>VIII</i>
<i>ÍNDICE DE TABLAS</i>	<i>XII</i>
<i>ÍNDICE DE ILUSTRACIONES</i>	<i>XIII</i>
<i>ÍNDICE DE ANEXOS</i>	<i>XV</i>
<i>RESUMEN</i>	<i>XVI</i>
<i>ABSTRACT</i>	<i>XVII</i>
<i>CAPÍTULO I</i>	<i>1</i>
<i>1 INTRODUCCIÓN</i>	<i>1</i>
1.1 <b>Introducción</b>	<b>1</b>
1.2 <b>Presentación del tema</b>	<b>2</b>
1.3 <b>Ubicación y contextualización de la problemática</b>	<b>2</b>
1.4 <b>Planteamiento del problema</b>	<b>3</b>
1.4.1    Problematización	3
1.4.2    Génesis del problema	4
1.4.3    Estado actual del problema	5
1.5 <b>Diagrama causa – efecto del problema</b>	<b>5</b>
1.6 <b>Objetivos</b>	<b>7</b>
1.6.1    Objetivo general	7
1.6.2    Objetivos específicos	7

<b>1.7</b>	<b>Justificación</b>	<b>7</b>
<b>1.8</b>	<b>Impactos esperados</b>	<b>8</b>
1.8.1	Impacto tecnológico	9
1.8.2	Impacto social	9
1.8.3	Impacto ecológico	10
<b>CAPÍTULO II</b>		<b>11</b>
<b>2</b>	<b>MARCO TEÓRICO</b>	<b>11</b>
<b>2.1</b>	<b>Antecedentes históricos</b>	<b>11</b>
<b>2.2</b>	<b>Antecedentes de investigaciones relacionadas al tema presentado</b>	<b>12</b>
<b>2.3</b>	<b>Definiciones conceptuales</b>	<b>14</b>
2.3.1	Seguridad de Redes	14
2.3.2	NORMA TIA/EIA 568.	20
2.3.3	Metodología de desarrollo Cascada (Waterfall)	26
<b>2.4</b>	<b>Conclusiones del marco teórico</b>	<b>27</b>
<b>CAPÍTULO III</b>		<b>28</b>
<b>3</b>	<b>MARCO INVESTIGATIVO</b>	<b>28</b>
<b>3.1</b>	<b>Introducción</b>	<b>28</b>
<b>3.2</b>	<b>Tipos de investigación</b>	<b>28</b>
<b>3.3</b>	<b>Métodos de investigación</b>	<b>29</b>
<b>3.4</b>	<b>Fuentes de información de datos</b>	<b>30</b>
3.4.1	Encuestas	30
3.4.2	Entrevista	30
3.4.3	Fichas de Observación	30
<b>3.5</b>	<b>Estrategia operacional para la recolección de datos</b>	<b>31</b>
3.5.1	Población	31
3.5.2	Muestra	31
3.5.3	Análisis de las herramientas de recolección de datos a utilizar	31
3.5.4	Plan de recolección de datos	37
<b>3.6</b>	<b>Análisis y presentación de resultados</b>	<b>38</b>

3.6.1	Tabulación	38
3.6.2	Presentación y descripción de los resultados obtenidos	43
3.6.3	Informe final del análisis de los datos	43
<b>CAPÍTULO IV</b>		<b>45</b>
<b>4</b>	<b>MARCO PROPOSITIVO</b>	<b>45</b>
<b>4.1</b>	<b>Introducción</b>	<b>45</b>
<b>4.2</b>	<b>Descripción de la propuesta</b>	<b>45</b>
<b>4.3</b>	<b>Determinación de recursos</b>	<b>46</b>
4.3.1	Humanos	46
4.3.2	Tecnológicos	47
4.3.3	Económicos	48
<b>4.4</b>	<b>Desarrollo (Metodología Cascada)</b>	<b>48</b>
4.4.1	Requisitos	49
4.4.2	Diseño	51
4.4.3	Implementación	54
4.4.4	Verificación	62
4.4.5	Mantenimiento	66
<b>5</b>	<b>EVALUACIÓN DE RESULTADOS</b>	<b>68</b>
<b>5.1</b>	<b>Introducción</b>	<b>68</b>
<b>5.2</b>	<b>Presentación y monitoreo de resultados</b>	<b>68</b>
5.2.1	Planificación de la evaluación	68
5.2.2	Ejecución del monitoreo	69
<b>5.3</b>	<b>Interpretación objetiva</b>	<b>73</b>
5.3.1	Acceso a la red desde dispositivos no autorizados	73
5.3.2	Compartición de recursos y documentos	73
5.3.3	Acceso a internet	74
5.3.4	Comparación de rendimiento y seguridad de la red	74
5.3.5	Circuito cerrado de cámaras de video vigilancia	74
5.3.6	Productividad y efectividad	75
<b>CAPÍTULO VI</b>		<b>76</b>

<b>6</b>	<b>CONCLUSIONES Y RECOMENDACIONES</b>	<b>76</b>
6.1	Conclusiones	76
6.2	Recomendaciones	77
	<b>BIBLIOGRAFÍA</b>	<b>79</b>
7	<i>Bibliografía</i>	79
	<b>ANEXOS</b>	<b>82</b>

## ÍNDICE DE TABLAS

TABLA 1. POBLACIÓN _____	31
TABLA 2. PLAN DE RECOLECCIÓN DE DATOS _____	37
TABLA 3. RESULTADOS DE LA ENCUESTA _____	40
TABLA 4. RESULTADOS DE LA ENTREVISTA _____	43
TABLA 5. RECURSOS HUMANOS _____	47
TABLA 6. RECURSOS TECNOLÓGICOS _____	48
TABLA 7. RECURSOS ECONÓMICOS _____	48
TABLA 8. EQUIPOS TECNOLÓGICOS DE LA JUNTA CANTONAL _____	52

## ÍNDICE DE ILUSTRACIONES

IMAGEN 1. CRIPTOGRAFÍA	15
IMAGEN 2. CONTROL DE ACCESO	16
IMAGEN 3. PROTECCIÓN CONTRA ATAQUES	17
IMAGEN 4. SEGURIDAD EN REDES INALÁMBRICAS	17
IMAGEN 5. SEGURIDAD EN DISPOSITIVOS DE RED	19
IMAGEN 6. COMPONENTES DE CABLEADO	21
IMAGEN 7. DISEÑO DE INFRAESTRUCTURA	22
IMAGEN 8. CONECTORES Y TERMINACIONES	23
IMAGEN 9. SISTEMAS DE CABLEADO	24
IMAGEN 10. METODOLOGÍA DE DESARROLLO	26
IMAGEN 11. METODOLOGÍA CASCADA	49
IMAGEN 12. DISEÑO DE LA RED	51
IMAGEN 13. CROQUIS DE LA JUNTA CANTONAL	53
IMAGEN 14. SITIO QUE NOS SERVIRÁ COMO DATA CENTER	54
<b>IMAGEN 15. CÁMARA 1 - PATIO DE LA INSTITUCIÓN</b>	<b>55</b>
<b>IMAGEN 16. CÁMARA 2 - OFICINAS ATENCIÓN CIUDADANA</b>	<b>55</b>
IMAGEN 17. CÁMARA 3 - INGRESO PRINCIPAL	56
IMAGEN 18. CÁMARA 4 - DATA CENTER	56
IMAGEN 19. DVR DE CÁMARAS	56
IMAGEN 20. ASIGNACIÓN DE IP A DVR	57
IMAGEN 21. EQUIPOS DE JEFATURA Y ASISTENTE	58
IMAGEN 22. EQUIPO ATENCIÓN A CIUDADANO	58
IMAGEN 23. EQUIPO DE RECEPCIÓN	58
IMAGEN 24. RELOJ BIOMÉTRICO	58
IMAGEN 25. PONCHADO DE CABLE UTP	60
IMAGEN 26. CABLE PONCHADO	60
IMAGEN 27. CREACIÓN DE REGLA DE INGRESO DE CADA EQUIPO	60
IMAGEN 28. REGLAS DE FIREWALL	61
IMAGEN 29. COMANDO PING	62
IMAGEN 30. COMPROBACIÓN EXITOSA	63
IMAGEN 31. COMANDO TRACERT	63
IMAGEN 32. CONSOLA TERMINAL DE WINBOX	64

IMAGEN 33. VERIFICACIÓN DE VIDEO DE CÁMARAS _____	65
IMAGEN 34. PRUEBAS DE GRABACIONES DE CÁMARAS _____	65
IMAGEN 35. EQUIPOS DE JEFATURA Y ASISTENTE _____	86
IMAGEN 36. EQUIPO ATENCIÓN A CIUDADANO _____	86
IMAGEN 37. EQUIPO DE RECEPCIÓN _____	86
IMAGEN 38. RELOJ BIOMÉTRICO _____	86
IMAGEN 39. ENTREVISTA AL ING. JAVIER ZAMBRANO, ENCARGADO DE STIC GAD _____	87
IMAGEN 40. ENCUESTA A JEFA DEL SISTEMA CANTONAL _____	87
IMAGEN 41. ENCUESTA AL PERSONAL DEL SISTEMA CANTONAL _____	88
IMAGEN 42. LEVANTAMIENTO DE FICHAS DE OBSERVACIÓN CON EQUIPOS DE RED _____	88

## ÍNDICE DE ANEXOS

ANEXO A: ASIGNACIÓN DE TUTOR.....	82
ANEXO B: CERTIFICADO DE LA EMPRESA.....	83
ANEXO D: REPORTE DEL SISTEMA ANTIPLAGIO .....	84
ANEXO E: FOTOGRAFÍAS .....	86
ANEXO F: FOTOGRAFÍAS DE EVIDENCIA DE APLICACIÓN DE ENCUESTAS Y ENTREVISTA .....	87

## **RESUMEN**

Este proyecto aborda la implementación de un Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen. El proyecto busca mejorar la eficiencia operativa y la seguridad de la información y de las instalaciones mediante la adopción de tecnologías avanzadas y prácticas seguras de TI. Se propone un enfoque mixto de investigación, utilizando métodos cualitativos y cuantitativos para evaluar tanto las percepciones de los usuarios como el rendimiento técnico del sistema de red. Además, se describe una estrategia de implementación que incluye la adquisición y configuración de equipos, la capacitación del personal y la creación de políticas de seguridad. La integración de un sistema de video vigilancia con la red de datos refuerza la capacidad de respuesta ante incidentes y la protección de los activos de la institución.

## **ABSTRACT**

This project addresses the implementation of a Network Security System Installation with structured cabling based on the TIA/EIA 568 standard for the Cantonal System of Equality and Comprehensive Protection of Rights of the Priority Attention groups of the Canton of El Carmen. The project seeks to improve operational efficiency and information and facility security through the adoption of advanced technologies and secure IT practices. A mixed approach to research is proposed, using qualitative and quantitative methods to assess both user perceptions and the technical performance of the network system. In addition, an implementation strategy is described that includes the acquisition and configuration of equipment, the training of personnel, and the creation of security policies. The integration of a video surveillance system with the data network strengthens the capacity to respond to incidents and the protection of the institution's assets.

# CAPÍTULO I

## 1 INTRODUCCIÓN

### 1.1 Introducción

El presente documento tiene consigo el proyecto final de la carrera de Ingeniería de Tecnología de la Información, y la misma consiste en la Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen (Junta Cantonal), ubicado en la Av. 3 de Julio diagonal a la Escuela Dr. Luis Aveiga Barberán, en el periodo 2023.

La solución consiste en la provisión de un sistema de seguridad, que tendrá consigo cámaras de circuito cerrado con el fin de salvaguardar la integridad de cada uno de los usuarios tanto internos como externos, así como también la integridad de los bienes muebles y tecnológicos que reposan en la Unidad Adscripta del GAD Municipal del Cantón El Carmen.

De igual forma se establecerá una RED de Datos certificada, la misma que brindará un servicio de alta disponibilidad del 99%, garantizando un óptimo funcionamiento de los servicios tanto de datos como de video, manteniendo una conexión permanente al Internet aprovechando la velocidad máxima contratada por la entidad.

El presente trabajo está dividido en seis capítulos, en el primero se indica la problematización del tema en estudio, con su árbol de problema y demás temas que involucran este contexto; en el capítulo dos, se encuentra todo lo que soporta la investigación de manera teórica con distintos autores que han realizado estudios sobre las variables que se usan para este proyecto; en el capítulo número tres se encuentra el marco metodológico, todo lo relacionado con la investigación en cuanto a métodos y herramientas usada para éste propósito; en el capítulo cuatro se encuentra la propuesta la misma que fue aplicada para tratar de resolver el problema investigado; el capítulo cinco brinda un análisis de resultados los cuáles fueron obtenidos con base a herramientas de investigación y por último el capítulo seis nos muestra las experiencias del trabajo presentado en las conclusiones y recomendaciones del mismo.

## **1.2 Presentación del tema**

Una vez identificada la necesidad de la Junta Cantonal, se procederá a la instalación de un sistema de seguridad diseñado para proteger la integridad de los usuarios, los bienes y los datos. Este sistema incluirá un cableado de red LAN interna que cumpla con las normas TIA/EIA 568 -B, permitiendo la integración de cámaras de seguridad y equipos informáticos. Al finalizar, se establecerá una conexión directa con el edificio principal del GAD Municipal de El Carmen, que será responsable del monitoreo del sistema de seguridad y de cada uno de los componentes de la red de datos implementada.

Una vez instalado el sistema de seguridad, se procederá en cada uno de los puntos tanto de las cámaras y de los equipos informáticos, con la marcación de todos los elementos que contenga el cableado estructurado, cables, paneles, canaletas, rack, cajetín, tal como lo indica el estándar ya mencionado con el fin de facilitar la administración del Sistema por parte de la Unidad de Servicios Tecnológicos del GAD Municipal El Carmen.

## **1.3 Ubicación y contextualización de la problemática**

Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen (Junta Cantonal), es el conjunto articulado y coordinado de sistemas, instituciones, políticas, normas, programas y servicios que aseguran el ejercicio, garantía y exigibilidad de los derechos reconocidos en la constitución, los instrumentos internacionales y el cumplimiento de los objetivos del régimen de desarrollo; será parte del Sistema Nacional de Inclusión y Equidad Social y de los Sistemas especializados y se regirá por sus mismos principios y ámbitos. Sus objetivos ante la ciudadanía son los siguientes:

- ✓ Asegurar el ejercicio, garantía y exigibilidad de los derechos consagrados en la Constitución, en las leyes y en los instrumentos internacionales.
- ✓ Promover la articulación, coordinación y corresponsabilidad entre las entidades que conforman el Sistema Nacional de Inclusión y equidad social y sus sistemas especializados y la sociedad; y,
- ✓ Generar espacios para la participación de los grupos de atención prioritaria y sociedad civil dentro del Sistema Cantonal de igualdad y Protección Integral de los grupos de atención prioritaria, conforme lo establece la ley de participación ciudadana y control social, para el cumplimiento de la ordenanza municipal.

Actualmente se encuentra ubicado en la Av. 3 de Julio diagonal a la escuela Dr. Luis Aveiga Barberán, en el antes denominado asilo de ancianos. Cuenta con 5 oficinas para la atención a la ciudadanía, las mismas que no cuentan con una red de datos estructurada y tampoco un sistema de video vigilancia adecuado para salvaguardar la integridad de los bienes, del personal que labora en el sitio y de la ciudadanía en general que frecuenta el lugar.

## **1.4 Planteamiento del problema**

La Junta Cantonal, ha decidido solicitar la instalación de una solución integral para la Seguridad de sus bienes materiales y tecnológicos. Este sistema incluirá un circuito cerrado de cámaras inteligentes equipadas con tecnología de detección de movimiento, reconocimiento facial, modo infrarrojo y visión nocturna. Las cámaras serán instaladas conforme a la norma TIE/EIA 568, con todos los puntos de conexión certificados de extremo a extremo.

De igual forma poder contar con alta disponibilidad de toda la red de datos y el acceso a Internet con un cableado estructurado y certificado con la norma TIE/EIA 568, la misma que facilite la conexión directa entre los equipos tecnológicos y el enlace de datos desde la unidad hasta el edificio principal del GAD Municipal del Cantón El Carmen.

### **1.4.1 Problematización**

La Junta Cantonal cuenta con una red de datos, que conecta un router, instalado por el proveedor de internet, a cada uno de los equipos informáticos de la institución mediante cables UTP algunos de Cat. 5 y otros de Cat. 6. Según Han (2016), la organización y estructuración adecuada de datos son esenciales para una minería de datos efectiva, ya que los datos bien estructurados facilitan el análisis y la extracción de información significativa.

Cabe resaltar que toda infraestructura tecnológica, tiene que ser administrada de manera correcta según la norma de red establecida para el efecto, es decir, se debe de gestionar cada uno de los dispositivos de la red, mantener una firme seguridad en la red priorizando cada uno de los paquetes tanto de subida como de bajada, como también categorizando los debidos perfiles de acceso, reduciendo en su totalidad los riesgos a los que se expone cada uno de los

usuarios con el uso del internet sin la seguridad adecuada, así como de la interconexión de los diferentes segmentos de red con los que se cuenta la institución.

Al final, se observa que no existe una administración adecuada ni se cuenta con principios básicos de diseño de red en la conexión de los equipos de la institución. A pesar de que los diferentes departamentos están interconectados, la red presenta una ausencia de normas y estándares de calidad en la gestión del tráfico de toda la LAN., Tanenbaum (2012) discute cómo una arquitectura de red inadecuada puede resultar en ineficiencia en el enrutamiento, congestión, pérdida de paquetes y tiempos de respuesta más lentos, lo que impacta negativamente en el rendimiento y la fiabilidad de la red. Además, es evidente que no hay una segmentación clara de las direcciones IP, ya que estas se asignan de manera aleatoria y se obtienen del router instalado por el proveedor del servicio de internet. Esto significa que ni siquiera existe un segmento de IP establecido por el edificio principal del GAD, lo cual impide asignar un ancho de banda adecuado para el trabajo que se realiza, causando congestión en horas pico y volviendo los servicios lentos e inaccesibles.

#### **1.4.2 Génesis del problema**

En 2021, la máxima autoridad del GAD Municipal del Cantón El Carmen decidió trasladar a los funcionarios del Concejo Cantonal de la Niñez al edificio ubicado en la Av. 3 de Julio, diagonal a la Escuela Dr. Luis Aveiga Barberán, que anteriormente se utilizaba como asilo de ancianos. Una vez ubicados en este edificio, se contrató un enlace de internet y se dejó un router básico para la conexión de los equipos tecnológicos necesarios para el trabajo diario.

Ese mismo año, debido a la falta de seguridad en el lugar, comenzaron a ocurrir robos de bienes materiales, incluidos equipos tecnológicos y pertenencias personales de los empleados. Los robos se producían tanto durante el día como en la noche, ya que no había un control adecuado de las personas que ingresaban al sitio.

Además, la falta de un equipo administrable para la red de datos y el acceso a internet ha generado inconvenientes entre los funcionarios que laboran en el lugar. El router básico instalado no gestiona el ancho de banda contratado de manera efectiva, lo que resulta en que algunos equipos tengan acceso a internet mientras que otros no. Asimismo, la ausencia de

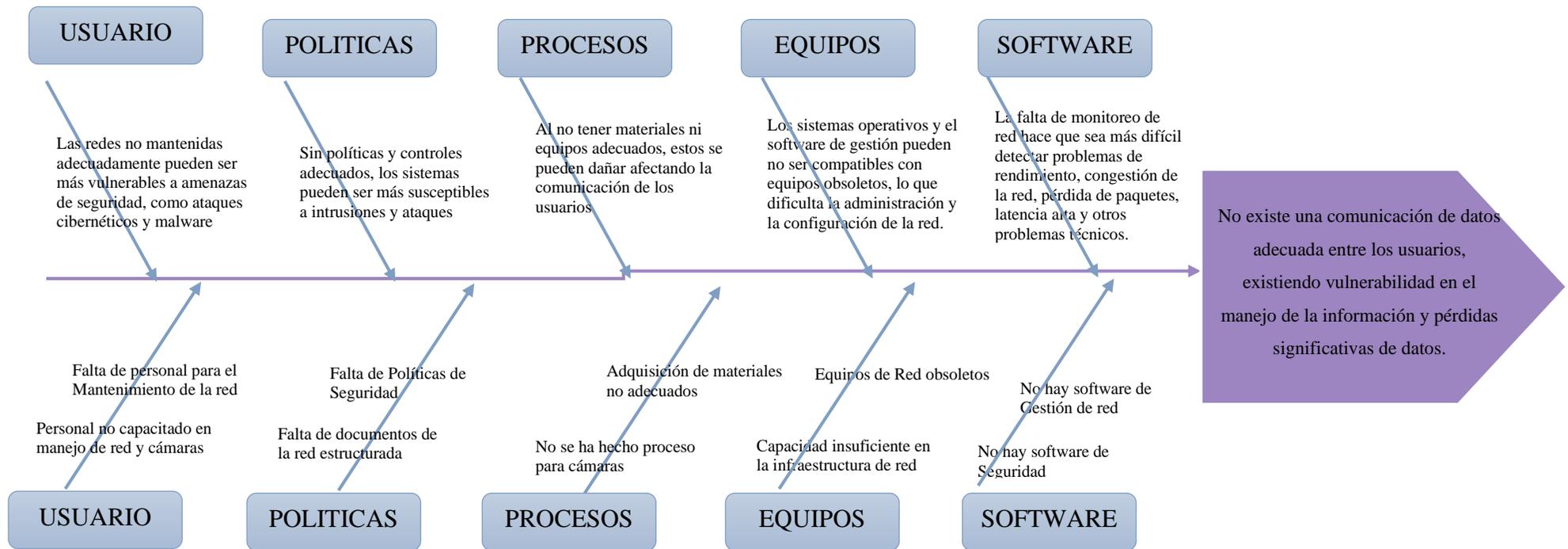
certificación y documentación de los cables instalados impide un control adecuado sobre los mismos.

### **1.4.3 Estado actual del problema**

Actualmente, el Sistema Cantonal de Igualdad y Protección Integral de los Derechos de los Grupos de Atención Prioritaria del Cantón El Carmen no cuenta con un sistema de seguridad en el lugar donde se encuentran laborando, tanto en la parte externa como interna del mismo. Asimismo, no dispone de una red estructurada para los equipos tecnológicos que utilizan en sus labores, lo que provoca un uso ineficiente de los recursos tecnológicos, como la red de datos local y el internet. La ausencia de un sistema de vigilancia ha resultado en varias pérdidas, incluyendo robos de equipos, documentos, bienes materiales y dinero. Esta falta de seguridad ha generado un ambiente de desconfianza e intranquilidad entre las personas que laboran en la institución, quienes no se sienten seguras dejando objetos de valor en las oficinas por temor a posibles robos.

Debido a estos antecedentes, es urgente la necesidad de instalar cámaras de seguridad, cámaras IP, y un cableado estructurado y documentado bajo la norma TIA/EIA 568. Además, se requiere una red LAN para los equipos de cómputo en el área, con el fin de mejorar la distribución de la red de datos y asegurar un uso adecuado del internet.

### **1.5 Diagrama causa – efecto del problema**



## **1.6 Objetivos**

### **1.6.1 Objetivo general**

Implementar un Sistema de Seguridad de redes con cableado estructurado, basado en la Norma TIA/EIA 568-B, para el Sistema Cantonal de Igualdad y Protección Integral de los derechos de los grupos de atención prioritaria del Cantón El Carmen, con el fin de poder obtener una solución integral en la infraestructura de red de la institución, el mismo que permita disponer de ambientes adecuados para los usuarios.

### **1.6.2 Objetivos específicos**

- ✓ Examinar las bases teóricas que respaldan el proyecto del sistema de seguridad de red con cableado estructurado, así como los aspectos claves, tales como estándares, vinculación con el proveedor de servicios de internet, conexión equipos de red y cámaras, características técnicas de los dispositivos, etc.
- ✓ Realizar un diagnóstico de la situación actual de la Junta Cantonal, en cuanto a la seguridad de la información, de cada uno de sus bienes, sus usuarios y de la ciudadanía en general.
- ✓ Diseñar un sistema de seguridad que permita salvaguardar la integridad de las personas que laboran en el sitio, de la información que se guarda a diario, de los bienes propios e institucionales y de la ciudadanía en general.
- ✓ Implementar el sistema de seguridad y analizar cada uno de sus beneficios a favor del GAD Municipal El Carmen y de la ciudadanía en General.

## **1.7 Justificación**

Una vez identificada la necesidad del Sistema Cantonal de Igualdad y Protección de Integral de los derechos de los grupos de atención prioritaria del Cantón El Carmen, se procederá con la instalación de un Sistema de Seguridad, el cual servirá como una solución para salvaguardar la integridad de los usuarios, bienes y los datos. Este sistema incluirá un cableado de red LAN interna para el uso de cámaras de seguridad y equipos informáticos, permitiendo una conexión directa al edificio principal del GAD Municipal de El Carmen.

Se definirá un cableado estructurado utilizando cables UTP de categoría 6A, con todos los puntos certificados y documentados. Tras la instalación y puesta en funcionamiento del cableado estructurado, se garantizará el cumplimiento de la norma TIA/EIA 568.

Se implementará un cableado horizontal desde el área de trabajo hasta el cuarto donde se instalará el rack, utilizando cables UTP (Unshielded Twisted Pair) de cobre con par trenzado de 100 Ohms, que cumplan con todos los parámetros de transmisión y comunicación establecido en la Norma TIA/EIA 568. Esto evitará interferencias y mejorará los resultados, especialmente en largas distancias o en entornos con ruido electromagnético.

Una vez completado el cableado en cada uno de los puntos, tanto para las cámaras como para los equipos informáticos, se procederá a marcar todos los elementos del cableado estructurado, incluyendo cables, paneles, canaletas, racks y cajetines, tal como lo indica la norma mencionada. Esto facilitará la administración del sistema por parte de la Unidad de Servicios Tecnológicos del GAD Municipal de El Carmen.

Este proyecto busca realizar un análisis exhaustivo y minucioso de toda la infraestructura integral de telecomunicaciones de la Junta Cantonal. La solución concebida en esta situación específica contribuirá al progreso de esta Institución. Así mismo, permitirá cumplir con la misión y visión establecida por la facultad de Tecnologías de la Información, lo que facilitará la obtención de mi título académico.

## **1.8 Impactos esperados**

Las cámaras de seguridad a nivel de empresas e instituciones actualmente tienen un impacto positivo ante la ciudadanía en general, ya que en su mayoría al ver estos equipos tecnológicos se sienten protegidos y seguros en el sitio en el cual se encuentran. Por otro lado, al tener una red estructurada se mantiene la seguridad ante ataques tanto internos como externos, y no está de más indicar que el flujo de información entre los equipos que se encuentran en la misma, será de manera organizada y bien distribuida.

### **1.8.1 Impacto tecnológico**

Kurose (2016) manifiesta que las redes inalámbricas y móviles han revolucionado la telefonía y están teniendo un impacto cada vez más profundo también en el mundo de las redes de computadoras. Con su acceso no restringido, en cualquier momento y en cualquier lugar, a la infraestructura global de red, no sólo están haciendo que el acceso de red sea más ubicuo, sino que también permiten un conjunto muy excitante de nuevos servicios dependientes de la ubicación.

Actualmente las Empresas Privadas e Instituciones Gubernamentales hacen uso de las cámaras de vigilancia y de Sistemas de Seguridad para el monitoreo frecuente de cada una de sus instalaciones, salvaguardando la integridad de cada uno de sus bienes tanto materiales como también la integridad de las personas que laboran en el sitio. Con esta tecnología moderna de los dispositivos de seguridad, la misma que permite identificar el rostro de cada una de las personas, se podrá dar con la identidad inmediata de las personas que cometieran algún delito dentro de la institución. En conclusión, se tiene un impacto tecnológico positivo al precautelar la integridad de cada una de las personas y los bienes que se encuentran en el edificio.

### **1.8.2 Impacto social**

La Instalación de un Sistema de Seguridad con cableado estructurado, basado en la Norma TIA/EIA 568-B, para el Sistema Cantonal de Igualdad y Protección de Integral de los derechos de los grupos de atención prioritaria del Cantón El Carmen, es netamente social, ya que la misma no será utilizada con fines de lucro, caso contrario la misma será utilizada para fortalecer la seguridad del personal que labora en el sitio, como la de las personas que visitan el lugar, considerando que estamos en una época donde el auge delincuencial se viene incrementando. En conclusión, al obtener el edificio un sistema de seguridad con las cámaras de vigilancia, la entidad podrá actuar de forma inmediata ante cualquier suceso que se suscite en el lugar en conjunto y de manera coordinada con las autoridades municipales y cantonales en favor de la ciudadanía.

Tal como indica Amo (2013), que la construcción de la sociedad de la información ha dado lugar a varias interpretaciones, desde la más optimista que plantea que las TIC representan el

progreso absoluto y el remedio para resolver cualquier crisis social o económica (ciberoptimistas o tecnófilos), pasando por las más pesimistas que concluyen que las nuevas tecnologías no tienen suficiente poder transformador (ciberpesimistas o tecnófobos) y que producen más trabas que beneficios, hasta posiciones intermedias que entienden que la tecnología es un instrumento más y que el cambio siempre es promovido por el hombre quien, a su vez, impulsa una u otra tecnología en función de las objetivos que espere conseguir.

### **1.8.3 Impacto ecológico**

Para la ejecución de este proyecto en el Sistema Cantonal de Igualdad y Protección de Integral de los derechos de los grupos de atención prioritaria del Cantón El Carmen, se utilizará equipos y materiales de libre venta en el mercado nacional, igualmente se tomará en cuenta que los mismos estén regulados con las normas vigentes de tecnología. La empresa que proveerá los productos aparte de emitir un certificado de garantía, emitirá un certificado que los mismos cumplen con las normas de calidad INEN y de licencia ambiental. Tal como lo mencionó (FEA, Rizzo, 2021) en el foro económico de economías ágiles celebrado en México “La aceleración digital continuará y para mantenernos vigentes en cualquier industria y sector, es importante actualizarnos y tener una apertura al cambio informados y preparados, no sólo en temas tecnológicos, sino también en asuntos medioambientales; es importante asegurarnos de que cada cambio aplicado logre también un impacto positivo en el medio ambiente”

## CAPÍTULO II

### 2 MARCO TEÓRICO

#### 2.1 Antecedentes históricos

Si bien es cierto en los últimos años, ha habido un avance notable en el desarrollo de las redes tecnológicas, transformando significativamente el intercambio y la transmisión de datos, así como la comunicación entre las personas. Anteriormente, la comunicación humana se basaba en cartas y pergaminos, métodos que a menudo implicaban largos periodos de espera de días o incluso meses para llegar a su destino. Con el tiempo, esta dinámica evolucionó con la aparición de inventos que revolucionaron la comunicación, como el telégrafo, el teléfono, la radio y la televisión. Sin embargo, el descubrimiento de las redes de datos conectando equipos informáticos supuso un cambio drástico, mejorando notablemente la transmisión y la comunicación entre distintos lugares.

Hinojosa (2010), reconoce que en la última década ha habido un progreso significativo, principalmente debido al surgimiento de enfoques innovadores en la administración de servicios informáticos. Este avance se ha vinculado con la introducción de nuevos productos y tecnologías, así como con las oportunidades que la informática y las redes ofrecen a la comunidad, a las empresas y a las instituciones en su conjunto.

Una red de datos proporciona a cada uno de los usuarios de la misma a estar conectados, y a poder comunicarse ilimitadamente en el momento que lo crea conveniente, además nos permite realizar intercambio de información, hacer uso de programas de manera simultánea, subir o bajar información de cualquier parte del mundo. Así mismo un Circuito cerrado de televisión con cámaras en la actualidad nos permite tener un control en vivo de los usuarios y los bienes de una institución. Además, nos permite revisar de forma exacta lo ocurrido minutos u horas antes de un evento en particular, pudiendo detectar a cada una de las personas que están en el sitio.

Según Alegsa (2015), una red de computadoras implica la conexión entre distintas computadoras con el fin de compartir información, recursos y servicios. Esta conexión puede establecerse mediante vínculos físicos (cableados) o de manera inalámbrica. Algunos

especialistas señalan que una red de computadoras genuina involucra la interconexión de tres o más dispositivos o computadoras.

Sin duda, esto mejora notablemente la comunicación entre las instituciones, algo que es crucial en la actualidad para las labores que se desarrollan en ellas. Asimismo, incrementa la seguridad de cada dispositivo y de los bienes que poseen, lo cual es fundamental para el desarrollo de sus actividades

## **2.2 Antecedentes de investigaciones relacionadas al tema presentado**

### **2.2.1. Propuesta de Red de Datos para la Gestión de los servicios de red en el campus politécnico de la ESPAM MFL.**

El proyecto de tesis de la ESPAM MFL se centra en mejorar la gestión de la red LAN de la institución. Se propone un diseño para controlar y dirigir el tráfico de la red, basado en la metodología PPDIOO. Esto busca resolver problemas de disponibilidad debido a interrupciones frecuentes del servicio de internet en momentos de alta demanda. El enfoque se basa en determinar velocidades óptimas, estimar el tráfico máximo y crear VLAN para cada área académica, asegurando así un uso eficiente de los recursos de red para satisfacer las necesidades de los usuarios conectados.

El proyecto que estoy realizando se centra específicamente en cambiar la Red de Datos Básica que se encuentra en la Junta Cantonal, por una Red de Datos estructurada, para que en la misma se pueda llevar un control de cada uno de los dispositivos que se conecten en el sitio y a mejorar la seguridad de los datos con reglas que eviten ataques externos como internos, además, aprovechando la estructura de la red se prevé instalar un circuito cerrado con cámaras de video vigilancia, con el fin de salvaguardar de igual forma los bienes informáticos y la integridad de las personas que frecuentan el sitio.

### **2.2.2. Diseño de una red integral de Telecomunicaciones según las Normas ANSI TIA/EIA 568 C, 569 C, 606 B, 607 B, para el Instituto Técnico Tecnológico Superior “COTACACHI” (ITTS).**

El proyecto de titulación implica el diseño de una red completa de telecomunicaciones para el Instituto Técnico Tecnológico Superior "COTACACHI" (ITTS), actualmente en construcción. Este diseño unifica servicios como voz, datos, video, acceso y seguridad, siguiendo normativas específicas de diseño y regulaciones internas. Además, se detallan los materiales, cálculos, diagramas y costos asociados. Por otro lado, la institución tiene capacidad para 1920 estudiantes y se espera que esta mejora educativa contribuya al desarrollo de la provincia y ofrezca mayores oportunidades laborales y de emprendimiento.

El proyecto que se está realizando para la Junta Cantonal, al igual que el proyecto antes mencionado se basa en las normas internacionales ANSI/TIA/EIA 568, y se enfoca de igual forma al unificar los servicios de datos, video y seguridad cumpliendo con las normativas de diseño y regulaciones internas. (Morales, 2014) Indica que un diseño de instalación de cableado puede ser complicado y desafiante. Como cada vez son más los servicios que comparten la red de cables común, como el control de temperatura de un edificio, la seguridad, los sensores contra incendios y la vigilancia, los estándares se vuelven cada vez más críticos porque los diseñadores de estas otras industrias tienen una idea fija sobre cómo hacer que su equipo trabaje en la red común.

### **2.2.3. Implementación de una red LAN con la utilización de cableado estructurado basado en las normas internacionales ANSI /TIA /EIA 568-B, en el Laboratorio de Investigación de Ingeniería de Software en la Universidad Técnica De Cotopaxi, Extensión La Maná, en el año 2017.**

El proyecto busca implementar una red LAN con cableado estructurado según estándares internacionales para el Laboratorio de Investigación de Ingeniería de Software de la Universidad Técnica de Cotopaxi, Extensión la Maná. Se realizó un estudio técnico para identificar los recursos necesarios y se investigaron los beneficios de esta implementación para optimizar la transmisión de datos. El objetivo es proporcionar herramientas tecnológicas adecuadas para los estudiantes de Ingeniería en Informática y Sistemas Computacionales y mejorar la eficiencia y competitividad de la institución.

El proyecto citado al igual que este proyecto realizará los estudios técnicos necesarios para la identificación de los recursos de la Junta Cantonal, de igual forma se procederá a la investigación de cada uno de los beneficios que brindará el Sistema de Seguridad,

optimizando cada uno de los recursos, información y el salvaguardo de los bienes tanto públicos como privados que reposan en el mismo, con herramientas tecnológicas actualizadas para la atención al ciudadano el Cantón El Carmen.

## **2.3 Definiciones conceptuales**

### **2.3.1 Seguridad de Redes**

#### **2.3.1.1 Fundamentos de Seguridad de Redes**

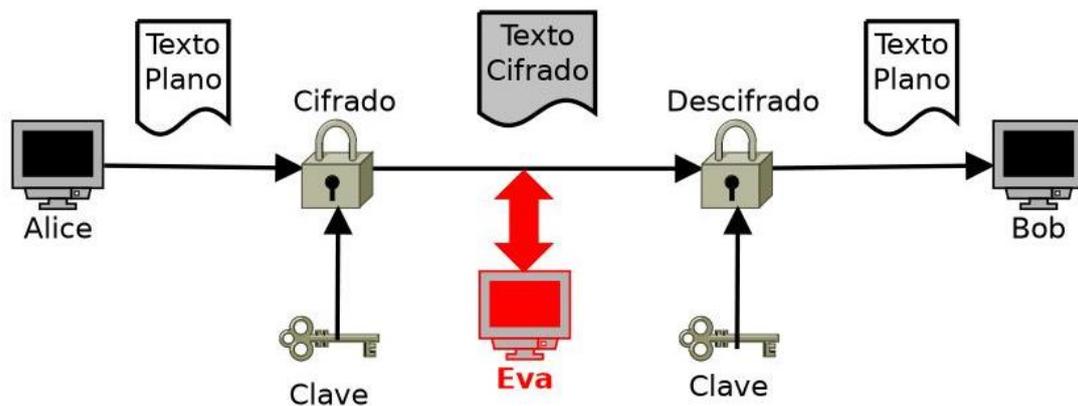
Briceño (2021) manifiesta que la seguridad de la información es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad híper conectada, en gran parte como resultado de nuestra adopción casi ubicua de la tecnología de información y comunicación. En nuestra vida cotidiana, muchos de nosotros trabajamos con computadoras para nuestros empleadores, jugamos en casa, en la escuela, en línea, revisamos el correo en distintos lugares, vemos nuestras cuentas bancarias, en fin, con muchos aspectos de nuestra vida cotidiana.

En otras palabras, la seguridad informática se refiere a las medidas, estrategias y procedimientos diseñados para proteger los sistemas, redes y datos digitales contra accesos no autorizados, ataques, daños o cualquier otra amenaza que pueda comprometer su confidencialidad, integridad o disponibilidad. Esta disciplina abarca diversas áreas como la criptografía, la gestión de accesos, la detección de intrusiones, entre otros, con el objetivo de garantizar la protección de la información sensible y los recursos tecnológicos.

#### **2.3.1.2 Criptografía y Seguridad de la Información**

Ortiz (2018) explica que la Criptografía simétrica, se ha implementado en diferentes tipos de dispositivos, desde manuales, mecánicos y eléctricos, hasta computadoras, donde se programan los algoritmos actuales. La idea general es aplicar diferentes funciones al mensaje que se desea cifrar de tal manera que solo pueda descifrarse conociendo la clave. Aunque no existe un tipo de diseño estándar, uno de los más populares es el de Fiestel, que realiza un número finito de interacciones de una manera particular, hasta que el mensaje es cifrado.

Por otro lado, la Criptografía de clave pública o asimétrica, también denominada RSA por las siglas de los apellidos de sus inventores Rivest Shamir y Adelman, se define por el uso de dos claves diferentes para cada usuario, una clave pública para cifrar y una clave privada para descifrar.



*Imagen 1. Criptografía*

*Fuente: Google Imágenes*

La criptografía simétrica es un enfoque donde se emplea una misma clave para cifrar y descifrar la información, utilizando esa clave compartida entre las partes para codificar y decodificar los datos. Algoritmos comunes en esta categoría son DES (Estándar de Cifrado de Datos) y AES (Estándar de Encriptación Avanzada). Por otro lado, la criptografía asimétrica, también llamada criptografía de clave pública, utiliza dos claves diferentes pero relacionadas matemáticamente: una clave pública que se comparte ampliamente para cifrar datos, y una clave privada que se mantiene en secreto y se emplea para descifrarlos. Este método se encuentra en protocolos de seguridad como RSA (Rivest-Shamir-Adleman) y ECC (Criptografía de Curva Elíptica).

### **2.3.1.3 Autenticación y Control de Acceso**

Ángel (2017) afirma que la mayoría de los protocolos basados en passwords en uso hoy en día dependen de lo complicada que sea la password que utilice el usuario. El Servidor provee de intentos de validación hacia el usuario solicitando una password que el cliente envía al servidor, validando éste la respuesta por parte del usuario contra dicha password que se

encuentra en una base de datos. Esta aproximación de carácter general se describe en CHAP, MS-CHAP, MS-CHAP-V2, EAP/MD5-Challenge y en EAP/One Time Password.



*Imagen 2. Control de Acceso*

*Fuente: Google Imágenes*

Autenticación es el proceso de verificar la identidad de un usuario o sistema, generalmente mediante credenciales como contraseñas, huellas dactilares, certificados digitales, tarjetas inteligentes u otros métodos biométricos. Su objetivo es asegurar que el usuario o sistema sea quien dice ser antes de otorgar acceso a recursos protegidos. Por otro lado, el Control de Acceso se refiere al conjunto de prácticas, políticas y tecnologías utilizadas para regular y gestionar quién tiene permiso para acceder a determinados recursos, sistemas o áreas protegidas. El control de acceso puede basarse en roles, privilegios, niveles de seguridad, entre otros mecanismos, para garantizar la protección de datos y la seguridad de sistemas.

#### **2.3.1.4 Protección Contra Ataques y Amenazas.**

Darío (2023) afirma que es fundamental que las empresas y los usuarios adopten medidas para protegerse de estas amenazas y vulnerabilidades. Algunas medidas de protección incluyen la implementación de programas antivirus, la educación de los usuarios sobre las prácticas de seguridad informática, el uso de contraseñas seguras y la actualización regular del software y hardware. Además, es importante contar con un plan de contingencia en caso de que se produzca una violación de seguridad.



*Imagen 3. Protección Contra Ataques*

*Fuente: Google Imágenes*

La protección ante ataques y amenazas abarca las estrategias, métodos y herramientas utilizadas para resguardar sistemas, datos, redes y dispositivos frente a posibles intrusiones, acciones maliciosas o riesgos para la seguridad. Este enfoque involucra el establecimiento de defensas de seguridad, sistemas de detección, protocolos de prevención, actualizaciones de software, autenticación sólida, y técnicas de encriptación, entre otras medidas, con el fin de identificar, prevenir, responder y reducir el impacto de cualquier actividad dañina que pueda comprometer la integridad, confidencialidad o disponibilidad de la información.

#### **2.3.1.5 Seguridad en Redes Inalámbricas**

Darío (2023) resalta que la seguridad de las redes inalámbricas, es un aspecto fundamental de la seguridad informática, ya que estas redes son susceptibles a una amplia gama de ataques, y se deben implementar medidas de seguridad adecuadas para prevenir los riesgos de acceso no autorizado, interceptación de datos, ataques DoS y ataques de fuerza bruta.



*Imagen 4. Seguridad en Redes Inalámbricas*

*Fuente: Google Imágenes*

La seguridad en redes inalámbricas comprende las medidas y estrategias aplicadas para resguardar la confidencialidad, integridad y disponibilidad de los datos que circulan en entornos de conectividad sin cables. Esto implica proteger contra accesos no autorizados, cifrar la información transmitida, autenticar dispositivos y usuarios, así como prevenir intrusiones y ataques maliciosos en redes que funcionan de manera inalámbrica. El propósito central es garantizar la privacidad y protección de los datos compartidos en este tipo de entornos de red.

### **2.3.1.6 Seguridad en Aplicaciones y Protocolos de Red**

Tanenbaum (2012) indica que la interconexión de redes ha tenido mucho éxito en la creación de redes extensas, pero sólo funciona cuando hay una capa de red común. De hecho, con el tiempo han surgido varios protocolos de red. Es difícil lograr que todos estén de acuerdo en cuanto a un solo formato cuando las empresas perciben como ventaja comercial el tener un formato propietario que puedan controlar. Algunos ejemplos además de IP, que ahora es el protocolo de red casi universal, son: IPX, SNA y AppleTalk. Ninguno de estos protocolos se utiliza mucho en la actualidad, pero siempre habrá otros protocolos. Probablemente ahora el ejemplo más relevante sea el de IPv4 e IPv6. Aunque ambas son versiones de IP, no son compatibles (o no hubiera sido necesario crear IPv6).

La seguridad en aplicaciones y protocolos de red abarca las medidas y prácticas adoptadas para resguardar la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de aplicaciones y los protocolos utilizados en redes informáticas. Esto involucra el empleo de técnicas de cifrado, verificación de identidad de usuarios, control de acceso, detección y prevención de intrusiones, así como la aplicación de actualizaciones para reducir riesgos de vulnerabilidades. El objetivo central es asegurar que las aplicaciones y protocolos de red sean seguros y estén protegidos contra posibles amenazas y ataques maliciosos.

### **2.3.1.7 Seguridad en Dispositivos de Red**

Darío (2023) afirma que una de las ventajas de la red cableada es que, es relativamente difícil de hackear a distancia, pero esto no significa que esté completamente segura. Es importante asegurarse de que los cables estén instalados correctamente y que las conexiones estén



La gestión de incidentes abarca el proceso de manejar y responder de manera efectiva a eventos imprevistos que afectan la seguridad o integridad de los sistemas de una organización. Por otro lado, la continuidad del negocio se centra en las estrategias y procedimientos establecidos para mantener las operaciones esenciales de una empresa durante y después de incidentes, como ciberataques o desastres naturales, con el fin de minimizar su impacto y garantizar la pronta recuperación de las actividades críticas para el funcionamiento de la organización.

## **2.3.2 NORMA TIA/EIA 568.**

### **2.3.2.1 Introducción a TIA/EIA 568**

Morales (2014) manifiesta que la Asociación de Industrias Electrónicas (EIA, Electronic Industries Alliance) y la Asociación de la Industria de las Telecomunicaciones (TIA, Telecommunications Industry Association) son asociaciones de comercio que desarrollan y publican juntas una serie de estándares que abarcan el cableado estructurado de voz y datos para las LAN. Estos estándares de la industria evolucionaron después de la desregulación de la industria telefónica de los EE.UU. en 1984, que transfirió la responsabilidad del cableado de las instalaciones al dueño del edificio. Antes de eso, AT&T utilizaba cables y sistemas propietarios.

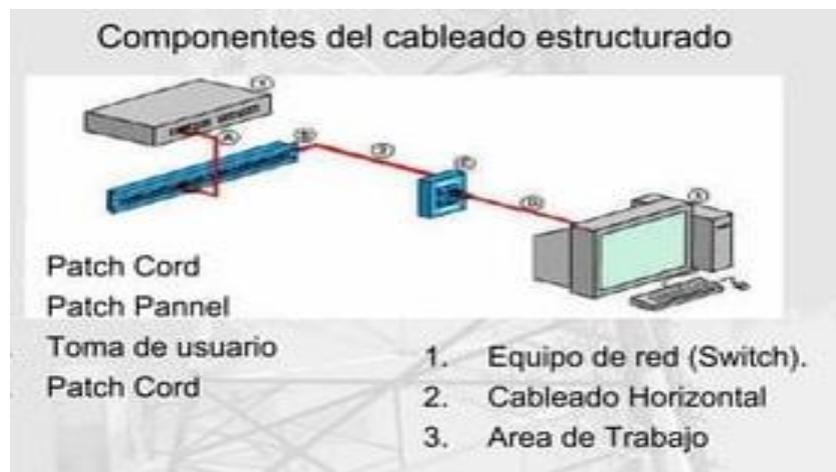
La norma TIA/EIA 568, desarrollada por la Telecommunications Industry Association (TIA) y la Electronic Industries Alliance (EIA), establece pautas para el cableado de telecomunicaciones en edificaciones comerciales. Define estándares para sistemas de cableado estructurado, asegurando una conectividad confiable y eficiente en redes de comunicación. Esta norma abarca categorías de cables, disposición de componentes y especificaciones de conexión para facilitar la implementación de redes de telecomunicaciones en diversos entornos comerciales.

### **2.3.2.2 Componentes de cableado**

Fernando Patricio (2021) indica que para instalar una red, se requiere el equipamiento esencial, como el medio de transmisión, el hardware y el software necesarios. Los componentes de red se dividen en dos categorías principales: activos y pasivos, los cuales facilitan la interconexión en una red. Los componentes pasivos, como cables, paneles y racks,

permiten la conexión entre equipos activos, posibilitando la integración de diversos servicios de comunicación. Además, para un funcionamiento óptimo de la red, se necesitan equipos específicos, como repetidores, hubs, bridges, switches y routers, cuya elección depende de las necesidades y características de la red.

Los componentes de cableado de la norma EIA/TIA 568 son elementos clave que cumplen con estándares específicos para sistemas de cableado estructurado. Estos componentes incluyen cables, conectores, paneles de conexión, tomas de pared, dispositivos de terminación y equipos de hardware necesarios para construir y mantener una infraestructura de red coherente y eficiente en entornos comerciales.



*Imagen 6. Componentes de Cableado*

*Fuente: Google Imágenes*

### **2.3.2.3 Diseño de infraestructura**

Comer (2015) El diseño de red se puede definir como el proceso de planificación y configuración de una estructura de red que permite la comunicación eficiente y segura entre dispositivos. No existe una definición específica de un autor en particular, ya que el diseño de red es un concepto ampliamente aceptado y aplicado en la informática y las telecomunicaciones.



*Imagen 7. Diseño de infraestructura*

*Fuente: Google Imágenes*

La norma EIA/TIA 568 establece lineamientos y estándares para la planificación de infraestructuras de cableado en ambientes comerciales. Este diseño incluye la organización física de cables, conectores, paneles y dispositivos de red, definiendo reglas específicas para sistemas de cableado estructurado. Ofrece directrices para la instalación, disposición y cuidado de estos sistemas, asegurando la calidad, la compatibilidad y el óptimo rendimiento de las redes de comunicación en edificaciones empresariales.

#### **2.3.2.4 Conectores y terminaciones**

Comer (2015) enfatiza que los conectores y terminales de red se representan por los componentes físicos usados en un sistema de cableado estructurado para conectar dispositivos y cables de red. Estos abarcan conectores, tomas, conectores hembra, y paneles de conexión, entre otros. Están desarrollados siguiendo estándares para asegurar conexiones estables y duraderas en las estructuras de red.



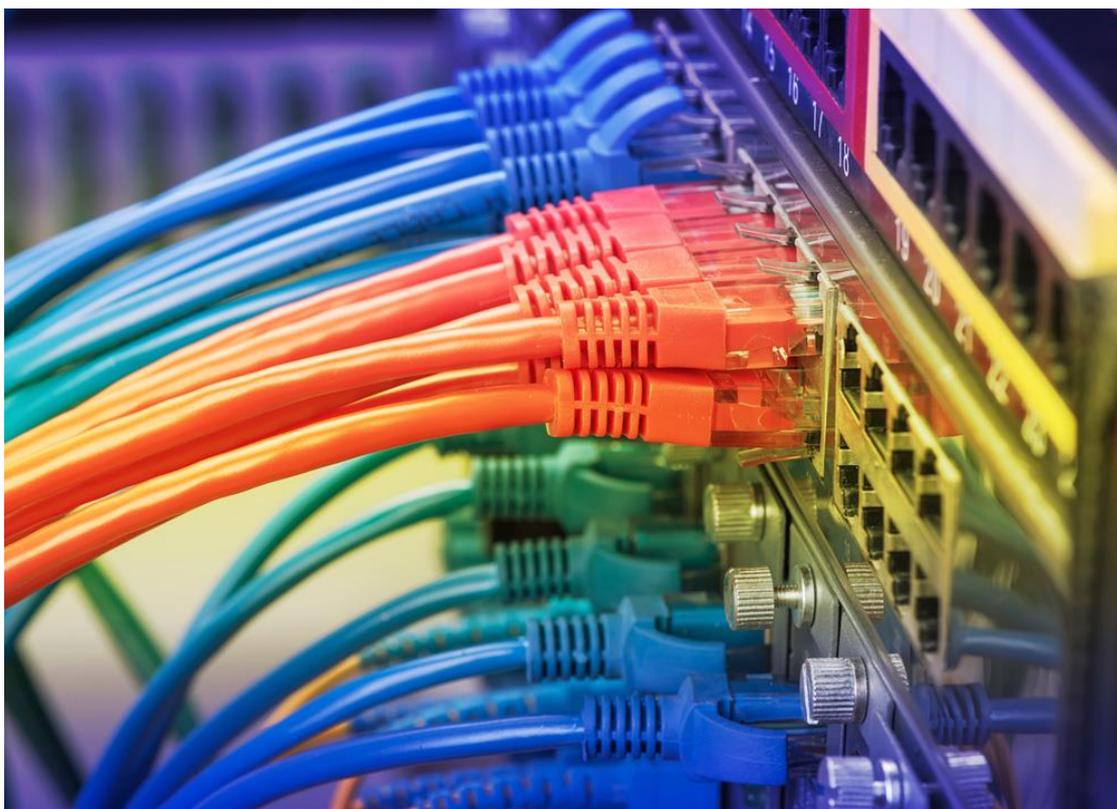
*Imagen 8. Conectores y Terminaciones*

*Fuente: Google Imágenes*

La norma EIA/TIA 568 establece los lineamientos para los conectores y terminaciones en sistemas de cableado estructurado, definiendo los componentes físicos como conectores, enchufes, jacks y paneles de conexión. Estos elementos se diseñan siguiendo estándares específicos para asegurar conexiones confiables y duraderas, facilitando la interconexión de cables y dispositivos de red con una integridad de señal óptima y compatibilidad entre equipos.

### **2.3.2.5 Sistemas de cableado**

Informática (2021) resalta en su artículo, que el cableado de red es la infraestructura necesaria para interconectar los equipos informáticos y permitir que la información fluya a través de la red. Los distintos tipos de cables se determinan según el tipo y tamaño de la red. Existen distintos tipos de cableado de red, como el cable de par trenzado sin apantallar (UTP), el cable de par trenzado apantallado (FTP), el cable de par trenzado apantallado (STP), el cable coaxial y el cable de fibra óptica.



*Imagen 9. Sistemas de cableado*

*Fuente: Google Imágenes*

Los sistemas de cableado, siguiendo la norma EIA/TIA 568, representan la infraestructura física y lógica que comprende todos los elementos necesarios para establecer una red de telecomunicaciones en un entorno comercial o empresarial. Esto abarca desde los cables hasta los dispositivos de interconexión, pasando por conectores, paneles de conexión y demás componentes involucrados en la transmisión de datos. Estos sistemas se diseñan, instalan y mantienen de acuerdo con estándares específicos para asegurar la fiabilidad y el óptimo funcionamiento de la red.

#### **2.3.2.6 Pruebas y certificaciones**

Morales (2014) indica claramente que los sistemas de cableado estructurado que se adhieren a los estándares de instalación deben estar certificados. Los analizadores, como la serie 4000 de Redes Fluke, llevan a cabo todos los análisis de rendimiento necesarios para que se cumplan los estándares ANSI/TIA/EIA 568

En otras palabras, las pruebas y certificaciones de red según la norma TIA/EIA 568 son procedimientos específicos que se realizan para verificar y garantizar que un sistema de cableado estructurado cumpla con los estándares establecidos en dicha normativa. Estas pruebas incluyen medidas de desempeño, integridad de la señal, niveles de ruido, entre otros parámetros, para asegurar que la infraestructura cumple con los requisitos de calidad y funcionamiento definidos en la norma TIA/EIA 568.

### **2.3.2.7 Mantenimiento y gestión**

RedHat (2022) explica que el mantenimiento y la gestión de una red de datos implican aplicar prácticas y protocolos para asegurar el funcionamiento adecuado, la integridad y el cuidado de la infraestructura de cableado estructurado según las pautas de TIA/EIA 568. Esto conlleva actividades como monitoreo, diagnóstico, resolución de problemas, actualizaciones y ajustes para garantizar el cumplimiento de los estándares de rendimiento y seguridad del sistema de cableado.

En otras palabras, el mantenimiento y la gestión de la red, dentro del alcance de la normativa TIA/EIA 568, abarcan las prácticas y procedimientos destinados a asegurar el funcionamiento adecuado, la integridad y el cuidado de la infraestructura de cableado estructurado según lo especificado por TIA/EIA 568. Esto incluye actividades como monitoreo, diagnóstico, resolución de problemas, actualizaciones y ajustes para garantizar que el sistema de cableado cumpla con los estándares de rendimiento y seguridad establecidos.

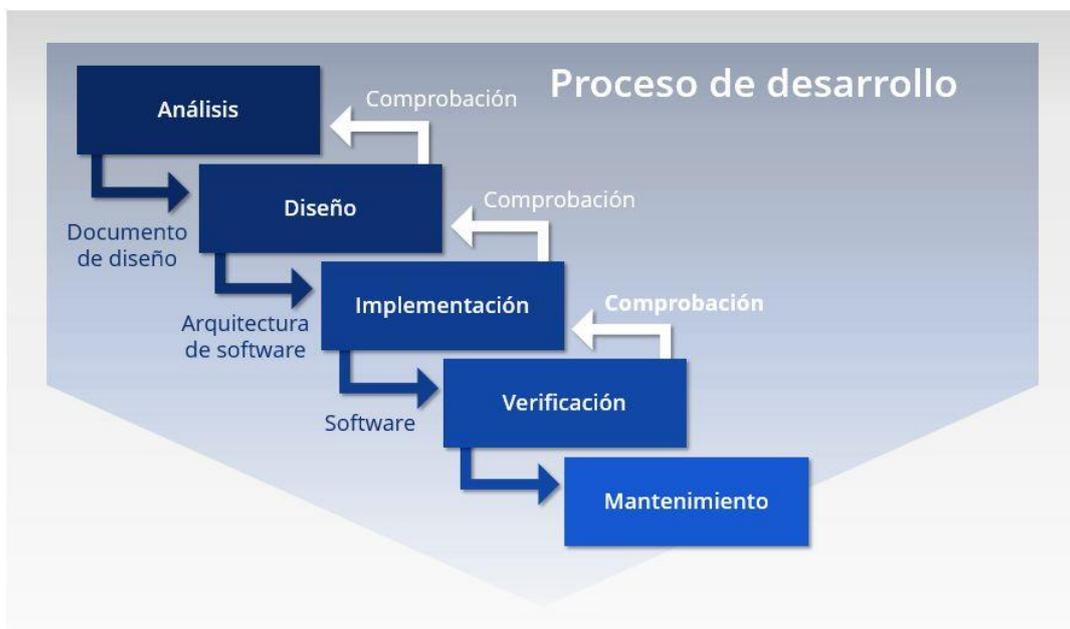
### **2.3.2.8 Cumplimiento y actualizaciones**

Group (2022) resalta que en la planificación de estructuras tecnológicas, la actualización de las redes es un aspecto esencial y no postergable. Su desempeño ahora es crucial, ya que influirá en la habilidad de la empresa para aprovechar tecnologías innovadoras y acceder a modelos de negocios emergentes.

Debemos garantizar el cumplimiento y las actualizaciones de la red, esto quiere decir que tenemos que asegurar que la infraestructura de cableado estructurado se ajuste a los estándares establecidos, esto requiere mantenerse al día con las especificaciones más recientes, realizando ajustes y modificaciones necesarias para mantener la red actualizada y en línea con los niveles de rendimiento y seguridad requeridos.

### 2.3.3 Metodología de desarrollo Cascada (Waterfall)

Alonso (2005) indica que en los años 70 se impuso un enfoque de desarrollo del software, introducido por Royce [Royce, 1970], a través de un ciclo de vida en “cascada”. Este método modela el ciclo convencional de la ingeniería del software, aplicando un enfoque sistemático y secuencial de desarrollo que comienza con la ingeniería del sistema y progresa a través del análisis, diseño, codificación, pruebas y mantenimiento. Normalmente, el “ciclo de vida del software” se suele dividir en tres fases: una de Planificación, otra de Desarrollo y una tercera de Mantenimiento, que engloban a las seis etapas (Ingeniería del Sistema, Análisis de los Requisitos, Diseño, Codificación, Pruebas y Mantenimiento) tradicionales del ciclo de vida.



*Imagen 10. Metodología de desarrollo*

*Fuente: Google Imágenes*

Monge (2023) aclara que fue el primer modelo de desarrollo de software en aplicarse y uno de los precursores de la gran crisis del software ya que era el único modelo que se aplicaba. Es un proceso que consta de una serie de fases, no se pasa a la siguiente hasta que no se finaliza en la que se está, la entrada de una fase es la salida de la anterior. Las fases son: Análisis de Requisitos, Diseño del Sistema, Implementación, Pruebas, Puesta en Producción y Mantenimiento.

## **2.4 Conclusiones del marco teórico**

En conclusión, este proyecto de implementación de una red de datos estructurada para la Junta Cantonal ha sido un desafío enriquecedor y crucial para mejorar la eficiencia operativa y la seguridad en nuestras instalaciones. A lo largo de este proceso, hemos explorado y aplicado los principios fundamentales de la seguridad de redes, la normativa TIA/EIA 568 para el cableado estructurado, y diversas estrategias para proteger nuestros sistemas y datos.

La seguridad de la red no solo implica implementar tecnologías avanzadas como firewalls y sistemas de detección de intrusiones, sino también educar y capacitar a nuestro personal sobre prácticas seguras de TI. Esto garantiza que estemos preparados para enfrentar amenazas actuales y futuras, protegiendo tanto la integridad de nuestros datos como la privacidad de nuestros ciudadanos.

Además, la adopción de un circuito cerrado de televisión conectado a nuestra red nos proporciona una vigilancia continua y mejorada, crucial para la seguridad física de nuestras instalaciones. Esta integración de tecnologías no solo fortalece nuestra capacidad de respuesta ante incidentes, sino que también mejora la eficiencia de nuestras operaciones diarias.

En resumen, esta iniciativa no solo busca modernizar nuestras infraestructuras tecnológicas, sino también establecer un estándar de seguridad que fortalezca la confianza de la comunidad en nuestros servicios. A medida que avanzamos hacia el futuro, continuaremos adaptando y mejorando nuestras redes para mantenernos a la vanguardia de las tecnologías emergentes y las prácticas de seguridad informática.

## CAPÍTULO III

### 3 MARCO INVESTIGATIVO

#### 3.1 Introducción

La Junta Cantonal de la niñez como unidad adscripta del GAD Municipal del Cantón El Carmen, posee información muy valiosa de cada uno de sus usuarios que visitan el lugar día a día con sus diferentes casos, los mismos que deben poseer una gran medida de seguridad y cautelar la privacidad que se merecen. Por ello se realizará la implementación de una red con todas las normas de seguridad para poder así salvaguardar la integridad y la privacidad de estos documentos y de igual forma un sistema de vigilancia para el salvaguardo de la integridad física de cada una de las personas que trabajan en el sitio como también a la ciudadanía en general

#### 3.2 Tipos de investigación

El tipo de investigación a utilizarse para la instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, será según su propósito una investigación aplicada, debido a que se busca mejorar cada uno de los procesos que se realizan en la unidad, resolviendo de esta forma los problemas prácticos que tienen actualmente con una red de datos altamente desorganizada y sin ningún tipo de seguridad en el flujo de los datos.

Ortega (2024) sostuvo que la investigación aplicada es un enfoque no sistemático, el mismo que busca soluciones directas a problemas específicos a nivel individual, grupal o social. Utiliza herramientas científicas para encontrar respuestas y, al igual que en la investigación tradicional, el investigador identifica el problema, formula una hipótesis y la pone a prueba mediante experimentos.

Adicional a esto sin estar de más se utilizará una investigación mixta, la misma que integra métodos cualitativos y cuantitativos. Los métodos cualitativos se utilizarán para explorar a fondo las percepciones, experiencias y necesidades de los usuarios de la Junta Cantonal y el personal de la Unidad de Servicios Tecnológicos del GAD Municipal. Esto incluirá

entrevistas en profundidad y grupos focales para captar perspectivas variadas y contextuales. Por otro lado, los métodos cuantitativos se aplicarán para recopilar datos objetivos sobre el rendimiento de la red, como la velocidad de transferencia de datos, la latencia y la capacidad de la red para soportar cargas de trabajo específicas. Esta combinación permitirá obtener una comprensión integral y holística de los desafíos y oportunidades en la implementación del sistema de seguridad de redes.

### **3.3 Métodos de investigación**

Para la instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, se requiere una investigación exhaustiva para poder garantizar al final su diseño y las operaciones efectivas. Para aquello se procederá a utilizar los siguientes métodos:

- **Análisis de Requisitos.** – Gracias a este método vamos a poder recopilar las necesidades de cada uno de los usuarios de la institución con respecto a la red institucional, para ello utilizaremos las técnicas de entrevistas, encuestas y de igual forma se realizarán reuniones y talleres con cada uno de los funcionarios.
- **Pruebas y Simulaciones.** – Utilizaremos un software como herramienta de trabajo, en la cual vamos a simular previamente el diseño de la red y su funcionamiento, en el mismo utilizaremos las técnicas de Simulación y de pruebas de laboratorio.
- **Investigación de Campo.** - Se harán las respectivas visitas al sitio donde se implementará la red de datos, de esta forma se podrá recolectar información relevante para nuestro propósito, para ello utilizaremos las técnicas de visitas al sitio para evaluar las condiciones ambientales, y mediciones de campo para evaluar potencias e interferencias.
- **Métodos Cualitativos.** – Al final recogeremos datos de tipo estadísticos que nos ayudarán en la toma de decisiones al momento de implementar la red de datos, para ello utilizaremos la técnica del Análisis de tráfico de red evaluando los patrones de uso actual.

## **3.4 Fuentes de información de datos**

### **3.4.1 Encuestas**

La encuesta, referida epistemológicamente a averiguaciones, es una de las herramientas de metodologías cuantitativas que recopila datos mediante consultas. Es útil para poder obtener información relevante sobre grupos o fenómenos. Juni & Urbano (2003) manifestó que a veces, se recomienda adoptar una actitud empática con los encuestados para una mejor recolección de datos.

Se realizarán encuestas a cada uno de los usuarios que laboran en la Junta Cantonal de Protección y Derechos, enfocado principalmente en conocer cada una de sus necesidades, además, conocer las expectativas de cada uno de ellos con respecto al trabajo que se va a realizar.

### **3.4.2 Entrevista**

Se llevará a cabo de igual forma una entrevista con la persona encargada de la Unidad de Tecnologías de la Información y Comunicación del GAD Municipal del Cantón El Carmen, con la finalidad de conocer el estado actual de la red y la forma en que ellos desean tener esta jefatura cantonal enlazada a los servidores principales del GAD, que se encuentran ubicados en el edificio principal.

### **3.4.3 Fichas de Observación**

Además de las encuestas y entrevistas, se implementarán fichas de observación para registrar el comportamiento y las interacciones de los usuarios con el sistema de red propuesto, además las mismas nos permitirán obtener detalles del sitio y la identificación de las zonas más vulnerables para la ubicación de las cámaras. Así mismo, estas fichas permitirán obtener datos detallados sobre cómo los usuarios interactúan con la infraestructura actual y cómo podrían beneficiarse del nuevo sistema de seguridad y cableado estructurado basado en la norma TIA/EIA 568.

### 3.5 Estrategia operacional para la recolección de datos

#### 3.5.1 Población

La población para este proyecto, son todos los trabajadores del Sistema Cantonal, los mismos que son un total de 14 personas distribuidas de la siguiente forma:

ÍTEM	CARGO	TOTAL
1	Vocales de la Junta Cantonal	3
2	Psicólogo Clínico	1
3	Trabajadora Social	1
4	Secretaria Ejecutiva	1
5	Asistente Técnica	2
6	Oficinistas	2
7	Auxiliar de limpieza	1
8	Notificador	1
9	Guardia	1
10	Jefe de STIC	1
Total de Funcionarios Públicos		<b>14</b>

*Tabla 1. Población*

#### 3.5.2 Muestra

Para este proyecto no se considerará una Muestra, ya que se trabajaría directamente con la población de la misma que es un total de 14 personas, dado que no es muy grande y se puede trabajar con la totalidad del personal que labora en el Sistema Cantonal, sumado el Jefe de la Unidad de Tecnologías del GAD Municipal.

#### 3.5.3 Análisis de las herramientas de recolección de datos a utilizar

##### 3.5.3.1 Encuesta

**Título:** Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen.

**Autor:** Luis Mario De La A Briones.

**Dirigido a:** Personal del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen.

**Problema:** Instalación de cámaras de seguridad, cámaras IP, cableado estructurado y documentado bajo la norma TIA/EIA 568, además, de una red LAN para los equipos de cómputo que se encuentran en el área, para una mejor distribución de la red de datos y el uso adecuado del internet.

### **Preguntas.**

1. – ¿Actualmente qué cargo ocupa en la Institución?
  - Administrativo
  - Soporte Informático
  - Atención al Público
  - Otro \_\_\_\_\_
  
2. - Especifique su nivel de conocimiento en Tecnologías
  - Ninguno
  - Básico
  - Intermedio
  - Avanzado
  
3. – ¿La Institución ha realizado capacitaciones de Seguridad Informática?
  - Si
  - No
  
4. – ¿En su puesto de trabajo o cargo asignado utiliza algún equipo informático para sus labores asignadas?
  - Si
  - No
  
5. – Si su respuesta fue (Si), indique ¿con qué frecuencia cambia la clave de su equipo?
  - No tiene clave
  - Cada 3 meses
  - Cada 6 meses
  - Cada año
  - No la ha cambiado
  - No está seguro
  
6. – Si su respuesta fue (Si), indique si otros usuarios de la Institución utilizan su equipo de trabajo

- Si
  - No
7. - ¿Utiliza algún dispositivo móvil personal o institucional conectado a la red inalámbrica de la institución?
- Si
  - No
8. - ¿Existen cámaras de seguridad y videovigilancia en la Institución?
- Si
  - No
9. - ¿Crees que las cámaras de seguridad son efectivas para salvaguardar la integridad de los empleados de la Institución?
- Si
  - No
10. - ¿Te sientes cómodo en tu sitio de trabajo conociendo de la ubicación de las cámaras de videovigilancia?
- Si
  - No
11. - ¿Conoces de qué forma se accede a las cámaras de seguridad de tu institución para la revisión de hechos que se hayan suscitado?
- No tiene idea
  - Por medio de un celular
  - Por medio de un computador
  - Por medio de un DVR/NVR
12. - ¿Te gustaría recibir más información sobre tus derechos en la Institución en relación con la privacidad y protección de datos de tus dispositivos de trabajo?
- Si
  - No
13. - ¿Ha recibido alguna capacitación sobre el uso seguro de las cámaras de vigilancia en su institución?
- Si
  - No
14. - ¿En su puesto de trabajo ha experimentado algún problema de seguridad relacionado con la red de datos o las cámaras de seguridad?
- Si
  - No
  - No está seguro

### 3.5.3.2 Entrevista

**Título:** Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen.

**Autor:** Luis Mario De La A Briones

**Dirigido a:** Jefe de la Unidad de Servicios Tecnológicos de la Información y Comunicación del GAD Municipal del Cantón El Carmen

**Problema:** Instalación de cámaras de seguridad, cámaras IP, cableado estructurado y documentado bajo la norma TIA/EIA 568, además, de una red LAN para los equipos de cómputo que se encuentran en el área, para una mejor distribución de la red de datos y el uso adecuado del internet.

1. ¿Qué rol ocupa actualmente en la Unidad de Servicios Tecnológicos de la Información y Comunicación y cuáles son sus funciones como tal?
2. ¿Actualmente qué medidas de seguridad tienen implementado en su Institución?
3. De los diferentes tipos de redes tales como LAN, VLAN, VPN, WAN, WIFI, etc. ¿Cuál es el que más utiliza en su Institución?
4. ¿Tienen implementados medidas de seguridad para los diferentes tipos de redes que se manejan dentro de la institución?
5. ¿Capacitan constantemente al personal de la Institución sobre el uso de la red y las medidas de seguridad que tienen implementadas en la Institución?
6. ¿Realizan auditorias sobre la seguridad de las redes de datos y con qué frecuencia se dan?
7. Desde el edificio principal donde se encuentra el DATA CENTER de la Institución ¿Se dispone de algún control y manejo de la red del Sistema Cantonal?
8. En el tema de videovigilancia ¿Qué tipo de cámaras utilizan en la Institución para salvaguardar la integridad de los bienes, datos y personal laboral?
9. ¿Disponen de políticas para el monitoreo en vivo y la recolección de grabaciones de los dispositivos?

10. ¿Cómo se aseguran de que tanto los videos como las imágenes capturadas por las cámaras estén protegidas contra accesos no autorizados?
11. ¿Cuánto tiempo reposan los videos guardados en los equipos?
12. ¿Tanto los dispositivos de la red de datos como los de videovigilancia de la Institución se encuentran debidamente actualizados?
13. ¿Cuáles serían las prioridades de la Institución a corto y largo plazo para la mejora de la seguridad en redes de datos y cámaras de vigilancia?
14. ¿Cuenta con algún proyecto para fortalecer o actualizar la seguridad de la información en conjunto con el tema de videovigilancia?

### **3.5.3.3 Estructura de los instrumentos de recolección de datos aplicados**

#### **Estructura de la encuesta elaborada:**

##### 1. Introducción

Título de la encuesta

Propósito de la encuesta

##### 2. Sección de Información Demográfica

Preguntas sobre la información básica del encuestado (edad, género, ocupación, nivel educativo, etc.)

##### 3. Sección de Preguntas Temáticas

Seguridad en Redes de Datos

Preguntas específicas sobre el uso y protección de redes de datos.

Frecuencia de cambios de contraseña, uso de medidas de seguridad.

Seguridad de Cámaras de Video Vigilancia

Preguntas sobre el uso y conocimiento de cámaras de vigilancia

Tipos de cámaras utilizadas, métodos de acceso a las grabaciones, medidas de seguridad, etc.

4. Sección de Opiniones y Sugerencias

5. Conclusión

**Estructura de la entrevista elaborada:**

1. Introducción

Título de la entrevista

Propósito de la entrevista

2. Sección de Preguntas Introdutorias

Preguntas generales para conocer el rol y experiencia del entrevistado (nombre, cargo, tiempo en el puesto, etc.)

3. Sección de Preguntas Temáticas

Seguridad en Redes de Datos

Preguntas sobre las políticas y prácticas de seguridad de la red

Medidas de seguridad implementadas, incidentes y desafíos enfrentados, etc.

Seguridad de Cámaras de Video Vigilancia

Preguntas sobre el uso y manejo de cámaras de vigilancia

Tipos de cámaras, acceso a grabaciones, incidentes y políticas de seguridad, etc.

#### 4. Sección de Opiniones y Perspectivas Futuras

Preguntas sobre tecnologías futuras, prioridades y recomendaciones

#### 5. Conclusión

Agradecimiento al entrevistado por su tiempo

### 3.5.4 Plan de recolección de datos

<b>Cronograma</b>		
<b>Fecha</b>	<b>Actividad</b>	<b>Resultado Esperado</b>
06/05/2024	Encuesta al Personal que labora en la Institución	Obtención de resultados sobre sus conocimientos de red y la seguridad de los datos
07/05/2024	Entrevista al Jefe de la Unidad de STIC del GAD Municipal El Carmen	Obtención de requerimientos por parte de la jefatura acerca de la instalación de los recursos de red en el Sistema Cantonal y el enlace hacia el GAD Municipal
07/05/2024	Inspección del lugar y verificación de cada uno de los equipos de cómputo y de red, llenado de Fichas de observación	Verificación del lugar de los equipos para la determinación de recursos a utilizar y la distancia hacia el centro de datos de la institución
08/05/2024	Socialización del sitio donde irán instaladas las cámaras, llenado de fichas de observación	Determinación del sitio adecuado donde se instalarán cada una de las cámaras de video vigilancia

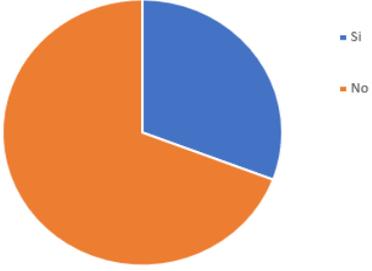
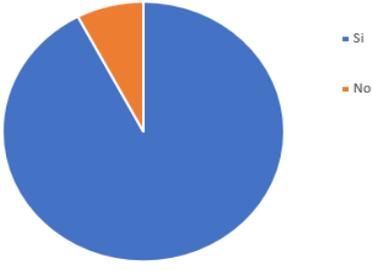
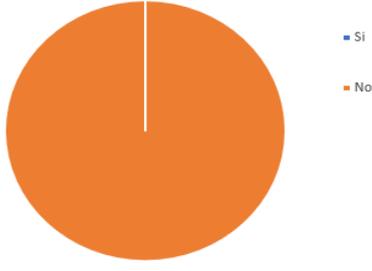
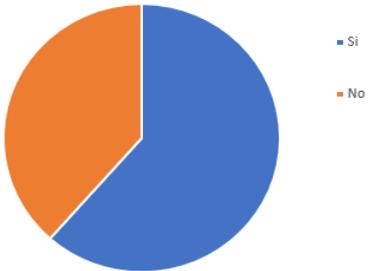
*Tabla 2. Plan de recolección de datos*

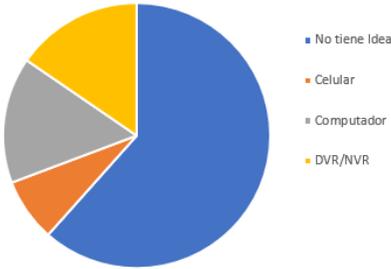
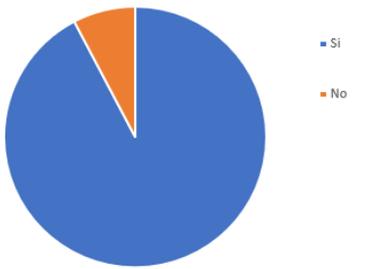
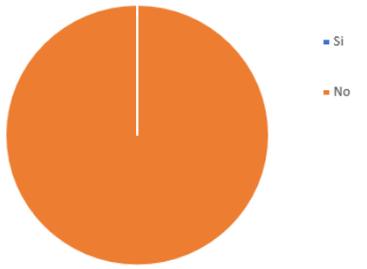
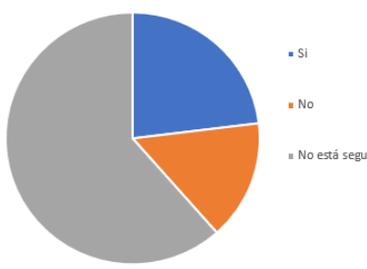
### 3.6 Análisis y presentación de resultados

#### 3.6.1 Tabulación

##### a) Encuesta

Pregunta	Resultado	Análisis
1. ¿Actualmente qué cargo ocupa en la Institución?	<ul style="list-style-type: none"> <li>■ Administrativo</li> <li>■ Soporte Informático</li> <li>■ Atención al Público</li> <li>■ Otro</li> </ul>	El gráfico en pastel muestra que un 60% de los empleados trabaja en atención, el 20% a nivel administrativo, el 20% restante en diferentes actividades y ninguno de ellos conoce de Soporte Técnico
2. Especifique su nivel de conocimiento en Tecnologías	<ul style="list-style-type: none"> <li>■ Ninguno</li> <li>■ Básico</li> <li>■ Intermedio</li> <li>■ Avanzado</li> </ul>	La gráfica muestra que el 70% posee un nivel de conocimiento básico sobre las tecnologías, preocupando que un 10% no conoce nada de las mismas y que solo un 20% tengo un conocimiento mediano.
3. ¿La Institución ha realizado capacitaciones de Seguridad Informática?	<ul style="list-style-type: none"> <li>■ Si</li> <li>■ No</li> </ul>	La gráfica muestra que el 95% de los encuestados afirma que no se han realizado capacitaciones de Seguridad Informática en el sistema cantonal
4. ¿En su puesto de trabajo o cargo asignado utiliza algún equipo informático para sus labores asignadas?	<ul style="list-style-type: none"> <li>■ Si</li> <li>■ No</li> </ul>	La gráfica muestra claramente que solo el 70% de los empleados utiliza equipo informático para sus labores, el resto no.
5. Si su respuesta fue (Si), indique ¿con qué frecuencia cambia la clave de su equipo?	<ul style="list-style-type: none"> <li>■ Sin clave</li> <li>■ 3 meses</li> <li>■ 6 meses</li> <li>■ Cada año</li> <li>■ No cambia</li> <li>■ Inseguro</li> </ul>	La gráfica nos muestra que Existe el 45% de equipos sin clave y los que tienen claves, llevan mucho tiempo sin cambiarla e incluso un 20% nunca la ha cambiado

<p>6. Si su respuesta fue (Si), indique si otros usuarios de la Institución utilizan su equipo de trabajo</p>	 <p>■ Si ■ No</p>	<p>En esta gráfica es preocupante conocer que el 30% de empleados comparten su equipo de trabajo con sus compañeros, mientras que el 70% no</p>
<p>7. ¿Utiliza algún dispositivo móvil personal o institucional conectado a la red inalámbrica de la institución?</p>	 <p>■ Si ■ No</p>	<p>En esta gráfica se expone que el 95% de los empleados disponen de un celular conectado al router que dispone la Institución. Solo el 5% utiliza sus datos personales</p>
<p>8. ¿Existen cámaras de seguridad y videovigilancia en la Institución?</p>	 <p>■ Si ■ No</p>	<p>Esta gráfica nos muestra que el 100% de empleados indica que aún no existen cámaras de seguridad instaladas en el sistema cantonal</p>
<p>9. ¿Crees que las cámaras de seguridad son efectivas para salvaguardar la integridad de los empleados de la Institución?</p>	 <p>■ Si ■ No</p>	<p>En esta gráfica Todos sin excepción, el 100% considera que las cámaras son muy útiles en sus puestos de trabajo</p>
<p>10. ¿Te sientes cómodo en tu sitio de trabajo conociendo de la ubicación de las cámaras de videovigilancia?</p>	 <p>■ Si ■ No</p>	<p>En esta gráfica se expone claramente que el 60% de los empleados se sentiría cómodo con la ubicación de las cámaras de seguridad, mientras que el 40% indica que no se sentiría cómodo con la ubicación de las mismas</p>

<p>11. ¿Conoces de qué forma se accede a las cámaras de seguridad de tu institución para la revisión de hechos que se hayan suscitado?</p>		<p>En esta gráfica se muestra que, al no existir cámaras en el sistema cantonal, los empleados enfocaron su respuesta a cultura general</p>
<p>12. ¿Te gustaría recibir más información sobre tus derechos en la Institución en relación con la privacidad y protección de datos de tus dispositivos de trabajo?</p>		<p>En esta gráfica se muestra que el 95% de los empleados desea que se les capacite sobre temas de seguridad y sobre el uso de cámaras</p>
<p>13. ¿Ha recibido alguna capacitación sobre el uso seguro de las cámaras de vigilancia en su institución?</p>		<p>En esta gráfica es claro observar que el 100% de los empleados nunca ha recibido capacitación alguna por parte de ningún organismo sobre este tema</p>
<p>14. ¿En su puesto de trabajo ha experimentado algún problema de seguridad relacionado con la red de datos o las cámaras de seguridad?</p>		<p>En esta gráfica se expone que el 60% de los empleados desconoce el tema, pero el 25% de ellos han presentado problemas al tratar de compartir archivos, imprimir en otras ubicaciones y con la pérdida de algún documento</p>

**Tabla 3. Resultados de la Encuesta**

**b) Entrevista**

Pregunta	Respuesta	Análisis
<p>1. ¿Qué rol ocupa actualmente en la Unidad de Servicios Tecnológicos</p>	<p>Actualmente soy el jefe de la Unidad de STIC del GAD municipal del Cantón El Carmen.</p>	<p>El GAD Municipal como tal cuenta con una Unidad de TI la cual entre sus</p>

de la Información y Comunicación y cuáles son sus funciones como tal?	La Unidad actualmente cuenta con diferentes áreas, como la de Soporte Técnico Informático, Desarrollo, Infraestructura y Administrativa.	responsabilidades está la de velar por la infraestructura y tener operativa la red de datos de cada una de las dependencias, así como precautelar el debido uso de cada uno de los equipos informáticos
	Mi rol fundamental es liderar cada una de estas áreas ya que son el pilar fundamental y la base tecnológica para el desenvolvimiento de las actividades que realiza el GAD como tal.	
	La red de datos esté 100% activa y que cada informático esté operativo y actualizado con cada una de las políticas establecidas por la Unidad.	
2. ¿Actualmente qué medidas de seguridad tienen implementado en su Institución?	Como medidas de seguridad actuales tenemos el control de cada uno de los dispositivos que se utilizan en cada una de las dependencias del GAD	Las medidas de seguridad que se tienen son muy limitadas para el control de la red de datos
	Se tiene pleno control del Usuario administrador de cada equipo de cómputo	
3. De los diferentes tipos de redes tales como LAN, VLAN, VPN, WAN, WIFI, etc. ¿Cuál es el que más utiliza en su Institución?	Bueno de los tipos mencionados se utilizan todos aquí en el GAD, pero el que más se utiliza es la red LAN, se podría decir que en su 80%	No se tiene un enfoque adecuado y definido sobre el dominio del 100% de sus equipos recurriendo a la improvisación de los mismos
	En algunas dependencias tenemos algunos inconvenientes por infraestructura y nos toca improvisar con otro tipo de conexión, tales como WIFI o VPN.	
4. ¿Tienen implementados medidas de seguridad para los diferentes tipos de redes que se manejan dentro de la institución?	Se está trabajando en un plan de seguridad, el mismo que una vez terminado tendrá que ser autorizado por la máxima autoridad para poner en ejecución	Actualmente no se cuenta con un plan definido de seguridad, se improvisa con las herramientas que disponen
	Actualmente procedemos con las herramientas que tenemos a disposición para evitar cualquier tipo de ataque tanto interno como externo.	
5. ¿Capacitan constantemente al personal de la Institución sobre el uso de la red y las medidas de seguridad que tienen implementadas en la Institución?	Una capacitación como tal no se ha dado actualmente, hablando de la red de datos y su seguridad	El personal del GAD no se encuentra capacitado sobre el uso y la seguridad de la red de datos.
	Lo que si se brinda es una capacitación de cada uno de los sistemas informáticos y su buen uso, para evitar inconvenientes con el desempeño de los mismos	
6. ¿Realizan auditorías sobre la seguridad de las redes de datos y con qué frecuencia se dan?	Actualmente no se han realizado auditorías externas por parte de los organismos de control del gobierno nacional	No se realizan auditorías de red, por lo tanto, se desconoce oficialmente el estado en el que se encuentran
	Y las auditorías internas se realizarán una vez sea aprobado el plan de seguridad que está en construcción	
7. Desde el edificio principal donde se encuentra el DATA CENTER de la	Claro, el equipo que se encuentra en el Sistema Cantonal se encuentra conectado por medio de un túnel de datos hacia el	Los equipos con los que se realiza el túnel de datos para tener conectados

Institución ¿Se dispone de algún control y manejo de la red del Sistema Cantonal?	edificio principal	ambas entidades son del proveedor de internet, es decir ellos también tienen acceso a los mismos
	Gracias a ese túnel podemos tener un control de cada uno de los equipos que se encuentran operativos en el Sistema Cantonal	
	El túnel de datos y el equipo para el mismo son provistos por el proveedor de internet	
8. En el tema de videovigilancia ¿Qué tipo de cámaras utilizan en la Institución para salvaguardar la integridad de los bienes, datos y personal laboral?	En el edificio principal y en otras dependencias del GAD Municipal hay circuitos cerrados de TV instalados	Solo se dispone de cámaras de seguridad en algunas dependencias, no en todas
	Se encuentran instaladas cámaras de tipo domo en los interiores de cada dependencia y de tipo tubo en los exteriores de la misma	
	Además de esto tenemos instaladas unas cámaras PTZ en sitios de mayor concurrencia de la urbe cantonal	
9. ¿Disponen de políticas para el monitoreo en vivo y la recolección de grabaciones de los dispositivos?	Políticas como tal aún no disponemos, para hacer uso de las grabaciones se solicita autorización a la máxima autoridad	Al no tener políticas para el monitoreo no se pueden asignar responsabilidades ni muchos responsables por el mal uso de las mismas
	En el plan de seguridad de redes que se está armando, se incluirán políticas sobre las cámaras de videovigilancia	
	Además de eso se establecerá a cargo de quien quedarán las mismas y las responsabilidades que quedarán consigo.	
10. ¿Cómo se aseguran de que tanto los videos como las imágenes capturadas por las cámaras estén protegidas contra accesos no autorizados?	Bueno, en los sitios que tenemos cámaras de videovigilancia contamos con un pequeño rack de pared, de los cuales el área de STIC somos los únicos que tenemos acceso a los mismos	Aún no se dispone a cargo de quién deben estar estos equipos teniendo acceso todo el personal del área de STIC
	Por otro lado, en el edificio principal el equipo de grabación se encuentra dentro del DATA CENTER al cual solo nosotros tenemos acceso	
11. ¿Cuánto tiempo reposan los videos guardados en los equipos?	Por lo general y en la mayoría de dispositivos tenemos una duración de al menos 30 días en que reposan los videos en los mismos	No todos los dispositivos tienen la misma configuración de grabado, ya que son de diferentes marcas y modelos
	No se tiene estimado más tiempo por rescatar la mejor resolución de cada video e imagen capturada	
12. ¿Tanto los dispositivos de la red de datos como los de videovigilancia de la Institución se encuentran debidamente actualizados?	Podemos estimar actualmente que el 30% de los equipos de infraestructura se encuentran debidamente actualizados	Hay equipos tecnológicos que ya cumplieron su vida útil y se siguen utilizando a pesar de los riesgos
	Se está trabajando en un proceso de adquisición para repotenciar ciertos equipos que ya cumplieron su vida útil	
	En este proceso se implementarán equipos de última tecnología tales como Fortinet	
13. ¿Cuáles serían las prioridades de la	A corto plazo la compra de equipos más	Se debería capacitar al personal del GAD a corto

Institución a corto y largo plazo para la mejora de la seguridad en redes de datos y cámaras de vigilancia?	sofisticados para la repotenciación de la seguridad a nivel de infraestructura	plazo
	A largo plazo la capacitación a los servidores públicos sobre las políticas y sanciones por el mal uso de los sistemas del GAD Municipal y el acceso a las tecnologías del mismo	
14. ¿Cuenta con algún proyecto para fortalecer o actualizar la seguridad de la información en conjunto con el tema de videovigilancia?	Proyecto como tal aún no se encuentra plasmado por la falta de presupuesto en el área, ya que al no ser dirección se debe de considerar el presupuesto de la dirección administrativa a la cual pertenece la unidad	Al no ser una dirección como tal no cuenta con un presupuesto propio para levantar un proyecto acorde a las necesidades actuales
	Para este año y para el próximo se tienen considerado la adquisición de equipos de alta tecnología para proveer a los usuarios un buen acceso a la red y a los sistemas informáticos	
	Y en el tema de videovigilancia así mismo un proceso para tener a todas las dependencias con este sistema y poder tener un solo control desde el edificio principal	

**Tabla 4. Resultados de la Entrevista**

### 3.6.2 Presentación y descripción de los resultados obtenidos

Una vez realizado el proceso de encuesta y el de entrevista, hemos notado que las interrogantes 3 y 13 de la encuesta están relacionadas directamente con la pregunta 5 de la entrevista en relación a la ausencia de capacitaciones al personal de la institución con respecto a lo relacionado a las redes informáticas, cámaras de video vigilancia y seguridad informática, dando como resultado que hasta la fecha no se han realizado capacitaciones a los usuarios del GAD Municipal del Cantón El Carmen respecto a seguridades informáticas, es decir que ningún usuario conoce temas de redes y el cuidado a tener para salvaguardar la integridad de los datos que son exclusivamente de uso institucional, en consecuencia se deduce que todos los problemas que se dan por temas de conexión es por el completo desconocimiento de los usuarios.

### 3.6.3 Informe final del análisis de los datos

El análisis de los datos recopilados a través de las encuestas y entrevista realizada no arrojan como resultado la falta de conocimiento y capacitación, al mostrar los usuarios un conocimiento limitado por no decir nulo en el uso de tecnologías y no ha recibido

capacitaciones sobre seguridad informática, representando un riesgo para la integridad de los datos. Para evitar esto se deben programar capacitaciones de políticas de seguridad al personal de la institución para de una u otra forma reducir los riesgos asociados al uso inadecuado de los sistemas informáticos, se debe también implementar programas de capacitaciones continuas en seguridad informática para todo el personal y de esta forma asegurar el uso adecuado y seguro de los recursos tecnológicos.

## CAPÍTULO IV

### 4 MARCO PROPOSITIVO

#### 4.1 Introducción

La mayor dependencia de la tecnología y la digitalización ha hecho que la seguridad de las redes de datos y los sistemas de videovigilancia sea una prioridad clave para las empresas privadas y las instituciones públicas. Para proteger tanto la información, como los activos fijos y de igual forma la parte humana, es importante proteger los datos críticos y los activos de vigilancia con cámaras de vigilancia eficaces.

Por ello, el propósito de este proyecto es definir las políticas y estrategias necesarias para implementar un sistema de seguridad integral que combine la protección de la red de datos y la instalación de cámaras de seguridad, teniendo como objetivo aparte de prevenir el acceso no autorizado y ataques cibernéticos, proporcionar una capa adicional de seguridad física, al poder monitorear y de registrar constantemente la actividad de cada una de las áreas del Concejo Cantonal, es decir, combinar la seguridad de la red de datos y la videovigilancia para poder responder de forma rápida y eficiente a cualquier tipo de incidente, reduciendo el riesgo y protegiendo los activos de la institución.

#### 4.2 Descripción de la propuesta

El objetivo principal de la propuesta se centra en el diseño e implementación de un sistema de seguridad que combine la protección avanzada de la red de datos con un circuito cerrado de videovigilancia. Este sistema tiene como finalidad garantizar la seguridad de la información gestionada en la institución, así como salvaguardar la integridad de los activos fijos y del personal que labora en el Concejo Cantonal.

El alcance de la propuesta incluye una evaluación de seguridad que consistirá en un análisis preliminar de las necesidades específicas en las instalaciones del Concejo Cantonal. A partir de esta evaluación, se procederá con el diseño detallado de la infraestructura, describiendo la arquitectura de la red y la disposición de cada una de las cámaras. Una vez finalizado el diseño, se realizará la adquisición de los equipos y el software necesario, incluyendo firewall, cámaras de alta resolución, sistemas de almacenamiento de datos, cifrado, entre otros.

Posteriormente, se procederá con la configuración e instalación de los dispositivos de la red de datos y de videovigilancia, realizando las respectivas pruebas y validación de las mismas para así asegurar el correcto funcionamiento y la capacidad de respuesta en caso de incidentes, terminando con una capacitación a la Unidad de Servicios Tecnológicos del GAD Municipal del Cantón El Carmen, sobre el uso y la gestión de cada uno de sus componentes y al final cuadrar el tema de soporte técnico.

Entre los componentes necesarios para el Sistema de Seguridad, se prevé la adquisición de un Firewall avanzado el mismo que permita controlar el tráfico de la red y poder de una u otra forma bloquear los accesos no deseados al entorno de trabajo. De igual forma en la adquisición se tendrá cámaras de alta resolución e identificador con reconocimiento facial y de alta gama para obtener una excelente resolución al momento de grabado, y para esto también se procederá a adquirir, un equipo de almacenamiento seguro y confiable que asegure la disponibilidad de los videos y la protección de los mismos, y para ello se dispondrá de un software de gestión, el mismo que facilitará la identificación de cada uno de los incidentes y la respuesta inmediata al mismo.

Una vez implementado el sistema de seguridad, inmediatamente se obtendrán beneficios tales como, la mejora de la seguridad, tanto interna como externa, detección e identificación de cada incidente ocurrido en la red, se evitarán ataques de riesgos asociados a ciberataques y accesos no autorizados, brindando la confianza a cada una de las personas que trabajan en el Concejo Cantonal.

### 4.3 Determinación de recursos

#### 4.3.1 Humanos

Cantidad	Rol	Descripción
1	Autor del Proyecto de Titulación	Persona encargada de la elaboración del proyecto de titulación
1	Tutor del Proyecto de Titulación	Persona designada en guiar, supervisar y asesorar al autor en el desarrollo del proyecto de titulación

13	Personas que laboran en el Sistema Cantonal	Personas encuestadas con el fin de recabar información necesaria de las necesidades informáticas del Sistema Cantonal
1	Persona entrevistada del GAD Municipal El Carmen	Jefe de la Unidad de Servicios Tecnológicos del GAD El Carmen, quien está a cargo de la Administración de la red de toda la Institución

**Tabla 5. Recursos Humanos**

### 4.3.2 Tecnológicos

Cantidad	Recursos	Descripción
1	Firewall	Dispositivo que se encarga de la protección de la red para evitar accesos no autorizados y posibles amenazas externas
4	Cámaras de Videovigilancia	Cámaras IP con capacidades de formato HD o 4K, las mismas que nos ayudarán con una vigilancia clara.
1	Servidor de Almacenamiento	Servidor de Tipo NAS (Network Attached Storage) en donde se almacenarán las grabaciones de un modo bien seguro.
1	Switch Administrable	Equipo de Red para el tráfico de los datos.
1	Router	Equipo de Red para el tráfico de los datos de forma inalámbrica.
1	UPS	Dispositivo para el almacenaje de la energía que evita que los dispositivos se apaguen en caso de existir cortes de energía
1	Plataforma de Gestión de Videovigilancia	Software que realiza la gestión centralizada de las cámaras, su almacenamiento y su análisis
1	Rollo de Cable UTP Cat6	Cable estructurado para el armado de la red y conexión de cada uno de los dispositivos al firewall
30	Conectores RJ45 Cat6	Conectores terminales para la conexión de los equipos a la red
1	Rack	Gabinete para el guardado de los equipos para su protección
1	Servicio de Configuración e instalación	Persona especializada para proceder con

		la instalación de cada uno de los dispositivos y la configuración de los mismos
1	Monitoreo y Mantenimiento	Servicio para realizar de forma constante un monitoreo y los mantenimientos correspondientes
1	Capacitación al personal	Capacitación al personal de Servicios Tecnológicos del GAD Municipal del Cantón El Carmen sobre el uso adecuado de cada uno de los dispositivos y plataformas

**Tabla 6. Recursos Tecnológicos**

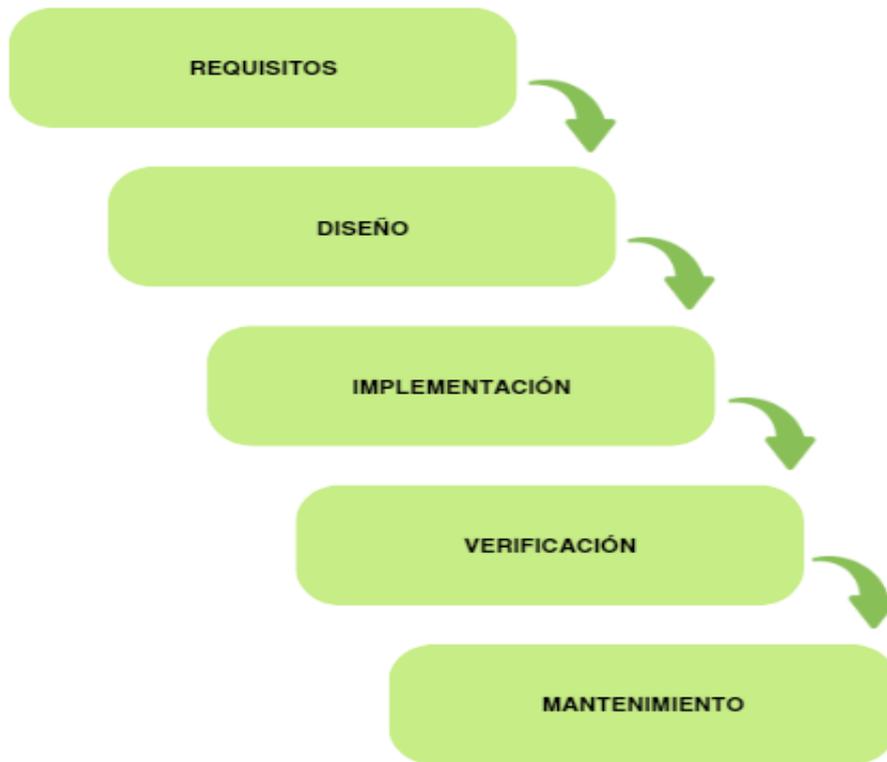
### 4.3.3 Económicos

Técnico	Acciones	Tiempo	Costos
Luis De La A	Aplicación de Entrevista	1 día	0,00
	Aplicación de Encuestas	2 días	0,00
	Instalación de la Red De Datos	2 días	3.700,00
	Instalación de las cámaras de Videovigilancia	2 días	1.200,00
	Configuración de Dispositivos y plataformas	1 día	750,00
	Mantenimiento y Monitoreo de Sistema de Seguridad	2 veces al año	400,00
	Capacitación de Usuarios en uso de las plataformas	1 día	300,00

**Tabla 7. Recursos Económicos**

### 4.4 Desarrollo (Metodología Cascada)

El desarrollo de este proyecto, tal como se ha descrito anteriormente, se llevará a cabo utilizando la metodología en cascada. Este enfoque es secuencial y sistemático, donde cada fase debe completarse antes de iniciar la siguiente. Para este proyecto, se seguirán las fases descritas en la Imagen 11.



*Imagen 11. Metodología Cascada*

#### **4.4.1 Requisitos**

Para la identificación y obtención de requisitos necesarios para el desarrollo de este proyecto, se realizaron encuestas a los usuarios de la Junta Cantonal de Protección y Derechos, para de este modo conocer sus necesidades y a la vez sus expectativas con la implementación del Sistema de Seguridad en redes y cámaras de video vigilancia, además de tener presente sus conocimientos informáticos, sobre todo en temas de seguridad.

De la igual manera se llevó a cabo una entrevista con la persona encargada de la Unidad de Servicios Tecnológicos del GAD Municipal del Cantón El Carmen. Esta entrevista fue fundamental para comprender los aspectos de seguridad de la Institución, conocer su estado actual, y determinar si cuentan con políticas de seguridad y capacitación para el personal en cuanto a las prohibiciones y el uso adecuado de la infraestructura de la Unidad. Además, permitió identificar los requisitos específicos para la integración del sistema de la Junta Cantonal con los servidores del GAD Municipal.

Por último, se emplearon fichas de observación que facilitaron la documentación del estado actual de la infraestructura de red de la Junta cantonal de Protección y Derechos.

De todo esto se pudo al final determinar la especificación de requerimientos de la siguiente forma:

#### **4.4.1.1 Requerimientos de usuario**

Se pudo conocer las necesidades y expectativas de los usuarios en relación con la implementación del sistema de seguridad en redes y cámaras de video vigilancia. Asegurando que el sistema cumpla con cada una de las expectativas de seguridad y funcionalidad de los usuarios.

Así mismo, se evaluó el nivel de conocimiento informático de cada uno de los empleados, el enfoque del técnico y en temas de seguridad, para de este modo poder diseñar un sistema que se ajuste a sus capacidades y requerimientos.

#### **4.4.1.2 Requerimientos técnicos**

Documentar el estado actual de la infraestructura de red de la Junta Cantonal de Protección y Derechos para poder al final identificar posibles deficiencias y áreas de mejora en la infraestructura existente

Verificar la existencia y adecuación de políticas de seguridad dentro de toda la institución, para de esta forma poder determinar la necesidad de establecer o mejorar las políticas de seguridad para el uso adecuado de la infraestructura tecnológica.

Identificar si se ha proporcionado capacitaciones al personal sobre las prohibiciones y el uso adecuado de la infraestructura tecnológica, para luego proponer programas de capacitación si se llegara a detectar una falta de conocimiento o procedimientos no adecuados.

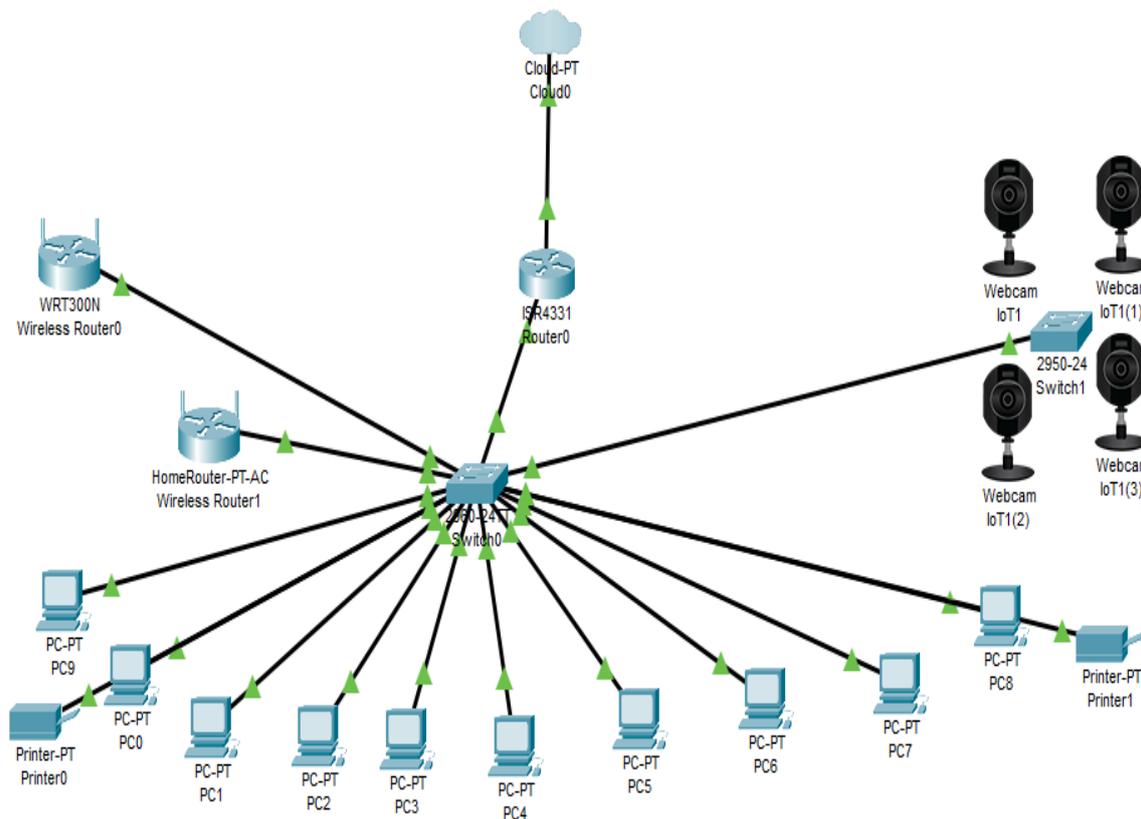
#### 4.4.1.3 Requerimientos de integración

Especificar los requisitos técnicos necesarios para la integración del sistema de la Junta cantonal de Protección y derechos con los servidores del GAD Municipal de El Carmen, para luego asegurar la compatibilidad y seguridad en la interconexión entre ambos sistemas.

#### 4.4.1.4 Requerimientos de documentación

Utilizar las fichas de observación para documentar el estado actual de la red y las instalaciones tecnológicas y mantener registros detallados que faciliten la planificación y ejecución del proyecto.

#### 4.4.2 Diseño



*Imagen 12. Diseño de la Red*

En la imagen podemos apreciar el diseño o prototipo de la red de datos propuesta para el Sistema Cantonal de Protección y Derechos, el mismo que parte desde un Router Administrable principal provisto por el proveedor del Servicio de Internet, el mismo que va a cumplir las funciones de Firewall y a la vez se encargará de crear y gestionar el túnel de datos para la conexión de la Junta Cantonal hasta el GAD Municipal edificio principal, de donde se tendrá el control de cada uno de los dispositivos que se conectarán en el sitio.

A continuación del Firewall se conectará un Switch de 24 puertos, en el mismo se conectarán todos los dispositivos de la Junta Cantonal de El Carmen tal como se aprecia en la imagen, se conectarán los equipos de cómputo, router inalámbrico, cámaras de video vigilancia y un reloj biométrico de control de personal, entrada y salida de sus labores.

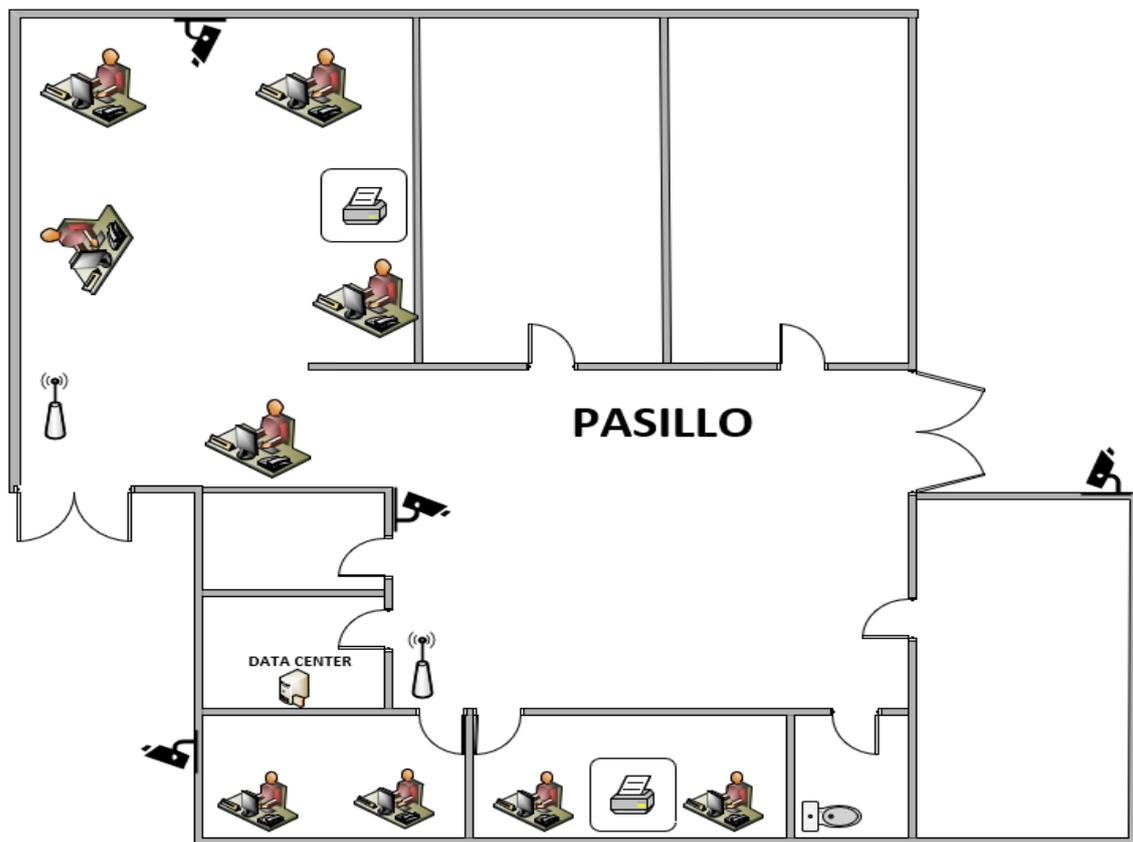
El Sistema de seguridad que se va a implementar comprende una red de cableado estructurado, la misma que va desde un switch administrable, hacia los equipos informáticos que se detallan a continuación:

ÍTEM	EQUIPO	IP	MAC
1	PC de Escritorio	192.168.45.106	52:54:00:E1:94:24
2	PC de Escritorio	192.168.45.102	52:54:00:DA:0E:19
3	PC de Escritorio	192.168.45.103	52:54:00:BB:DD:88
4	PC de Escritorio	192.168.45.104	52:54:00:80:BA:57
5	PC de Escritorio	192.168.45.105	52:54:00:69:2D:E8
6	PC de Escritorio	192.168.45.107	52:54:00:0F:03:93
7	PC de Escritorio	192.168.45.108	4C:5E:0C:F6:C0:AB
8	PC de Escritorio	192.168.45.109	4C:5E:0C:97:FD:99
9	PC de Escritorio	192.168.45.110	4C:5E:0C:74:76:80
10	Router Inalámbrico	192.168.45.120	E4:8D:8C:35:95:AC
11	Router Inalámbrico	192.168.45.130	E4:8D:8C:17:E4:1A
12	DVR de Cámaras de Seguridad	192.168.45.125	D4:CA:6D:1C:37:54
13	Reloj Biométrico	192.168.45.135	00:0C:42:F0:B2:E6

*Tabla 8. Equipos Tecnológicos de la Junta Cantonal*

Una vez identificados los equipos que se conectarán al sistema de red de la Junta Cantonal, se procedió a diseñar la disposición de cada equipo en las distintas áreas de las oficinas de la institución. También se determinó la ubicación estratégica de los routers inalámbricos y las cámaras de video vigilancia, de modo que cubran adecuadamente todas las zonas del edificio y permitan un óptimo funcionamiento.

Para la ejecución de este proyecto se seleccionó una de las oficinas para que funcione como el centro de datos (data center) de la Junta Cantonal. En esta oficina se instalarán los equipos principales, como el switch, el DVR de las cámaras, y los equipos del proveedor de internet. Para obtener una visión clara de la disposición final de los equipos, se puede consultar la imagen 13.



*Imagen 13. Croquis de la Junta Cantonal*

### 4.4.3 Implementación

#### 4.4.3.1 Identificación y ubicación del centro de datos

Para iniciar la implementación, se realizó un reconocimiento preliminar del área donde se ubicarán los equipos principales del sistema de seguridad, es decir, el centro de datos. En esta área se encuentran los equipos del proveedor de internet. Desde este punto, se conectará el router principal del proveedor al switch, el cual distribuirá el servicio de internet y la red de datos a cada uno de los dispositivos en la Junta Cantonal, como equipos de cómputo, routers y cámaras de videovigilancia. Además, se llevará a cabo una reestructuración del cableado para los equipos, organizando de manera ordenada cada uno de los componentes principales de la red.



*Imagen 14. Sitio que nos servirá como DATA CENTER*

#### **4.4.3.2 Identificación e instalación de las cámaras de video vigilancia**

Asimismo, se identificó la ubicación de las cámaras de seguridad en sitios estratégicos que permitirán captar todos los detalles de las personas que ingresen al lugar, ya sean empleados de la Junta Cantonal o ciudadanos en general. Se determinaron cuatro ubicaciones para las cuatro cámaras de seguridad, y se procedió de inmediato a instalarlas en los lugares correspondientes.

Una vez instaladas las cámaras, se conectaron al DVR, que se ubicó en el centro de datos propuesto por el personal de la Junta Cantonal de Protección y Derechos en conjunto con el personal de Servicios Tecnológicos del GAD Municipal. Posteriormente, el DVR se conectó al switch principal, que a su vez se enlazó con el router principal, permitiendo la supervisión del sistema desde el edificio principal del GAD Municipal.



*Imagen 15. Cámara 1 - Patio de la Institución*



*Imagen 16. Cámara 2 - Oficinas Atención Ciudadana*



*Imagen 17. Cámara 3 - Ingreso principal*



*Imagen 18. Cámara 4 - Data Center*

Una vez ubicadas las cámaras, se procede con la ubicación del DVR en el DATA CENTER y la conexión de cada una de las cámaras hacia este dispositivo.



*Imagen 19. DVR de Cámaras*

#### 4.4.3.3 Configuración de DVR e identificación de las cámaras en el equipo

Posteriormente, se procedió con la configuración del DVR, asignándole una dirección IP estática dentro del rango designado para la red local, como se detalla en la Tabla 8 de este documento. De este modo, el equipo quedó conectado a la red, lo que permitió, mediante su dirección IP y MAC, otorgar los permisos necesarios y protegerlo de posibles ataques externos.

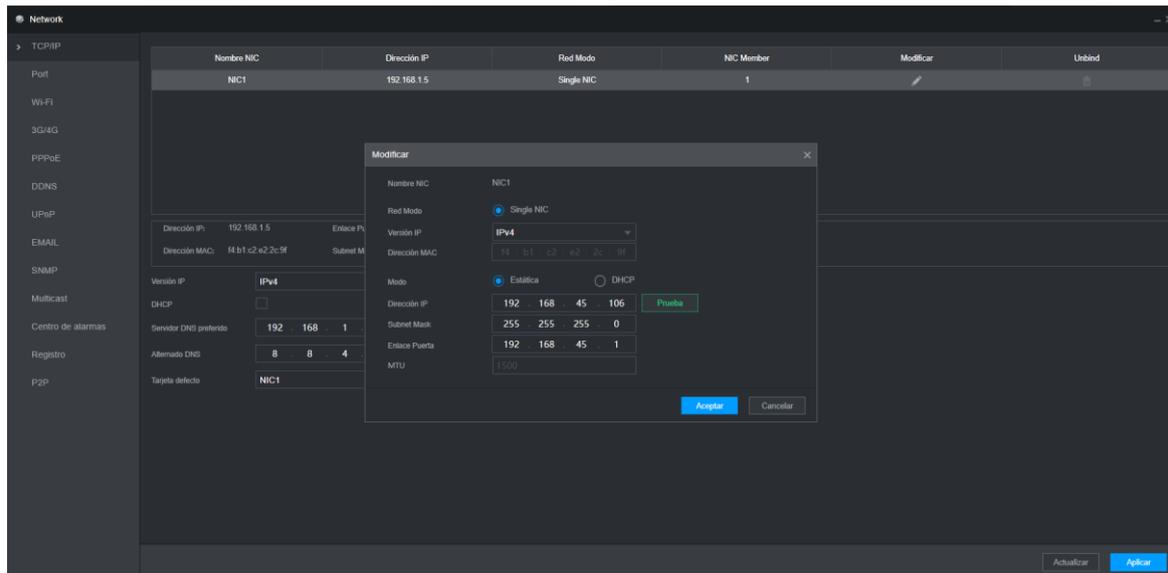
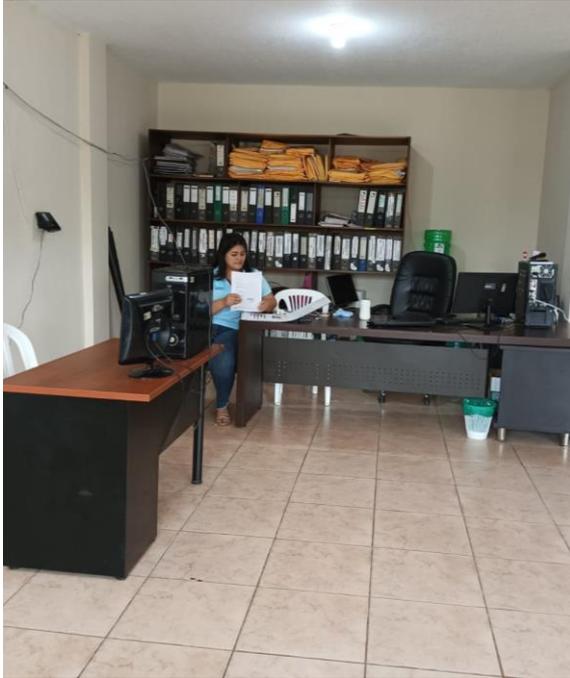


Imagen 20. Asignación de IP a DVR

#### 4.4.3.4 Instalación de los equipos informáticos de la junta cantonal

Una vez realizada esta conexión, se procedió a conectar cada uno de los equipos de cómputo a la red local. Para ello, se asignó una dirección IP estática a cada equipo, lo que permitió luego validar su IP y dirección MAC en el firewall, otorgándoles el permiso correspondiente.



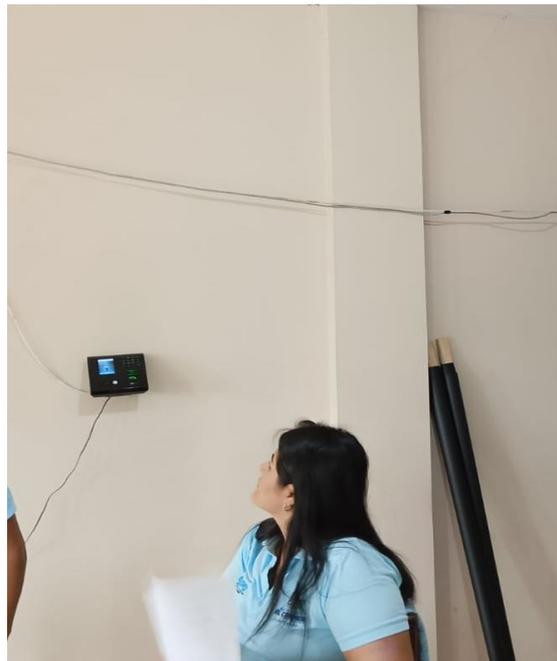
*Imagen 21. Equipos de Jefatura y Asistente*



*Imagen 22. Equipo Atención a Ciudadano*



*Imagen 23. Equipo de Recepción*



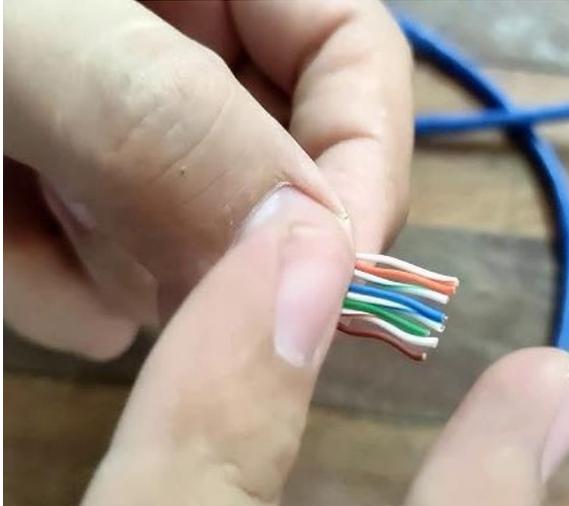
*Imagen 24. Reloj Biométrico*

#### **4.4.3.5 Ponchado de cables para el cableado estructurado**

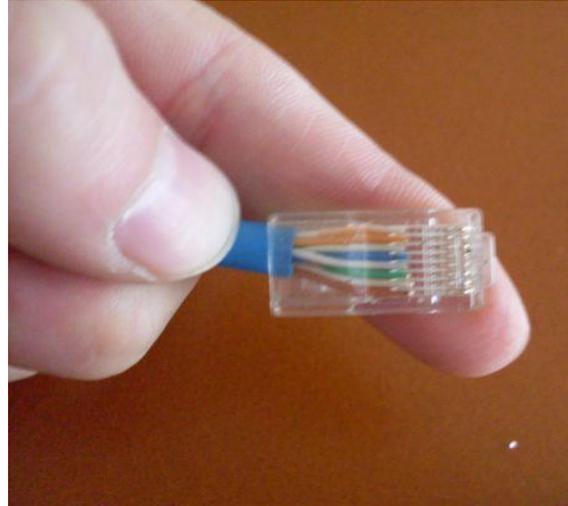
Se realizó el cableado estructurado para cada uno de los equipos basado en la norma TIA/EIA 568 conociendo que este es un proceso muy meticuloso el cual requiere mucha atención para poder garantizar una conexión fiable y de alta calidad, para este proceso utilizaremos cable de red par trenzado UTP Cat 6E, los terminales RJ45 Cat 6, herramienta de crimpado o ponchadora y una peladora de cables. Tomamos un extremo del cable y empezamos quitando la cubierta del cable aproximadamente 2 cm dejando expuestos los pares de hilos trenzados, desenrollamos y ordenamos los hilos bajo el estándar T568B de la siguiente forma:

1. Blanco/Naranja
2. Naranja
3. Blanco/Verde
4. Azul
5. Azul/Blanco
6. Verde
7. Café/Blanco
8. Café

Alineamos los hilos en el orden mencionado, enderezamos cada hilo para luego unirlos y cortarlos a una medida de 12mm, luego de insertamos los hilos en el conector asegurándonos de que cada hilo llegue al fondo del conector manteniéndose en el orden correcto. Una vez verificado que cada hilo esté en el orden correcto procedemos a utilizar la herramienta de ponchado presionando firmemente para asegurar que los contactos metálicos perforen el aislamiento de cada hilo realizando una buena conexión.



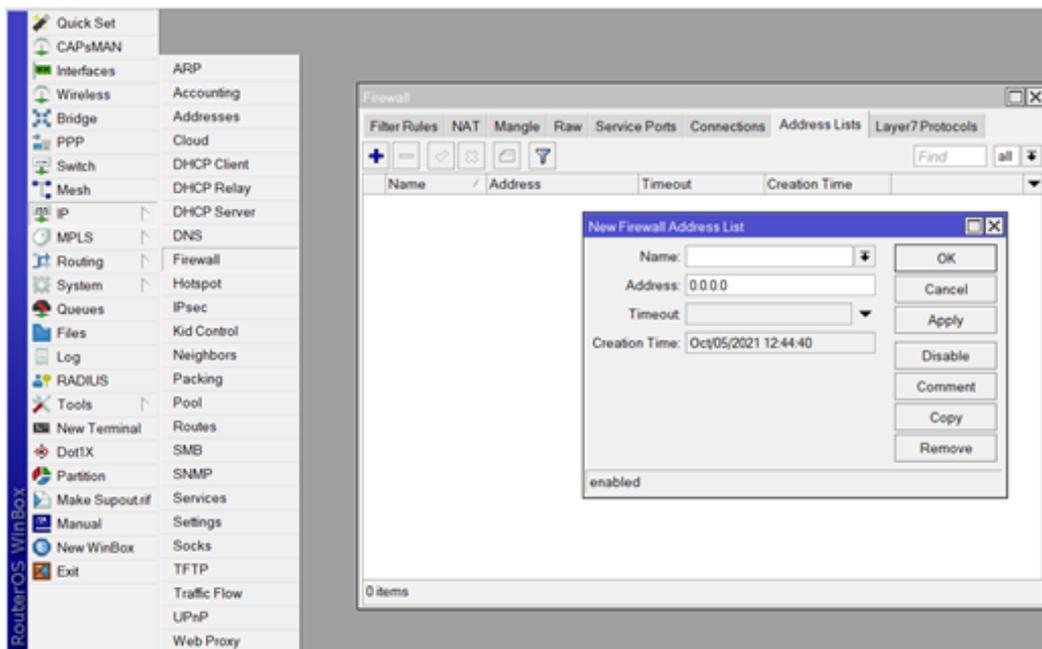
*Imagen 25. Ponchado de Cable UTP*



*Imagen 26. Cable Ponchado*

#### 4.4.3.6 Identificación de equipos e ingreso en el Firewall

Una vez ingresado cada uno de los equipos a la red local se procede ingresando al equipo router del proveedor de internet de Marca Mikrotik, para realizar la respectiva validación y proceder con la primera regla que es la de permitir únicamente el ingreso a la red de los equipos mencionados, así mismo para darle los permisos necesarios de navegación y de control por parte del administrador de red del GAD Municipal de El Carmen.



*Imagen 27. Creación de regla de ingreso de cada equipo*

En la imagen 27 podemos apreciar claramente la configuración de cada uno de los equipos que van a formar parte de la red de datos, para de esta forma solo estos equipos puedan tener acceso a la red y a los recursos de la red, equipo que no se encuentre registrado en esta regla del firewall, simplemente se le rechazará la conexión y no podrá entrar de ninguna forma.

#### 4.4.3.7 Creación de reglas para no permitir accesos no autorizados

Accedemos a la sección del Firewall, en el menú buscamos IP y luego Firewall, vamos añadir la regla correspondiente en la cadena Filter escogiendo la opción Filter Rules dando un clic en el botón con el signo (+), y en ese apartado configuramos la regla para permitir el tráfico a los usuarios con IP y MAC específicas, escogemos la opción forward e introducimos la IP y luego la MAC de cada uno de los equipos de la Institución, en la pestaña de acción escogemos la opción accept.

Para terminar con esta configuración añadimos otra regla para bloquear el tráfico a los demás, en la pestaña general escogemos la opción de forward y en la pestaña acción nos ubicamos en drop.

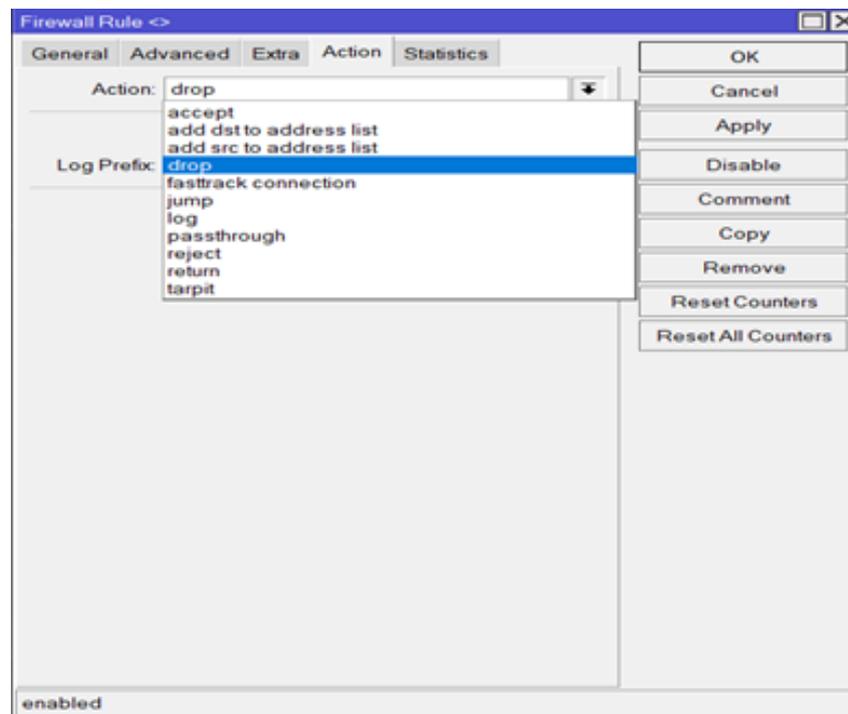
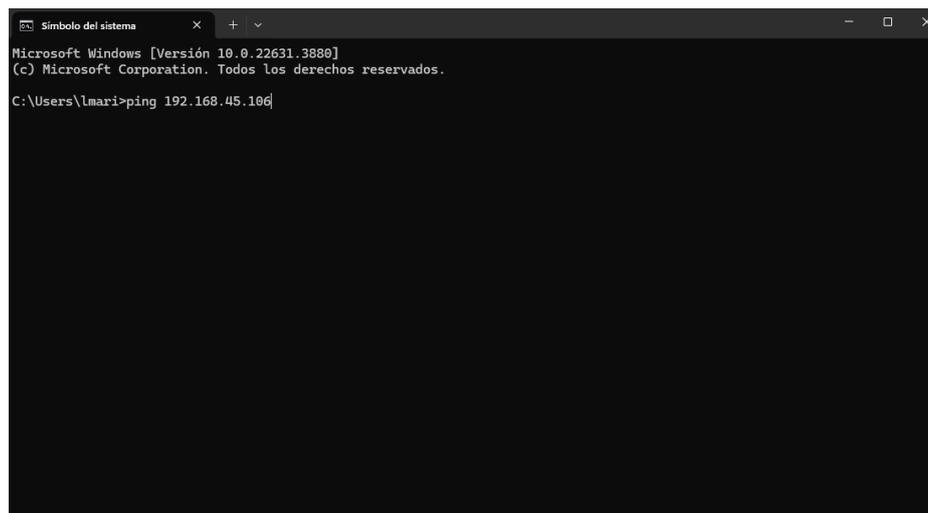


Imagen 28. Reglas de Firewall

#### 4.4.4 Verificación

Una vez instalado cada uno de los dispositivos se realizaron pruebas a la red utilizando la consola CMD de Windows, con ello se pudo evidenciar que la red si funciona y que hay conexión en cada uno de los equipos conectados a la red.

En la prueba realizada tomamos uno de los computadores conectados a la red y procedimos a abrir la consola de Windows presionando las teclas 'WIN + R' para abrir la ventana ejecutar, en ella escribimos 'cmd' y presionamos 'ENTER', una vez abierta la consola procedemos a utilizar el comando 'ping' seguido de la IP a la que vamos a verificar, para el primer caso realizamos una comprobación de red al DVR que posee la IP 192.168.45.106 para comprobar si el equipo está dentro de la red de datos

A screenshot of a Windows Command Prompt window. The title bar reads 'Símbolo del sistema'. The window content shows the following text: 'Microsoft Windows [Versión 10.0.22631.3888]', '(c) Microsoft Corporation. Todos los derechos reservados.', and 'C:\Users\lmari>ping 192.168.45.106'. The cursor is positioned at the end of the command line.

*Imagen 29. Comando ping*

Una vez ejecutado el comando adicionamos el modificador '-t' para que nos presente resultados extendidos, y para detener estos resultados continuos presionamos las teclas 'Ctrl + C'. Otra forma de tener paquetes fijos es utilizando el modificador '-n' seguido del número de paquetes que deseamos obtener

```
Símbolo del sistema
C:\Users\lmari>ping 192.168.1.5 -t

Haciendo ping a 192.168.1.5 con 32 bytes de datos:
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=3ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.5: bytes=32 tiempo=19ms TTL=64

Estadísticas de ping para 192.168.1.5:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 19ms, Media = 4ms
Control-C
^C
C:\Users\lmari>
```

*Imagen 30. comprobación exitosa*

En la misma consola de Windows ‘cmd’ se realizó otra prueba utilizando el comando ‘tracert’, esto con la finalidad de poder determinar la ruta de destino de los datos, para nuestra evaluación y verificación de resultados utilizamos el dominio de Google, al realizarlo nos muestra un rastreo completo del paso de los datos hacia su destino final, este comando también nos ayuda a verificar si existe un problema en la red y en donde exactamente se están quedando los paquetes de datos y resolver en el mismo instante.

```
Símbolo del sistema
C:\Users\lmari>tracert google.com

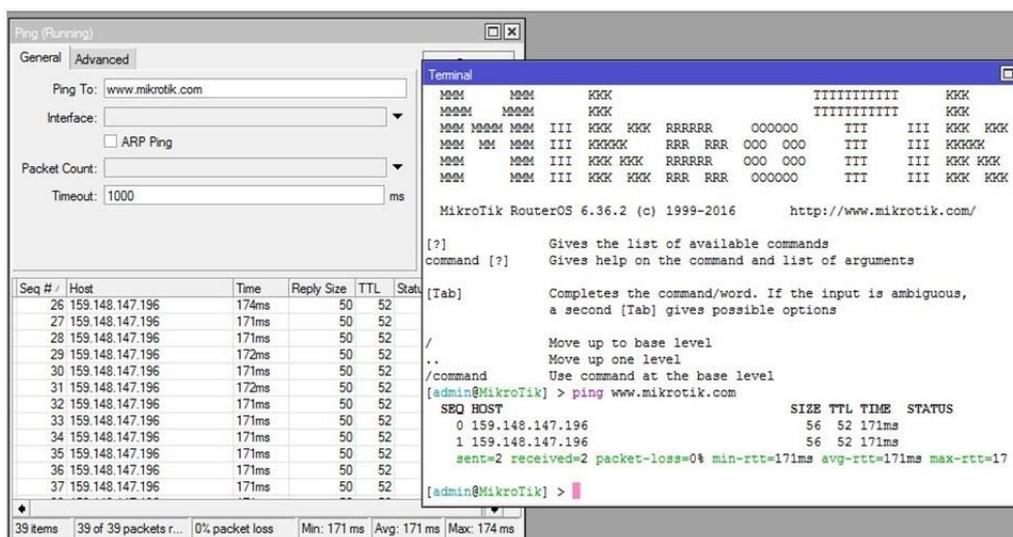
Traza a la dirección google.com [2800:3f0:4005:409::200e]
sobre un máximo de 30 saltos:

 1  *      *      *      Tiempo de espera agotado para esta solicitud.
 2  6 ms   3 ms   5 ms   2800:bf0:34e0:228::1
 3  8 ms   6 ms   8 ms   fc00:25:77:4001::1
 4  7 ms   7 ms   8 ms   fc00:25:78:4000::1
 5  7 ms   7 ms   6 ms   2800:2a0:21:10::1d
 6  23 ms  20 ms  20 ms  2800:2a0:21:10::1e
 7  23 ms  26 ms  21 ms  2800:2a0:21:10:1::7
 8  22 ms  21 ms  22 ms  2800:3f0:800f::1
 9  21 ms  20 ms  20 ms  2001:4860:0:1::3952
10  21 ms  20 ms  20 ms  2001:4860:0:1::8800
11  20 ms  20 ms  20 ms  2001:4860:0:1::3553
12  21 ms  29 ms  27 ms  2001:4860:0:1::4d93
13  21 ms  20 ms  20 ms  2800:3f0:4005:409::200e

Traza completa.
C:\Users\lmari>
```

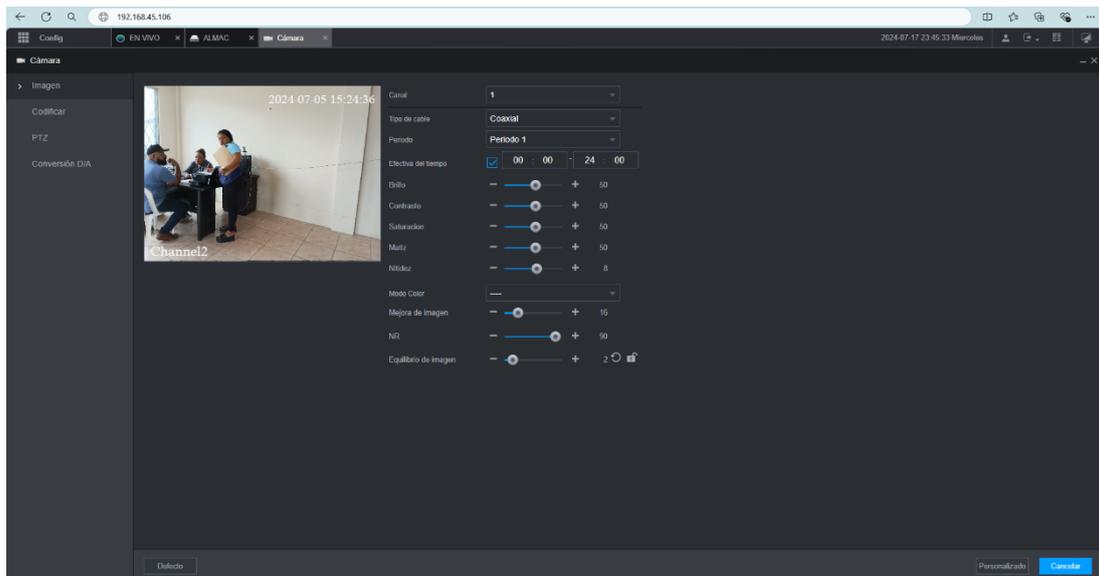
*Imagen 31. Comando tracert*

Una vez realizada la verificación de la red LAN en la Junta Cantonal de Protección y Derechos y determinar que todos los equipos estaban conectados a la misma sin novedad alguna, procedimos a dirigirnos hasta el GAD Municipal El Carmen, edificio principal, para verificar la conexión desde ese punto hasta la Junta Cantonal, prueba que la realizamos utilizando la consola terminal de Mikrotik desde uno de los computadores de la Unidad de Servicios Tecnológicos, utilizando la herramienta o aplicación ‘WinBox’. Ingresamos a la aplicación de winbox y en el menú principal ubicamos la opción ‘New Terminal’, una vez en la consola realizamos el mismo procedimiento como lo hicimos en la Junta Cantonal con la consola de Windows ‘cmd’. Al final de esto obtuvimos el resultado esperado de que si había conexión hacia el equipo que realizamos el ‘ping’. Del mismo modo con esta herramienta tan fundamental podemos hacer diagnósticos de red para así poder determinar y verificar la conectividad entre cada uno de los dispositivos que se encuentran conectados en la red.



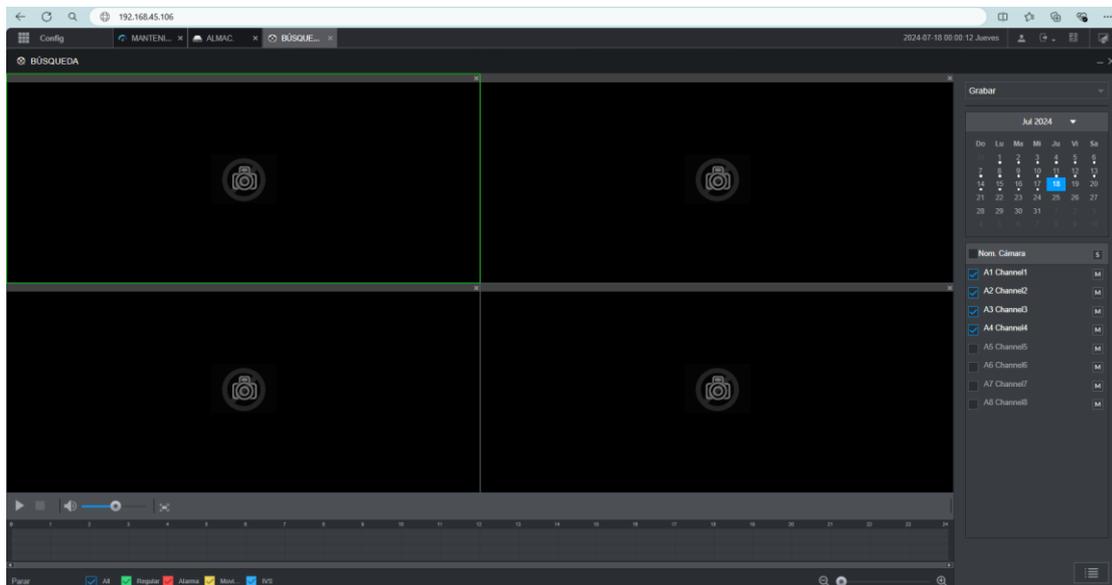
**Imagen 32. Consola Terminal de Winbox**

Una vez realizada con éxito las pruebas de red de los equipos conectados a la red de datos de la Junta Cantonal de Protección y Derechos, procedimos a revisar y configurar las cámaras de seguridad, empezamos con la resolución de cada una de ellas, dándole el brillo, contraste necesario para una excelente visualización desde el medio al que accedan a las mismas.



*Imagen 33. Verificación de video de cámaras*

De igual forma se hace la respectiva verificación de las grabaciones, para poder comprobar el estado de las mismas y del disco en el cual se están respaldando cada una de las imágenes. Se revisa en el día lo que ha grabado la cámara, así como también la calidad del video obtenido por el dispositivo.



*Imagen 34. Pruebas de Grabaciones de cámaras*

## **4.4.5 Mantenimiento**

### **4.4.5.1 Mantenimiento Preventivo**

El mantenimiento preventivo se lo debe realizar al menos 2 veces al año y en el mismo se deben realizar tareas o actividades tales como:

- Revisión de forma visual de cada uno de los cables de red y las conexiones como tal, con el fin de detectar posibles desgastes o daños.
- Realiza una verificación de la correcta operación de cada uno de los dispositivos que conforman la red de datos, desde los equipos de cómputo, hasta el switch y router principal.
- Se debe actualizar el firmware y el software de cada uno de los dispositivos de red y de igual forma a los de seguridad.
- Se debe de forma obligatoria realizar una limpieza en cada uno de los equipos que conforman la red y seguridad, para evitar la acumulación de polvo, humedad y suciedad.
- Revisión y optimización de las configuraciones de red y seguridad, todo esto con el fin de asegurar el mejor rendimiento de la red y proteger cada uno de los dispositivos.

### **4.4.5.2 Mantenimiento Correctivo**

Luego de realizar un mantenimiento preventivo y habiendo encontrado fallas en alguno de los dispositivos se debe realizar un mantenimiento correctivo considerando el siguiente procedimiento:

- Primeramente, identificamos el problema a través de los monitoreos realizados de manera constante.
- Se realizará un diagnóstico y a la vez una solución a los problemas de conectividad, del rendimiento y de seguridad que hayan ocurrido en cierto momento.
- Se realizará el reemplazo de cables, conectores, o de alguno de los dispositivos de red que esté presentando algún inconveniente.
- Se procederá a la reconfiguración de dispositivos y sistemas en caso de determinar fallas o cambios en los requerimientos de red de las configuraciones realizadas.

#### **4.4.5.3 Monitoreo continuo**

Para realizar un monitoreo continuo de la red de datos y sistema de seguridad se utilizarán herramientas de monitoreo de red tales como la aplicación WinBox de los dispositivos Mikrotik, además se utilizará la herramienta por defecto del sistema Operativo Windows, la consola de comandos 'cmd'.

Con estas herramientas realizaremos monitoreos al tráfico de la red y analizaremos los patrones que nos ayuden a identificar posibles amenazas o algún tipo de irregularidad. Además de esto se harán periódicamente revisiones de logs de seguridad y eventos para identificar y responder a incidentes de seguridad que se hayan presentado. Para finalizar se realizarán comprobaciones regulares del estado de los sistemas de respaldo y almacenamiento de datos de la red y del circuito de cámaras de video vigilancia.

#### **4.4.5.4 Documentación y reportes**

Para la documentación, se llevará a cabo una bitácora electrónica, en la que mantendrán detallados los registros de las actividades de cada uno de los mantenimientos, esta bitácora deberá incluir fechas, problemas detectados, acciones tomadas, y los resultados obtenidos de cada intervención. Además, se documentará cualquier tipo de cambio realizado en la red de datos y de cada uno de los dispositivos de seguridad, por más mínimo que sea.

En consecuencia, se levantarán también reportes, que no serán otra cosa que la elaboración de informes periódicos sobre el estado de la red y del sistema de seguridad, detallando antecedentes y culminando con las debidas recomendaciones para las mejoras y actualizaciones futuras. Este informe se procederá a entregarlo a la unidad de Servicios Tecnológicos de la Información y comunicación del GAD Municipal de El Carmen, para que el personal técnico esté informado sobre cualquier incidente significativo y las medidas tomadas que se dieron para resolver el problema.

## CAPÍTULO V

# 5 EVALUACIÓN DE RESULTADOS

## 5.1 Introducción

La implementación e instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, ha sido un paso muy crucial para la mejora de la eficiencia operativa y la seguridad de la información. Sin embargo, para asegurar que los objetivos del proyecto se han cumplido a carta cabal, es esencial realizar una evaluación de los resultados obtenidos. Esta evaluación no solo permitirá medir la efectividad de las soluciones implementadas, sino también identificar áreas de mejora y garantizar que las inversiones realizadas generen el objetivo esperado.

El proceso de evaluación principalmente se centró en varios aspectos claves que incluyen el acceso a la red de datos desde dispositivos no autorizados, la eficiencia en la compartición de recursos y documentos, la calidad del acceso a internet, y la comparación del rendimiento y seguridad de la red antes y después de la intervención. Mediante el uso de herramientas de monitoreo y la recopilación de datos precisos, se proporcionó una visión íntegra del impacto de cada una de las mejoras implementadas, así se demostró que la red anteriormente desorganizada y vulnerable ante cualquier ataque, ahora es una infraestructura robusta y segura, capaz de soportar las demandas operativas de los usuarios en cada una de sus actividades diarias en una forma mucho más efectiva y segura.

Esta evaluación de resultados, sirve además como un documento que al final validó el éxito de este proyecto, el mismo que orientará a futuras iniciativas de la Institución.

## 5.2 Presentación y monitoreo de resultados

### 5.2.1 Planificación de la evaluación

Una vez realizada la conexión de cada equipo al Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen,

es fundamental evaluar la efectividad del sistema implementado. Para ello, se analizará el acceso a la red desde dispositivos no autorizados en el área de trabajo, la compartición de recursos, documentos, y el acceso a internet, entre otros aspectos de la infraestructura. Esta evaluación permitirá compara la red anterior, con sus problemas y limitaciones, con la nueva red estructurada y segura

El resultado de esta comparación demuestra que la intervención en la red de datos anteriormente improvisada, ha transformado el sistema en una red bien estructurada y segura. Esto ha mejorado significativamente la productividad y efectividad de los usuarios en sus actividades diarias, facilitando el uso de los sistemas informáticos del GAD Municipal y gubernamental.

## **5.2.2 Ejecución del monitoreo**

Para llevar a cabo la ejecución del monitoreo de la Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, seguiremos el siguiente procedimiento:

### **5.2.2.1 Planificación del monitoreo**

Para empezar con la planificación del monitoreo debemos tener primeramente los objetivos claros, es decir definir a principio de cuentas como garantizar la seguridad de la información, como vamos a optimizar el rendimiento y al final como vamos a detectar cada uno de los problemas. Luego de tener nuestros objetivos claros, seleccionaremos las herramientas y el software necesario para realizar el monitoreo (consola de Windows, terminal de winbox, speedtest). Al final de nuestra planificación tendremos que definir indicadores de rendimiento KPIs (Key Performance indicator), que nos permitan evaluar el desempeño de nuestro sistema de seguridad.

### **5.2.2.2 Configuración de las herramientas de monitoreo**

Nuestro primer paso será instalar las herramientas de monitoreo, en nuestro caso instalaremos la aplicación winbox, la misma que descargaremos de la página oficial de Mikrotik y la segunda herramienta ya conocida como terminal de Windows o cmd que viene incluida en el

Sistema Operativo Windows de Microsoft. Desde un browser o navegador abriremos la aplicación de speedtest, el cual me permitirá medir el ancho de banda que utiliza cada equipo de la red, evaluando si la repartición de este recurso funciona adecuadamente.

### **5.2.2.3 Monitoreo activo y pasivo**

Como parte del monitoreo activo realizaremos pruebas de manera periódica en la consola de Windows, tales como pings, tracerts, igualmente realizaremos pruebas de conectividad para poder verificar el estado de la red.

Como parte del monitoreo pasivo analizaremos el tráfico de la red y cada uno de los logs de eventos, que nos permitirán identificar comportamientos inusuales en la red como también posibles amenazas.

### **5.2.2.4 Evaluación del acceso a la red**

Realizamos una simulación de acceso no autorizado con el único objetivo de evaluar la efectividad de las medidas de seguridad, intentando acceder a la red desde un dispositivo desconocido. Conectamos un computador portátil con un patch cord directamente al Switch principal donde están conectados todos los equipos de la red, el equipo no se pudo conectar a la red ya que la misma por DHCP o IP dinámica asignaba valores desconocidos para poder conectarse a la red, lo que comúnmente llamamos basura. Luego de esto revisamos en otro equipo el rango de IP de la red y asignamos una IP estática a nuestro equipo de prueba, el equipo se conectó a la red por la IP asignada, pero el mismo no tenía acceso a la misma, ya al realizar un ping a uno de los equipos o al equipo principal los pines salían ‘tiempo de espera agotado’, en conclusión, este equipo no se pudo conectar a nuestra red de datos, ni pudo acceder a la información del resto de equipos.

Dado este tema pudimos asegurarnos de que las políticas de seguridad implementadas en el Firewall tales como el control de acceso (ACLs), está correctamente implementada y que funciona perfectamente.

### **5.2.2.5 Monitoreo de recursos compartidos**

Para este proceso realizamos primeramente la compartición de dispositivos en la red, al escoger un equipo que tenía conectado una impresora por medio de cable USB, y la misma solo operaba para ese computador. Como el computador si está en la red accedimos a él y compartimos ese recurso, al momento de ser compartido pudimos acceder sin problema desde otro equipo de la red y realizamos una conexión hacia este dispositivo, el resultado es que desde el otro dispositivo ya tuvimos conexión hacia la impresora realizando una impresión de prueba, la misma que fue todo un éxito, de este modo ya los usuarios podían hacer uso de este recurso compartido desde sus equipos, ya que anteriormente grababan la información o la pasaban por correo para que el compañero que tenía la impresora les haga el trabajo de imprimir el documento.

Lo segundo que realizamos es evaluar la capacidad de compartir recursos, tales como carpetas o archivos desde un equipo a otro, este proceso lo realizamos desde el equipo de la jefatura el cual contenía una carpeta en la que se guardaban documentos que necesitan tanto la jefa como la asistente de la misma. Se procedió a compartir esta carpeta dando único acceso al equipo de la asistente de jefatura para que pueda acceder a la misma y hacer uso de los archivos que se encontraban en ella. Al dar solo acceso a este equipo verificamos si algún otro equipo de la red podía tener acceso al mismo y nos dimos cuenta que no, ya que el mismo no tenía los permisos del administrador, de este modo se pudo apreciar que los recursos compartidos están protegidos contra accesos no autorizados.

### **5.2.2.6 Monitoreo del acceso a internet**

Para este proceso lo primero que se realizó es asegurarse que todos los equipos de la red tengan acceso a internet según las políticas establecidas. Revisamos uno a uno los equipos del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, y todos navegaron sin novedad alguna. Luego de verificar que cada uno de los equipos navegue en internet, se realizó un monitoreo del tráfico de internet para poder de una u otra forma detectar posibles amenazas además de verificar el uso adecuado de los recursos. Para esta verificación utilizamos la herramienta winbox, que nos permite realizar monitoreo de tráfico en la red y en cada una de las IPs conectadas al equipo principal.

Así mismo se realizaron descargas de archivos y visualización de videos, todo esto con el fin de verificar el ancho de banda asignado a cada equipo, en la red anterior no se tenía esta regla implementada, y cuando uno de los equipos hacía mal uso de los recursos, los demás equipos de la red se quedaban limitados de poder navegar con fluides, teniendo problemas de intermitencia y en ocasiones quedarse sin servicio, provocando desgaste en el personal técnico porque tenían que dirigirse al sitio a resolver un problema técnico provocado por otro equipo en la red.

#### **5.2.2.7 Análisis y comparación**

Para poder realizar la parte de análisis y comparación lo primero que se hizo es la recopilación de datos con las herramientas de monitoreo utilizadas para el efecto durante un periodo definido por nosotros. Luego de esto se realizó el análisis de los datos recogidos con el fin de identificar patrones, como por ejemplo problemas de navegación e identificar directamente las áreas de mejora para el problema encontrado.

Una vez obtenido estos resultados se realizó una comparación con la red anterior, para poder evaluar cada una de las mejoras y los beneficios obtenidos con la nueva red de datos, teniendo resultados que sobrepasaron las expectativas de cada uno de los usuarios del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen.

#### **5.2.2.8 Mantenimiento Continuo**

Para efectos de una buena conectividad a largo plazo se debe realizar un monitoreo continuo de la red, estableciendo un programa o aplicación para tal efecto y de esta forma poder asegurar que la red y los sistemas de seguridad sigan funcionando de manera óptima y eficaz. Además de esto se deben realizar actualizaciones y ajustes en las configuraciones y reglas del firewall de forma periódica según sea necesario.

#### **5.2.2.9 Revisión periódica**

Para mantener un servicio y una red en buen estado se requiere de revisiones regulares, es decir que tenemos que dejar programado revisiones para evaluar la efectividad del monitoreo y con esto realizar mejoras continuas en nuestro sistema de seguridad.

Y para complementar los buenos resultados de nuestra red de datos se debe asegurar que el personal que labora en el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, tiene que estar plenamente capacitado sobre el uso de cada una de las herramientas de monitoreo y en la identificación de amenazas potenciales, a más de también conocer el manejo de los recursos compartidos y el uso adecuado del internet.

### **5.3 Interpretación objetiva**

Una vez realizada la Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, se realizó una evaluación detallada, que nos permitió medir la efectividad de cada una de las mejores realizadas e implementadas. Los resultados que se obtuvieron en conjunto con personal de la Institución dieron claramente una visión de los desafíos y beneficios con la nueva red de datos.

#### **5.3.1 Acceso a la red desde dispositivos no autorizados**

Al realizar esta evaluación, el resultado obtenido por la misma reveló una gran mejora en la seguridad de datos ya que cada intento de acceso desde dispositivos que no se encontraban autorizados fueron efectivamente bloqueados sin permitir el ingreso a la red, resaltando en sí que las medidas de autenticación e ingreso a la red que fueron implementadas son robustas. El resultado obtenido demostró que la red de datos de la institución está mejor protegida contra las posibles amenazas de intrusos y de cualquier acceso no deseado.

#### **5.3.2 Compartición de recursos y documentos**

De igual forma se realizaron pruebas con la compartición de recursos tecnológicos, tales como impresoras y la de documentos desde cada uno de los dispositivos de la red, el mismo que se ha optimizado considerablemente, ya que antes de la intervención, los usuarios del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, experimentaban muchas dificultades, además de lentitud en la transferencia de archivos y el uso compartido de equipos de impresión y otros periféricos. Con la implementación y esta nueva estructura de red, las tareas que realizan cada uno de los

usuarios son de forma más fluida y eficiente, mejorando notablemente la colaboración y productividad del personal que labora en la institución.

### **5.3.3 Acceso a internet**

El uso y el acceso al internet de cada uno de los usuarios ha mostrado una gran mejora en términos de velocidad y estabilidad, ya que anteriormente los usuarios reportaban frecuentemente la intermitencia y lentitud en la conexión, haciéndose imposible la atención rápida a los ciudadanos. La nueva conexión de la red y la excelente distribución de los recursos, en este caso el ancho de banda suministrado hacia esta entidad, ha reducido estos problemas, permitiendo una navegación más rápida sin interrupciones y por lo más confiable, lo cual es crucial y oportuno para el buen desempeño de las diversas tareas administrativas y operativas realizada por cada uno de los usuarios de la institución.

### **5.3.4 Comparación de rendimiento y seguridad de la red**

Comparando la situación actual del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, antes de la intervención a la red de datos, se observa una notable transformación, ya que la red solía estar completamente desorganizada y siempre propensa a fallos sobre todo de seguridad, actualmente la misma es estructurada y completamente segura a cualquier tipo de ataques. Actualmente los usuarios reportan una notable mejoría en su productividad y una completa reducción a problemas técnicos diarios ya que la estructura ordenada de la red aparte de facilitar la gestión de cada proceso facilita también el mantenimiento a la misma, reduciendo de forma considerable el tiempo y los recursos necesarios para la resolución de problemas.

### **5.3.5 Circuito cerrado de cámaras de video vigilancia**

Dentro de uno de los grandes objetivos de nuestro proyecto estaba la implementación de cámaras de video vigilancia para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, ya que en la misma no habían estos necesarios equipos que permiten salvaguardar la integridad de cada uno de los usuarios y de cada uno de los bienes que se encuentran dentro de la institución, y porque no decir de la integridad de cada uno de los ciudadanos que llegan a la institución por algún trámite. Los usuarios de la institución una vez ubicado estas cámaras, se sienten más seguros

de desempeñar cada una de sus actividades sin temor a nada, ya que ellos mismos cuentan que antes de tener estos dispositivos sufrieron varios atentados, entre los cuales hubieron perdida de pertenencias y equipos de la institución, las mismas que ya cuentan con denuncias a la fiscalía del cantón. El circuito de cámaras de video vigilancia se encuentra trabajando de forma óptima ya que se encuentra dentro de la red y es imposible el ingreso a la misma si no se encuentra autorizado.

### **5.3.6 Productividad y efectividad**

La Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 para el Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, ha tenido un impacto realmente positivo en la productividad y efectividad de todos los usuarios de la institución al poder utilizar de forma fluida y sin problemas los sistemas del GAD Municipal y de los sistemas de cada una de las entidades gubernamentales. La red estructurada actual ha eliminado muchos de los obstáculos que antes interferían con el trabajo que llegaba a diario, permitiendo actualmente a cada uno de los funcionarios públicos que ahí laboran, realizar sus tareas con mayor rapidez y sobre todo con mucha eficiencia.

## CAPÍTULO VI

### 6 CONCLUSIONES Y RECOMENDACIONES

#### 6.1 Conclusiones

Se identificaron y analizaron detalladamente los fundamentos teóricos que sustentan el proyecto del sistema de seguridad de red con cableado estructurado. Esto incluyó la revisión de estándares como la Norma TIA/EIA 568-B, la vinculación con el proveedor de servicios de Internet, la conexión de equipos de red y cámaras, y las características técnicas de los dispositivos. Estos análisis proporcionaron una base sólida para el diseño e implementación del sistema, asegurando que se cumplan los requisitos técnicos y de seguridad necesarios para proteger la infraestructura de la institución.

El diagnóstico realizado reveló importantes deficiencias en la seguridad de la información, tanto en términos de infraestructura como de procedimientos. Se detectaron vulnerabilidades en la red existente y una falta de políticas claras de seguridad, lo cual representaba un riesgo significativo para los bienes, usuarios y la ciudadanía en general. Este diagnóstico fue crucial para identificar las áreas críticas que requerían mejoras inmediatas, lo que guió el diseño del nuevo sistema de seguridad.

Se diseñó un sistema integral que combina la protección de la red de datos con un circuito cerrado de videovigilancia, enfocado en salvaguardar tanto la integridad de las personas como la seguridad de la información y los bienes institucionales. Este diseño incluyó la implementación de tecnologías avanzadas como firewalls, cámaras de alta resolución y sistemas de almacenamiento seguro. El enfoque en la seguridad integral permitió crear un entorno más seguro y confiable para todas las operaciones del GAD Municipal de El Carmen.

La implementación del sistema de seguridad no solo mejoró significativamente la seguridad interna y externa de la institución, sino que también facilitó la detección e identificación de incidentes en la red, reduciendo la exposición a ciberataques y accesos no autorizados. El análisis posterior a la implementación demostró que el sistema no solo cumplió con los objetivos de proteger a la institución y a sus usuarios, sino que también generó beneficios

tangibles en términos de confianza y eficiencia operativa, contribuyendo al bienestar de la ciudadanía en general.

En definitiva la Instalación de Sistema de Seguridad de Redes con cableado estructurado basado en la norma TIA/EIA 568 ha transformado la infraestructura tecnológica del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen, esta nueva estructura ha solucionado de gran forma los problemas de desorganización y la falta de seguridad informática que existía con la red anterior, actualmente esta red proporciona una base sólida y completamente segura para una operación diaria.

## **6.2 Recomendaciones**

Es fundamental mantener cada uno de los equipos tecnológicos debidamente actualizados, para de esta forma poder asegurar un desempeño óptimo y una mayor seguridad. Se recomienda realizar evaluaciones periódicas de la infraestructura tecnológica y planificar actualizaciones de hardware y software de forma regular.

De igual forma mantener la implementación de programas de capacitación continua en tecnologías y seguridad de la información para todos los funcionarios públicos. La formación constante de los funcionarios asegura que los mismos estén al tanto de las últimas prácticas y herramientas, para así poder reducir riesgos de errores humanos, mejorando notablemente la eficiencia en el uso de cada uno de los sistemas informáticos.

Así mismo se sugiere realizar mantenimientos periódicos de la red y de cada uno de los sistemas de seguridad para poder prevenir errores y mantener la infraestructura en óptimas condiciones. Recomendar el uso de la bitácora electrónica y la actualización de la misma en cada una de las intervenciones que se den en la red de datos, documentando cada problema detectado, las acciones que fueron tomadas y al final los resultados que se obtuvieron.

El llevar a cabo evaluaciones periódicas de seguridad, que al final permitirá identificar vulnerabilidades potenciales, asegura de que las medidas de prevención implementadas sean

efectivas. Cada evaluación realizada deberá incluir pruebas de penetración y auditorías de seguridad para poder garantizar la integridad de los datos y salvaguardar la información de la institución protegiéndola sobre todo de ciberataques.

Fomentar una cultura de manera continua en la gestión de la red y los sistemas de seguridad implementados, esto implica siempre estar atentos a las actualizaciones tecnológicas y a las buenas prácticas que puedan ser implementadas en aras de mejorar la eficiencia y la seguridad de la infraestructura tecnológica del Sistema Cantonal de Igualdad y Protección Integral de Derechos de los grupos de Atención Prioritaria del Cantón El Carmen.

Establecer canales de comunicación efectivos entre el personal técnico del GAD Municipal El Carmen y los funcionarios públicos de la institución, para poder asegurar que cualquier problema o necesidad sea atendido de forma oportuna e inmediata. La colaboración entre diferentes áreas del GAD Municipal es clave para mantener un entorno tecnológico robusto y sobre todo seguro.

# BIBLIOGRAFÍA

## 7 Bibliografía

Alegsa, L. (2015). *Definición de la red de computadoras*. Obtenido de <http://www.alegsa.com.ar/Dic/red%20de%20computadoras.php>

Alonso, F. (2005). *Introducción a la Ingeniería de Software*. Publicaciones Delta.

Amo, M. O. (2013). *Sociedad Red: Estado, Economía y Sociedad en la era de la Información*. Barcelona: UOC.

Angel, V. C. (2017). Seguridad y control del acceso a las redes inalámbricas en la UNSM-T mediante servidores de autenticación Radius con el uso de certificados digitales. 65.

Briceño, E. V. (2021). *Seguridad de la Información*. Área de innovación y desarrollo.

Comer, D. E. (2015). *Computer Networks and Internets*.

Dandy, L. T. (2020). Comparativa de las metodologías Magerit y Octave, para determinar la más adecuada. Perú.

Dario, A. G. (2023). *El ABC de la seguridad informática: guía práctica para entender la seguridad digital*.

Fernando Patricio, G. V. (2021). DISEÑO DE UNA RED INTEGRAL DE TELECOMUNICACIONES SEGÚN LAS NORMAS ANSI/TIA/EIA 568 C, 569C, 606 B, 607 B PARA EL INSTITUTO TÉCNICO TECNOLÓGICO SUPERIOR “COTACACHI” (ITTS). Ibarra.

Group, O. C. (2022). *¿POR QUÉ ES NECESARIO ACTUALIZAR LA RED DEL DATA CENTER Y CÓMO?* Obtenido de <https://www.orbit.es/por-que-es-necesario-actualizar-la-red-del-data-center/>

Han, J. (2016). *Data Mining: Concepts and Techniques*. Illinois.

- Hinojosa, L. (2010). *Evolución de las redes de computadoras*. Obtenido de <http://es.slideshare.net/efracbtis/evolucion-de-redes-de-computadoras>
- Informática, A. (2021). *¿Qué es el cableado de red y qué tipos existen?* Obtenido de <https://www.aurum-informatica.es/blog/cableado-de-red-tipos>
- Juni, J., & Urbano, C. (2003). Técnicas para investigar, recursos metodológicos para la preparación de proyectos de investigación. *Córdoba: Ed. Brujas. Vol. 1.*
- Kurose, J. F. (2016). *Redes de Computadoras, un enfoque descendente*.
- Monge, M. C. (2023). *Bases de Datos Avanzadas e Ingeniería del Software*. Madrid: Ra-Ma.
- Morales, E. C. (2014). *Guía para aplicar la norma TIA/EIA 568 para cableado estructurado*. Obtenido de <https://tabasco.gob.mx/sites/default/files/Manual-para-aplicar-la-norma-TIA-EIA-para-Cableado-Estructurado.pdf>
- Ortega, C. (2024). *Investigación aplicada: Definición, tipos y ejemplos*. Obtenido de <https://www.questionpro.com/blog/es/investigacion-aplicada/>
- Ortiz, B. L. (2018). La Criptografía como elemento de la seguridad informática. 14.
- RedHat. (2022). *¿Qué es la gestión de los datos?* Obtenido de <https://www.redhat.com/es/topics/data-services/what-is-data-management>
- Tanenbaum, A. S. (2012). *"Computer Networks" (Redes de Computadoras)*. Washington.

## ANEXOS

### Anexo A: Asignación de tutor

#### *Anexo A: Asignación de tutor*



**Universidad Laica Eloy Alfaro de Manabí**

---

**Periodo 2023-2024(2) - Notificación de tutor asignado -  
TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)**

---

Estimad@  
Docente y Estudiante  
Uleam

En cumplimiento de lo establecido en la Ley, el Reglamento de Régimen Académico y las disposiciones estatutarias de la Uleam, por medio de la presente se oficializa la dirección y tutoría en el desarrollo del Trabajo de Integración Curricular del siguiente estudiante:

**Tema:** SISTEMA DE SEGURIDAD DE RED CON CABLEADO ESTRUCTURADO BASADO EN LA NORMA TIA/EIA 568 PARA EL SISTEMA CANTONAL DE IGUALDAD Y PROTECCIÓN INTEGRAL DE DERECHOS DE LOS GRUPOS DE ATENCIÓN PRIORITARIA DEL CANTÓN EL CARMEN.

**Estado de aprobación:** Aprobado

**Tipo de titulación:** Trabajo de Integración Curricular

**Tipo de proyecto:** Trabajo de Integración Curricular se articula con proyectos y programas de Investigación.

**Apellidos y nombres del tutor asignado:** MINAYA MACIAS RENELMO WLADIMIR

**Apellidos y nombres del estudiante:** DE LA A BRIONES LUIS MARIO

**Carrera:** TECNOLOGÍAS DE LA INFORMACIÓN 2022 (EL CARMEN)

**Periodo de inducción:** Periodo 2023-2024(2)

Sírvase(n) cumplir con lo dispuesto en el Manual de Procedimientos de TITULACIÓN DE ESTUDIANTES DE GRADO BAJO LA UNIDAD DE INTEGRACIÓN CURRICULAR: <https://departamentos.uleam.edu.ec/gestion-aseguramiento-calidad/files/2023/04/Titulacion-de-Est.-Grado-Bajo-la-Unidad-Integr.-Curri.-V.2-1-1.pdf>.

Particular que se informa para los fines consiguientes.

Atentamente,

Comisión Académica y Responsable de Titulación.

## Anexo B: Certificado de la empresa

### Anexo BB: Certificado de la empresa



SISTEMA CANTONAL DE PROTECCIÓN INTEGRAL DE DERECHOS DE LOS GRUPOS DE ATENCIÓN PRIORITARIA UR

Yo, María Eugenia Rodríguez Acosta,  
Responsable del Sistema Cantonal de Protección de Derechos,

## CERTIFICO

Que el Sr. Luis Mario De La A Briones, con cédula Id. 0918021999, ha culminado con éxito la implementación del proyecto de titulación, titulado "SISTEMA DE SEGURIDAD DE REDES CON CABLEADO ESTRUCTURADO BASADO EN LA NORMA TIA/EIA 568 PARA EL SISTEMA CANTONAL DE IGUALDAD Y PROTECCIÓN INTEGRAL DE DERECHOS DE LOS GRUPOS DE ATENCIÓN PRIORITARIA DEL CANTÓN EL CARMEN".

Este proyecto ha sido debidamente evaluado y se encuentra actualmente en funcionamiento, siendo utilizado tanto por el personal que labora en la institución como por la ciudadanía en general que a diario nos visita. Consideramos que esta iniciativa representa una valiosa contribución al desarrollo institucional y tecnológico para el beneficio de la ciudadanía en general y de los funcionarios de la institución.

La presente se firma a los 19 días de julio del 2024

Atentamente,

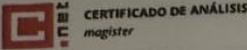


Sra. María Eugenia Rodríguez Acosta.  
SECRETARIA EJECUTIVA DEL SCIPID.  
Contacto: 0991172770  
C.I: 1712002391  
Correo: [maria.rodriguez@hotmail.es](mailto:maria.rodriguez@hotmail.es) / [maria.rodriguez@redmuc.gob.ec](mailto:maria.rodriguez@redmuc.gob.ec)

*"Sistema Cantonal de Protección de Derechos trabajando por los Grupos de Atención"*

# Anexo D: Reporte del sistema antiplagio

## Anexo AAA: Reporte del sistema antiplagio



### TESIS LMDB ULTIMA PARA ANTIPLAGIO

5%

Textos sospechosos

4% Similitudes  
< 1% similitudes entre comillas  
 0% entre las fuentes mencionadas

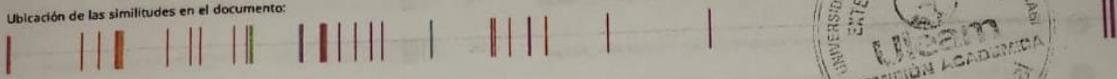
Δ < 1% Idiomas no reconocidos

Nombre del documento: TESIS LMDB ULTIMA PARA ANTIPLAGIO.docx  
 ID del documento: e05f5d1cb9593ec0d6e8232d6fd4fbc04d0cd1e  
 Tamaño del documento original: 3,58 MB

Depositante: RENELMO MINAYA MACIAS  
 Fecha de depósito: 5/8/2024  
 Tipo de carga: interface  
 fecha de fin de análisis: 5/8/2024

Número de palabras: 20.718  
 Número de caracteres: 132.568

Ubicación de las similitudes en el documento:



**Fuentes principales detectadas**

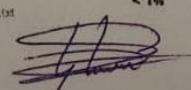
N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<a href="http://eprints.rcdis.org/5034/1/criptografia.pdf">eprints.rcdis.org</a> 2 fuentes similares	< 1%		Palabras idénticas: < 1% (135 palabras)
2	<a href="http://repositorio.utn.edu.ec/bitstream/123456789/4720/7/05_FECYT_2291_TRABAJO_GRADO.pdf.txt">repositorio.utn.edu.ec</a> 5 fuentes similares	< 1%		Palabras idénticas: < 1% (105 palabras)
3	<a href="http://dspace.unach.edu.ec/bitstream/51000/4121/1/UNACH-EC-FCP-DER-2017-0061.pdf">dspace.unach.edu.ec</a>	< 1%		Palabras idénticas: < 1% (96 palabras)
4	<a href="https://dspace.uniandes.edu.ec/bitstream/123456789/810/1/TUPDER002-2015.pdf">dspace.uniandes.edu.ec</a> 4 fuentes similares	< 1%		Palabras idénticas: < 1% (89 palabras)
5	Documento de otro usuario #313ca7 El documento proviene de otro grupo 3 fuentes similares	< 1%		Palabras idénticas: < 1% (83 palabras)

**Fuentes con similitudes fortuitas**

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	Trabajo de titulación Kevin Tipán correccion final 1.docx   Tesis Kevin Tipán #0x357a El documento proviene de mi grupo	< 1%		Palabras idénticas: < 1% (40 palabras)
2	<a href="https://saquisil.gov.ec/wp-content/uploads/2019/03/ordenanza-de-creacion-del-sistema-cantonal-d...">saquisil.gov.ec</a>	< 1%		Palabras idénticas: < 1% (40 palabras)
3	P-I-Pablo Navarrete 1.docx   P-I-Pablo Navarrete 1 #0935ce El documento proviene de mi biblioteca de referencias	< 1%		Palabras idénticas: < 1% (20 palabras)
4	<a href="https://repositorio.utmachala.edu.ec/bitstream/48000/20242/1/TT_MATAILOJENNIFER_041.pdf">repositorio.utmachala.edu.ec</a>	< 1%		Palabras idénticas: < 1% (37 palabras)
5	<a href="http://repositorio.utc.edu.ec/bitstream/27000/4618/3/PIM-000107.pdf.txt">repositorio.utc.edu.ec</a>	< 1%		Palabras idénticas: < 1% (38 palabras)

**Fuentes Ignoradas** Estas fuentes han sido retiradas del cálculo del porcentaje de similitud por el propietario del documento.

N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	<a href="https://www.gob.ec/index.php/gad-carmen/framiles/proteccion-integral-derechos-grupos-atencion...">www.gob.ec</a>   Protección Integral de derechos de los grupos de atención prioritari... 3%	3%		Palabras idénticas: 3% (560 palabras)
2	<a href="https://www.gob.ec/sites/default/files/signipprocedure-14210-20220606151515-14533546-signed.pdf">www.gob.ec</a>	3%		Palabras idénticas: 3% (560 palabras)
3	Documento de otro usuario #7e3a29 El documento proviene de otro grupo	3%		Palabras idénticas: 3% (558 palabras)
4	<a href="http://esacc.corteconstitucional.gob.ec/storage/app/media/1/10_DWL_FU/eyjYXWZXRhIjoiYmRlY2U1dWki...">esacc.corteconstitucional.gob.ec</a>	2%		Palabras idénticas: 2% (295 palabras)
5	<a href="https://elcarmen.gob.ec/2023/07/20/el-sistema-cantonal-de-proteccion-de-derechos-trabaja-en-ben...">elcarmen.gob.ec</a>   EL SISTEMA CANTONAL DE PROTECCIÓN DE DERECHOS TRABAJA... 1%	1%		Palabras idénticas: 1% (252 palabras)
6	<a href="http://repositorio.ucsg.edu.ec/bitstream/3317/16448/8/1-UCSG-POS-MDC-200.pdf.txt">repositorio.ucsg.edu.ec</a>	< 1%		Palabras idénticas: < 1% (168 palabras)



N°	Descripciones	Similitudes	Ubicaciones	Datos adicionales
7	<a href="http://www.loja.gob.ec">www.loja.gob.ec</a> <a href="https://www.loja.gob.ec/files/documentos/2014-10/ord_sistema_igual_y_proteccion_personas_y_gn...">https://www.loja.gob.ec/files/documentos/2014-10/ord_sistema_igual_y_proteccion_personas_y_gn...</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (168 palabras)
8	Documento de otro usuario El documento proviene de otro grupo	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (179 palabras)
9	<a href="http://scielo.sld.cu">scielo.sld.cu</a>   La Criptografía como elemento de la seguridad informática <a href="http://scielo.sld.cu/scielo.php?script=sci_arttext&amp;pid=S1024-94352003000600012">http://scielo.sld.cu/scielo.php?script=sci_arttext&amp;pid=S1024-94352003000600012</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (135 palabras)
10	<a href="http://repositorio.puce.edu.ec">repositorio.puce.edu.ec</a> <a href="http://repositorio.puce.edu.ec/bitstream/22000/7022/5/12j01.001728.pdf.pdf">http://repositorio.puce.edu.ec/bitstream/22000/7022/5/12j01.001728.pdf.pdf</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (110 palabras)
11	<a href="http://esacc.corteconstitucional.gob.ec">esacc.corteconstitucional.gob.ec</a> <a href="http://esacc.corteconstitucional.gob.ec/storage/ppl/v1/10_DWL_FUeyjYjw2XRNjorm8LJC1dWfkj0...">http://esacc.corteconstitucional.gob.ec/storage/ppl/v1/10_DWL_FUeyjYjw2XRNjorm8LJC1dWfkj0...</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (104 palabras)
12	<a href="http://consejoderechoscuencia.gob.ec">consejoderechoscuencia.gob.ec</a> <a href="https://consejoderechoscuencia.gob.ec/wp-content/uploads/2019/09/INFORME-EJEC.PRES_2018.pdf">https://consejoderechoscuencia.gob.ec/wp-content/uploads/2019/09/INFORME-EJEC.PRES_2018.pdf</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (106 palabras)
13	<a href="http://consejoderechoscuencia.gob.ec">consejoderechoscuencia.gob.ec</a> <a href="http://consejoderechoscuencia.gob.ec/wp-content/uploads/2019/09/INFORME-EJEC.PRES_2018.pdf">http://consejoderechoscuencia.gob.ec/wp-content/uploads/2019/09/INFORME-EJEC.PRES_2018.pdf</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (106 palabras)
14	<a href="http://www.oficial.ec">www.oficial.ec</a>   Ordenanza Municipal Que regula la estructura y funcionamiento ... <a href="https://www.oficial.ec/ordenanza-municipal-que-regula-estructura-y-funcionamiento-sistema-protecci...">https://www.oficial.ec/ordenanza-municipal-que-regula-estructura-y-funcionamiento-sistema-protecci...</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (93 palabras)
15	<a href="http://tesis.unsm.edu.pe">tesis.unsm.edu.pe</a> <a href="https://tesis.unsm.edu.pe/bitstream/11458/2206/1/TP_GI_00040_2017.pdf">https://tesis.unsm.edu.pe/bitstream/11458/2206/1/TP_GI_00040_2017.pdf</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (75 palabras)
16	<a href="http://repositorio.uncp.edu.pe">repositorio.uncp.edu.pe</a> <a href="http://repositorio.uncp.edu.pe/bitstream/20.500.12894/6111/1/1010_74622243_T_1.pdf">http://repositorio.uncp.edu.pe/bitstream/20.500.12894/6111/1/1010_74622243_T_1.pdf</a>	< 1%		<input type="checkbox"/> Palabras idénticas: < 1% (21 palabras)

**Fuentes mencionadas (sin similitudes detectadas)** Estas fuentes han sido citadas en el documento sin encontrar similitudes.

- 1 <http://es.slideshare.net/efracbtis/evolucion-de-redes-de-computadoras>
- 2 <https://tabasco.gob.mx/sites/default/files/Manual-para-aplicar-la-norma-TIA-EIA-para-Cableado-Estructurado.pdf>



**Anexo E: Fotografías**



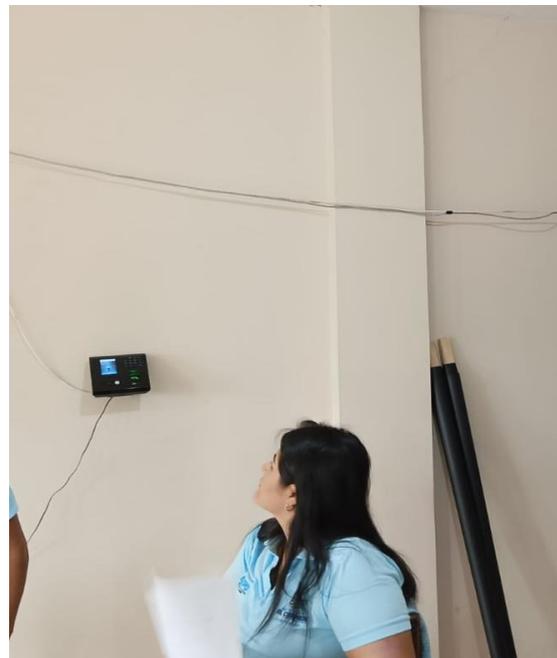
*Imagen 35. Equipos de Jefatura y Asistente*



*Imagen 36. Equipo Atención a Ciudadano*



*Imagen 37. Equipo de Recepción*

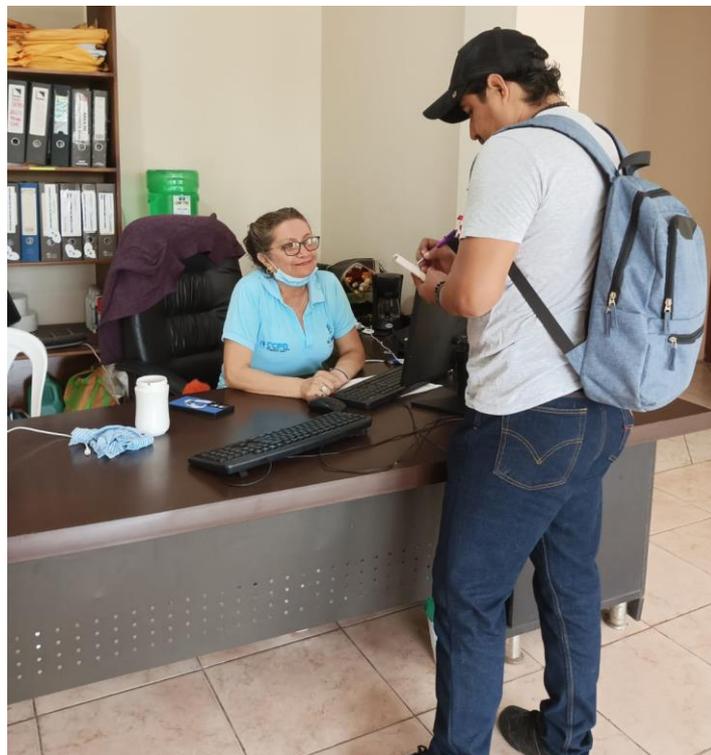


*Imagen 38. Reloj Biométrico*

**Anexo F:** Evidencia de aplicación de encuestas y entrevistas



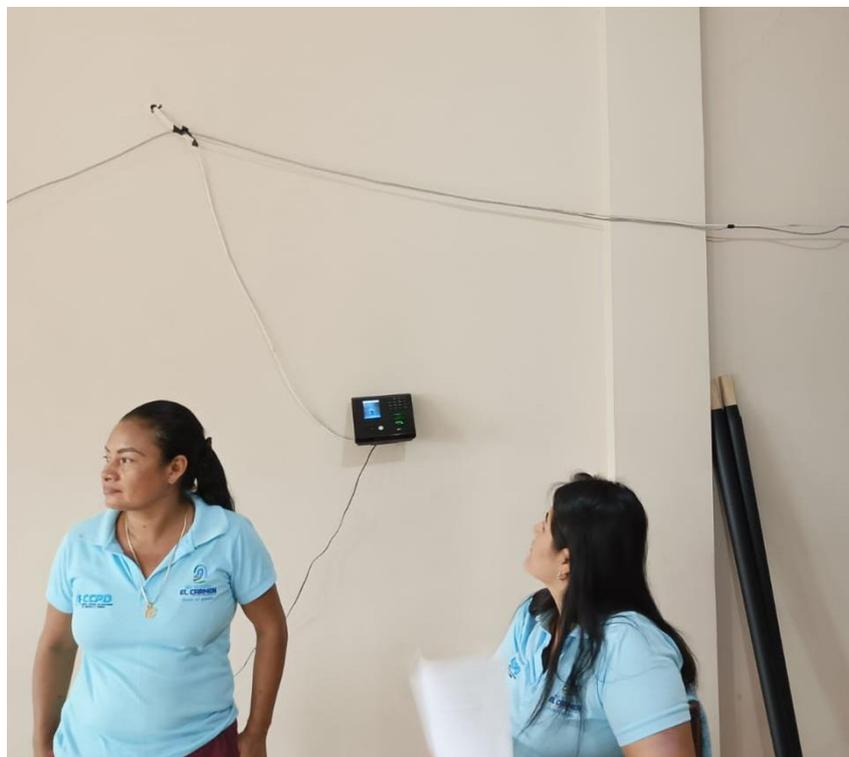
*Imagen 39. Entrevista al Ing. Javier Zambrano, encargado de STIC GAD*



*Imagen 40. Encuesta a Jefa del Sistema Cantonal*



*Imagen 41. Encuesta al personal del Sistema Cantonal*



*Imagen 42. Levantamiento de Fichas de Observación con equipos de red*