



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES  
INSTITUTO DE POSTGRADO**

**TÍTULO**

**ANÁLISIS DE SEGURIDAD EN PROTOCOLO RTSP USADO EN  
STREAMING DE VIDEO EN EL SIS ECU 911 ZONAL CUENCA**

**AUTOR**

**Cárdenas Carangui Xavier Andrés**

**TRABAJO DE TITULACIÓN**

**Previo a la obtención del grado académico en  
MAGÍSTER EN CIBERSEGURIDAD**

**TUTOR**

**Ing. Edison Pompilio Quintuña Padilla, MSc**

**Santa Elena, Ecuador**

**Año 2024**



**UPSE**

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES  
INSTITUTO DE POSTGRADO**

**TRIBUNAL DE SUSTENTACIÓN**

---

**Ing. Alicia Andrade Vera, Mgtr  
COORDINADORA DEL  
PROGRAMA**

---

**Ing. Edison Pompilio Quintuña  
Padilla, MSc  
TUTOR**

---

**Ing. Jaime Benjamín Orozco  
Iguasnia, Mgtr  
DOCENTE ESPECIALISTA**

---

**Ing. María Daniela Álvarez  
Galarza, Mgtr  
DOCENTE ESPECIALISTA**

---

**Abg. María Rivera, Mgtr  
SECRETARIO GENERAL UPSE**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES  
INSTITUTO DE POSTGRADO**

**CERTIFICACIÓN**

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por CÁRDENAS CARANGUI XAVIER ANDRÉS, como requerimiento para la obtención del título de Magíster en Ciberseguridad.

**TUTOR**

---

**Ing. Edison Pompilio Quintuña Padilla, MSc**

**Santa Elena, 15 de octubre de 2024**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES  
INSTITUTO DE POSTGRADO**

**DECLARACIÓN DE RESPONSABILIDAD**

**Yo, CÁRDENAS CARANQUI XAVIER ANDRÉS**

**DECLARO QUE:**

El trabajo de Titulación, “Análisis de seguridad en protocolo RTSP usado en streaming de video en el SIS ECU 911 Zonal Cuenca”, previo a la obtención del título en Magíster en Ciberseguridad, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, 15 de octubre de 2024

**EL AUTOR**

---

**Ing. Xavier Andrés Cárdenas Carangui**



**UPSE**

**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE CIENCIAS DE LA INGENIERÍA  
INSTITUTO DE POSTGRADO**

**CERTIFICACIÓN DE ANTIPLAGIO**

Certifico que después de revisar el documento final del trabajo de titulación denominado “Análisis de seguridad en protocolo RTSP usado en streaming de video en el SIS ECU 911 Zonal Cuenca”, presentado por el estudiante, CÁRDENAS CARANGUI, XAVIER ANDRÉS fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al 3%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

 <b>CERTIFICADO DE ANÁLISIS</b> magister		
<b>ANÁLISIS DE SEGURIDAD EN PROTOCOLO RTSP USADO EN STREAMING DE VIDEO EN EL SIS ECU 911 ZONAL CUENCA</b>		<b>3%</b> Textos sospechosos
		<b>3%</b> Similitudes 0% similitudes entre comillas 0% entre las fuentes mencionadas 0% Idiomas no reconocidos
<b>Nombre del documento:</b> ANALISIS DE SEGURIDAD EN PROTOCOLO RTSP USADO EN STREAMING DE VIDEO EN EL SIS ECU 911 ZONAL CUENCA.pdf <b>ID del documento:</b> 77803cbe47078d9a4777fe9b078970b5f81c01f2 <b>Tamaño del documento original:</b> 2.53 MB <b>Autor:</b> Xavier Andrés Cárdenas Carangui	<b>Depositante:</b> EDISSON POMPILO QUINTUÑA PADILLA <b>Fecha de depósito:</b> 14/10/2024 <b>Tipo de carga:</b> interface <b>fecha de fin de análisis:</b> 14/10/2024	<b>Número de palabras:</b> 14.718 <b>Número de caracteres:</b> 107.208

**TUTOR**

---

**Ing. Edison Pompilio Quintuña Padilla, MSc**



**UNIVERSIDAD ESTATAL PENÍNSULA  
DE SANTA ELENA  
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES  
INSTITUTO DE POSTGRADO**

**AUTORIZACIÓN**

**Yo, CÁRDENAS CARANQUI XAVIER ANDRÉS**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de mi trabajo de examen de carácter complejo con fines de difusión pública, además apruebo la reproducción de este trabajo de examen de carácter complejo dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, 15 de octubre de 2024

**EL AUTOR**

---

**Ing. Xavier Andrés Cárdenas Carangui**

## **AGRADECIMIENTO**

Quiero expresar mi más sincero agradecimiento a todas las personas que, de una u otra forma, han sido parte importante de este logro académico. En primer lugar, agradezco a mi familia y mi pareja quienes siempre han sido mi pilar y fuente de inspiración. Su apoyo incondicional me ha motivado a seguir adelante.

A mis profesores, quienes con su guía y conocimientos me han ayudado a enriquecer mis capacidades y visión en el campo de estudio, les agradezco profundamente. Su dedicación y compromiso fueron clave para el desarrollo de esta investigación.

A mi director de tesis, por su invaluable guía, paciencia y conocimientos compartidos. Su orientación fue fundamental para mantener el enfoque adecuado y elevar la calidad de esta investigación.

Finalmente, agradezco a la institución que me permitió la recopilación de información y datos para la realización de mi trabajo de titulación orientado hacia un campo tan relevante como la ciberseguridad.

*Xavier Andrés Cárdenas Carangui.*

## **DEDICATORIA**

A mi madre, por su amor incondicional y su apoyo constante, que me han dado la fuerza para seguir adelante. A mi hermana, por ser mi compañera y motivadora en cada paso de este camino. A mi tía, por su sabiduría y aliento en momentos difíciles. Y a mi pareja, por su amor y comprensión, que han sido mi refugio y mi inspiración. Gracias a todos por estar siempre a mi lado.

*Xavier Andrés Cárdenas Carangui*



# ÍNDICE GENERAL

TÍTULO DEL TRABAJO DE TITULACIÓN.....	I
TRIBUNAL DE SUSTENTACIÓN.....	II
CERTIFICACIÓN.....	III
DECLARACIÓN DE RESPONSABILIDAD.....	IV
CERTIFICACIÓN DE ANTIPLAGIO .....	V
AUTORIZACIÓN .....	VI
AGRADECIMIENTO .....	VII
DEDICATORIA .....	VIII
ÍNDICE GENERAL .....	IX
ÍNDICE DE TABLAS .....	XII
ÍNDICE DE FIGURAS .....	XIII
RESUMEN .....	XV
ABSTRACT.....	XVI
INTRODUCCIÓN.....	1
1.1    Planteamiento del Problema .....	1
1.2    Objetivos.....	2
1.2.1    Objetivo General.....	2
1.2.2    Objetivos Específicos .....	2
1.2.3    Alcance .....	3
1.2.4    Importancia del estudio.....	3
DESARROLLO .....	5
2.1    Marco Teórico.....	5
2.1.1    Streaming de video .....	5
2.1.2    Protocolo RTSP (Real Time Streaming Protocol).....	5

2.1.3	Componentes de una entrega RTSP.....	6
2.1.4	Propiedades de RTSP.....	8
2.1.5	Funcionamiento de RTSP .....	9
2.1.6	Vulnerabilidades del protocolo RTSP .....	11
2.1.7	Problemas de seguridad en protocolos de streaming .....	12
2.1.8	Diferencias entre protocolos de streaming.....	13
2.1.9	Vulnerabilidades sobre cámaras IP .....	14
2.1.10	Protocolo SRTP (Secure Real-Time Transport Protocol).....	15
2.2	Modelo de gestión del sistema de videovigilancia del SIS ECU 911 Zonal 6	15
2.2.1	Modelo de infraestructura del ECU 911 Zonal 6 para streaming de video ....	15
2.2.2	Diagrama de red de los enlaces de datos utilizados.....	16
2.2.3	Puntos de videovigilancia .....	17
2.2.4	Tipos de cámaras .....	17
2.2.5	Enlaces de datos.....	18
2.2.6	Direccionamiento IP .....	18
2.2.7	VMS (Video Management System).....	19
2.2.8	IVS (Intelligent Video Surveillance) .....	19
2.3	Criterios generales de seguridad de la información aplicados en los sistemas de videovigilancia del SIS ECU 911.....	20
2.3.1	Seguridad de redes para consolas de videovigilancia.....	20
2.3.2	Seguridad Perimetral.....	20
2.3.3	Seguridad Física.....	20
2.3.4	Controles de acceso .....	21
2.4	Vulnerabilidades identificadas y reconocidas en el sistema de videovigilancia del SIS ECU 911 .....	21
2.4.1	Registro histórico de vulnerabilidades encontradas sobre los sistemas de videovigilancia del SIS ECU 911 .....	22
2.5	Análisis de la seguridad del Protocolo RTSP en el sistema de video vigilancia del SIS ECU 911 .....	23
2.5.1	Herramientas utilizadas para análisis de vulnerabilidades .....	23
2.5.2	Escaneo de red, puertos abiertos y tráfico RTSP de los hosts de prueba .....	24
2.6	Pruebas automatizadas en Nessus.....	29

2.7	Pruebas manuales para identificación de vulnerabilidades.....	34
	RESULTADOS Y CONCLUSIONES .....	38
3.1	Vulnerabilidades identificadas.....	38
3.1.1	Vulnerabilidades encontradas en cámaras Hikvision .....	38
3.1.2	Vulnerabilidades encontradas en cámaras Dahua.....	38
3.1.3	Vulnerabilidad en la integración de cámaras al sistema de visualización (IVS) 38	
3.1	Alternativas de mitigación .....	40
3.1.1	Recomendaciones generales .....	40
3.1.2	Recomendaciones específicas .....	42
3.1.3	Configuración del mecanismo de autenticación en cámaras Hikvision .....	42
3.1.4	Configuración del protocolo SRTP en cámaras Hikvision.....	43
	CONCLUSIONES .....	45
	RECOMENDACIONES.....	47
	REFERENCIAS.....	49
	ANEXOS .....	51

## ÍNDICE DE TABLAS

Tabla 1. Protocolos de streaming de video. ....	14
Tabla 2. Tipos de cámaras utilizados en el SIS ECU 911 Zonal Cuenca. ....	18
Tabla 3. Ejemplos de direccionamiento IP. ....	19
Tabla 4. Roles usados para los usuarios que monitorean el sistema de videovigilancia. ....	21
Tabla 5. Vulnerabilidades obtenidas de las pruebas automatizadas. ....	33
Tabla 6. Muestra de cámaras para realización de pruebas. ....	34

## ÍNDICE DE FIGURAS

Figura 1. Entrega RTSP.....	7
Figura 2. Comunicación streaming de video. ....	9
Figura 3. Captura de paquetes de comandos RTSP. ....	10
Figura 4. Paquete de datos correspondiente al comando de control “PLAY” del protocolo RTSP.....	11
Figura 5. Topología del sistema de videovigilancia del SIS ECU 911.....	16
Figura 6. Diagrama de red de enlaces de datos con puntos de videovigilancia.....	17
Figura 7. Escaneo de dispositivos que utilicen RTSP mediante Nmap. ....	25
Figura 8. Escaneo para recabar información adicional de los dispositivos detectados. .	26
Figura 9. Identificación de URLs conocidas desprotegidas. ....	27
Figura 10. Diagrama de la topología de red del sistema de videovigilancia del SIS ECU 911 Zonal 6. ....	28
Figura 11. Captura de paquetes RTSP mediante WireShark. ....	28
Figura 12. Componentes de una entrega RTSP. ....	29
Figura 13. Configuración de host para prueba.....	29
Figura 14. Configuración de los puertos a ser analizados. ....	30
Figura 15. Configuración del tipo de ataque que se llevará a cabo. ....	30
Figura 16. Resultados de la primera prueba obtenidos por Nessus. ....	31
Figura 17. Configuración para la segunda prueba. ....	32
Figura 18. Configuración de parámetros de prueba.....	32
Figura 19. Resultados de la segunda prueba obtenidos por Nessus.....	33
Figura 20. Configuración de autenticación de una cámara Hikvision.....	35

Figura 21. Parámetros de configuración de administración de usuario de una cámara Tiandy PTZ.....	35
Figura 22. Configuración de autenticación de una cámara Dahua. ....	36
Figura 23. Parámetros de configuración de administración de usuario de una cámara CEMAX.....	36
Figura 24. Parámetros de configuración de administración de usuario de una cámara TIANDY fija.....	36
Figura 25. Resultado de un script de uno de los scripts de pruebas utilizados. ....	37
Figura 26. Vinculación de dispositivos con servidor de streaming. ....	39
Figura 27. Detalles de una cámara IP agregada al IVS. ....	40
Figura 28. Acceso a una cámara IP a través de un reproductor de video. ....	40
Figura 29. Algoritmos de autenticación RTSP. ....	42
Figura 30. Configuración de protocolo SRTP. ....	43
Figura 31. Configuración del certificado digital para SRTP. ....	43
Figura 32. Configuración de protocolo y certificado SRTP. ....	44
Figura 33. Establecimiento de conexión desde VLC hacia la cámara.....	44

## **RESUMEN**

Este trabajo analiza la seguridad del protocolo Real-Time Streaming Protocol (RTSP), empleado en la plataforma de videovigilancia del Servicio Integrado de Seguridad ECU 911 en la ciudad de Cuenca. Se enfoca en identificar vulnerabilidades en el protocolo RTSP, debido a la falta de cifrado y autenticación robusta, lo que puede exponer la integridad y confidencialidad de la transmisión de video en tiempo real. A través de pruebas automatizadas y manuales, se examinan cámaras IP de diferentes marcas y configuraciones, revelando riesgos significativos, como el uso de algoritmos de encriptación obsoletos y vulnerabilidades en la integración del sistema de visualización. Se proponen medidas de mitigación, como la actualización de credenciales, la implementación de autenticación fuerte y el uso de cifrado en las transmisiones. Los resultados y recomendaciones no solo mejorarán la seguridad del sistema del SIS ECU 911, sino que también servirán como referencia para otras instituciones que utilicen sistemas similares.

**Palabras claves:** RTSP, videovigilancia, vulnerabilidades.

## **ABSTRACT**

This study analyzes the security of the Real-Time Streaming Protocol (RTSP) used in the video surveillance platform of the Integrated Security Service ECU 911 in the city of Cuenca. It focuses on identifying vulnerabilities in the RTSP protocol, due to the lack of encryption and strong authentication, which can expose the integrity and confidentiality of real-time video transmissions. Through automated and manual testing, IP cameras from different brands and configurations are examined, revealing significant risks such as the use of outdated encryption algorithms and vulnerabilities in the integration of the visualization system. Mitigation measures are proposed, such as updating credentials, implementing strong authentication, and using encryption for transmissions. The results and recommendations will not only improve the security of the SIS ECU 911 system but also serve as a reference for other institutions that use similar systems.

**Keywords:** RTSP, video surveillance, vulnerabilities.



# INTRODUCCIÓN

El presente trabajo analizará la seguridad del protocolo *Real-Time Streaming Protocol* (RTSP), un protocolo de control de transmisión diseñado para la gestión de flujos de video en tiempo real, ampliamente utilizado en sistemas de videovigilancia. Se prestará especial atención a su aplicación dentro del Servicio Integrado de Seguridad ECU 911 (SIS ECU 911) de la ciudad de Cuenca, perteneciente a la Coordinación Zonal 6. El análisis se centrará en la identificación y evaluación de vulnerabilidades del protocolo RTSP en la infraestructura del SIS ECU 911, y se propondrán mejoras para mitigar los riesgos identificados.

La plataforma de videovigilancia del SIS ECU 911 constituye una infraestructura tecnológica que podría definirse como crítica a nivel nacional, ya que permite el monitoreo ininterrumpido las 24 horas del día, los 7 días de la semana, y, en caso de emergencias, el sistema actúa como soporte en la coordinación de respuestas con entidades como salud, la policía, bomberos y otros organismos de seguridad.

Debido a que se captura información visual a través de cámaras IP, es importante aplicar las medidas de seguridad necesarias para evitar accesos no autorizados y mantener la integridad de los datos, esto representa un desafío complejo debido a la heterogeneidad de su infraestructura y la complejidad propia de un sistema de estas características.

La importancia de este estudio radica en que las soluciones propuestas no solo beneficiarán al SIS ECU 911, sino que también podrán servir como un modelo replicable para otras instituciones que utilicen sistemas similares. Con este enfoque, se busca reforzar la seguridad en las transmisiones de video en tiempo real y salvaguardar la integridad de los datos en un sistema crítico para la seguridad pública del país.

## 1.1 Planteamiento del Problema

El sistema de videovigilancia del SIS ECU 911 desempeña un papel central en la seguridad pública a nivel nacional, ya que permite el monitoreo continuo de áreas estratégicas mediante cámaras IP, sin embargo, este sistema está expuesto al riesgo de ser blanco de ataques informáticos que podrían comprometer tanto la integridad como la confidencialidad de la información transmitida.

Este riesgo es particularmente significativo porque las cámaras IP utilizan el protocolo RTSP, el cual, en su diseño original, carece de mecanismos de seguridad robustos, como el cifrado y la autenticación fuerte.

Casos recientes, como la filtración masiva de cámaras de seguridad de Verkada en 2021, donde más de 150,000 cámaras fueron vulneradas debido a credenciales expuestas, como lo menciona Turton William (2021), y la exposición de cámaras IP sin seguridad adecuada a través de motores de búsqueda como Shodan, demuestran que los sistemas de videovigilancia mal protegidos son blancos fáciles para los atacantes, mencionado en Tejaswi et al. (2023). Estos incidentes resaltan cómo una gestión deficiente de credenciales y la falta de cifrado en las transmisiones pueden resultar en accesos no autorizados y filtraciones de video, comprometiendo tanto la seguridad institucional como la privacidad de los ciudadanos.

Dado el alcance nacional del sistema de videovigilancia del SIS ECU 911, las consecuencias de una vulneración de seguridad podrían ser aún mayores, afectando también a la coordinación de respuestas en situaciones de emergencia, lo que incrementa el impacto potencial de cualquier incidente.

## **1.2 Objetivos**

### **1.2.1 Objetivo General**

Realizar una revisión bibliográfica de los avances en carácter de seguridad aplicados a protocolos de transmisión de video (RTSP) usado en la plataforma de videovigilancia del SIS ECU 911.

### **1.2.2 Objetivos Específicos**

- Documentar cada una de las vulnerabilidades encontradas en la transmisión de video y cómo pueden ser mitigadas.
- Exponer las diferentes alternativas de mejoras en seguridad aplicadas a transmisión de video.
- Identificar qué tipo de seguridad aplicada al protocolo RTSP encaja de mejor manera sobre los sistemas de videovigilancia del SIS ECU 911.

### **1.2.3 Alcance**

Este trabajo tiene como objetivo identificar y documentar las vulnerabilidades presentes en el protocolo RTSP, utilizado en el sistema de videovigilancia del SIS ECU 911 en la Coordinación Zonal 6 de Cuenca. El análisis se centrará en los aspectos relacionados con la transmisión de video mediante cámaras IP, evaluando configuraciones inadecuadas, ausencia de cifrado y autenticación débil.

El estudio no abordará otros componentes de la infraestructura de red ni sistemas de seguridad física, asimismo, se limitará al análisis de las partes del sistema implementadas durante los dos últimos años. Finalmente, se propondrán mejoras aplicables a los mecanismos de seguridad en el protocolo RTSP, con el objetivo de mitigar las vulnerabilidades encontradas y mejorar la seguridad general del sistema de videovigilancia.

### **1.2.4 Importancia del estudio**

Este estudio aborda un problema que afecta directamente la seguridad pública y la privacidad de los ciudadanos en Ecuador, al enfocar su análisis en el protocolo RTSP, una tecnología utilizada como base en la transmisión de video en tiempo real. Las vulnerabilidades inherentes al diseño de RTSP representan un riesgo significativo en el contexto del sistema de videovigilancia del SIS ECU 911, que desempeña una función central en la coordinación de respuestas ante emergencias y la vigilancia de áreas estratégicas a nivel nacional. Las amenazas a la seguridad de este sistema son cada vez más evidentes en un entorno donde los ataques informáticos se han vuelto más sofisticados y frecuentes, por lo que la mitigación de estas vulnerabilidades es prioritaria.

Los resultados esperados de este trabajo no solo fortalecerán la seguridad del sistema del SIS ECU 911, sino que también proporcionarán una guía útil para otras instituciones que empleen sistemas similares, tanto en Ecuador como en otros países. Además, se espera aportar nuevo conocimiento sobre las vulnerabilidades del RTSP, un área que ha sido subestimada a pesar de su importancia en el campo de la videovigilancia. Por lo tanto, este trabajo es necesario y oportuno, y su viabilidad está garantizada gracias al acceso a los recursos técnicos y logísticos disponibles.

Por último, se espera que este trabajo genere un impacto positivo tanto a nivel institucional como social, mejorando la seguridad de los sistemas de videovigilancia y reforzando las medidas de protección de los datos visuales. La implementación de las soluciones propuestas no solo beneficiará al SIS ECU 911, sino que también servirá como modelo para otras entidades que busquen mejorar la seguridad de sus sistemas de videovigilancia.

# DESARROLLO

## 2.1 Marco Teórico

En el siguiente apartado se presentarán los aspectos más relevantes sobre el funcionamiento y uso del protocolo RTSP, así como sus principales vulnerabilidades de seguridad.

### 2.1.1 Streaming de video

Apostolopoulos et al. (2002) menciona que la transmisión de video (streaming de video) puede ser definido como la transferencia digital de video, entre un servidor multimedia<sup>1</sup> y un cliente, permitiendo la opción de ser observado en tiempo real, además, la transmisión de video puede ser comprimida y almacenada en formatos como: MP4, MP4G, AVI, VMW.

Mateos Costilla & Montoro (2008) explican que existen dos modelos de streaming de video:

- **Live Streaming (Transmisión en vivo):** Es la transferencia de contenido multimedia en tiempo real, abarcando desde dispositivos como cámaras hasta sistemas de videovigilancia. La transmisión ocurre desde un dispositivo hacia un visualizador en el mismo momento en que se produce.
- **On-demand streaming (Transmisión bajo demanda):** Este modelo almacena los archivos multimedia en un servidor, lo que permite que puedan ser compartidos posteriormente con una audiencia. Los usuarios podrán acceder a los archivos en cualquier momento.

### 2.1.2 Protocolo RTSP (Real Time Streaming Protocol)

El Protocolo de Transmisión en Tiempo Real, (RSTP) es un protocolo no orientado a la conexión, empleado para el flujo de datos multimedia. El protocolo trabaja

---

<sup>1</sup> Servidor Multimedia: Dispositivo diseñado para almacenar, organizar y transmitir archivos como audio, video e imágenes.

a nivel de capa de aplicación del modelo OSI<sup>2</sup>, controlando que el contenido multimedia se entregue de manera correcta, como lo menciona Yan Liu et al., (2008).

Chu et al. (2013) mencionan que el protocolo RTSP envía datos a través de redes IP, pudiendo establecer uno o más flujos sincronizados de audio y video. El protocolo puede funcionar sobre UDP<sup>3</sup>, RDP<sup>4</sup> o TCP<sup>5</sup>, permitiendo que un cliente pueda usar conexiones estables con los servidores mediante las peticiones RTSP. Es común que se utilice TCP para controlar el reproductor y UDP como canal de envío de datos.

Se debe indicar que el protocolo RTSP usa por defecto el puerto de comunicación 554, no obstante, este puede ser configurado de manera manual a un puerto diferente en la negociación entre cliente y servidor.

El protocolo RTSP se define originalmente en el RFC 2326 (publicado en 1998), en 2016, se introdujo RTSP 2.0 (definido en el RFC 7826), una actualización importante que no es compatible retroactivamente con RTSP 1.0.

### **2.1.3 Componentes de una entrega RTSP**

Se conoce como una entrega RTSP al proceso de gestionar una transmisión de datos multimedia en tiempo real, desde un dispositivo hacia un cliente.

Para garantizar una entrega exitosa, intervienen dos protocolos adicionales: RTP y RTCP, como lo menciona Schulzrinne (2003).

- **Protocolo RTP (Protocolo de Transporte en Tiempo Real)**

Protocolo utilizado para transporte de datos de audio y video en tiempo real, dado que la entrega de la información de datos multimedia puede presentar retrasos, se emplea el protocolo UDP como mecanismo de entrega dentro de la capa de

---

<sup>2</sup> Modelo OSI (Open System Interconnection): El modelo de carácter universal para comunicaciones de red, tiene como propósito estandarizar la comunicación entre diferentes sistemas, de modo que dispositivos y aplicaciones de fabricantes diferentes puedan comunicarse entre sí.

<sup>3</sup> UDP: Protocolo de datagrama de usuario (User datagram protocol).

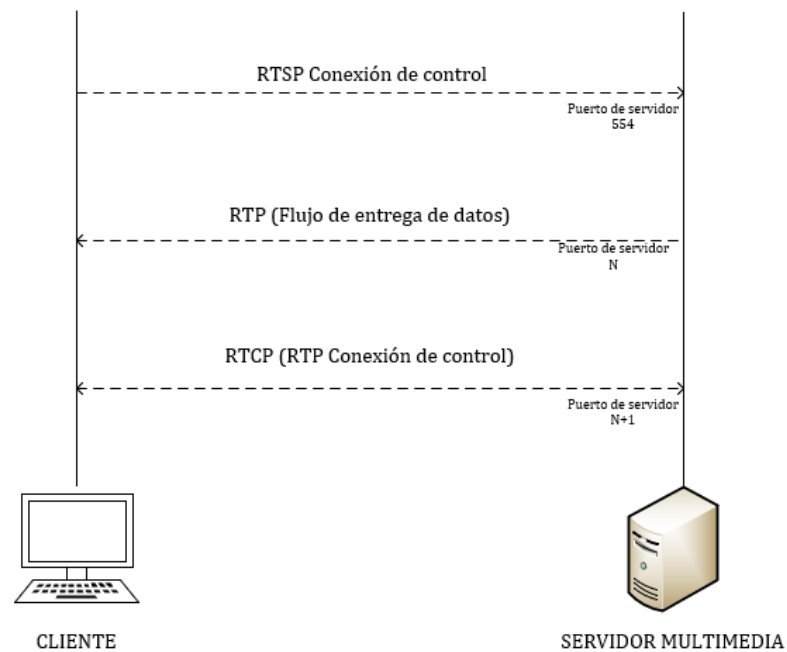
<sup>4</sup> RDP: Protocolo de escritorio remoto (Remote Desktop Protocol).

<sup>5</sup> TCP: Protocolo de control de transmisión (Transfer Control Protocol).

transporte del modelo OSI. RTP es un flujo de transmisión unidireccional desde el servidor hacia el cliente.

- **Protocolo RTCP (Control en tiempo real)**

Este protocolo complementa al RTP, siendo bidireccional y utilizando también UDP, permite al cliente controlar la calidad de las transmisiones en tiempo real.



*Figura 1. Entrega RTSP.*

En la figura 1 se aprecia la interacción entre el cliente y el servidor multimedia mediante:

- La **conexión de control del protocolo RTSP**, utilizada para gestionar de manera eficiente las sesiones de streaming.
- El **protocolo RTP**, utilizado para entregar los datos multimedia (audio y video).
- El **protocolo RTCP**, utilizado de manera bidireccional para transportar información referente a la calidad del stream RTP.

#### 2.1.4 Propiedades de RTSP

Schulzrinne et al. (1998) mencionan ciertas características importantes del protocolo, entre las cuales se destacan:

- **Extensible:** Permite fácilmente añadir nuevos parámetros y métodos.
- **Seguro:** Utiliza mecanismos de seguridad web, como TLS/SSL y autenticación HTTP.
- **Capacidad multiservidor:** Permite que el contenido sea distribuido desde múltiples servidores, posibilitando que diferentes partes de un contenido puedan residir en servidores distintos, esta característica es utilizada en escenarios donde se requiere alta disponibilidad y redundancia.
- **Amigable con HTTP:** Utiliza conceptos de HTTP para reutilizar la infraestructura existente, esta infraestructura incluye PICS (Platform for Internet Content Selection) que sirve para etiquetar páginas web y controlar el acceso a contenido en Internet.
- **Control adecuado de servidor:** El cliente puede iniciar y detener una transmisión; los servidores no pueden iniciar una transmisión que no pueda ser detenida por el cliente.
- **Negociación de transporte:** El cliente puede negociar un método de transporte antes de iniciar un proceso de flujo continuo.
- **Negociación de capacidad:** Si las funcionalidades básicas están deshabilitadas, el cliente debe tener un mecanismo para determinar que métodos no se podrán implementar.
- **Control de dispositivos de grabación:** El protocolo controla dispositivos de grabación y reproducción.
- **Separación del control de transmisión y el inicio de la conferencia:** Esta característica permite gestionar las sesiones del streaming multimedia. RTSP maneja el control de los flujos de datos y la configuración inicial de la conferencia. El control de la transmisión lo gestiona a través de los comandos PLAY, PAUSE, TEARDOWN, mientras que el inicio de la conferencia se establece a través del comando SETUP. Esto permite gestionar de forma separada diferentes flujos de datos multimedia.



### 2.1.5 Funcionamiento de RTSP

Cmpe (2009) señala que RTSP se utiliza para llevar a cabo acciones como reproducir, detener y repetir el streaming mediante comandos específicos. En la siguiente figura, se muestran los protocolos que intervienen en una comunicación de streaming.

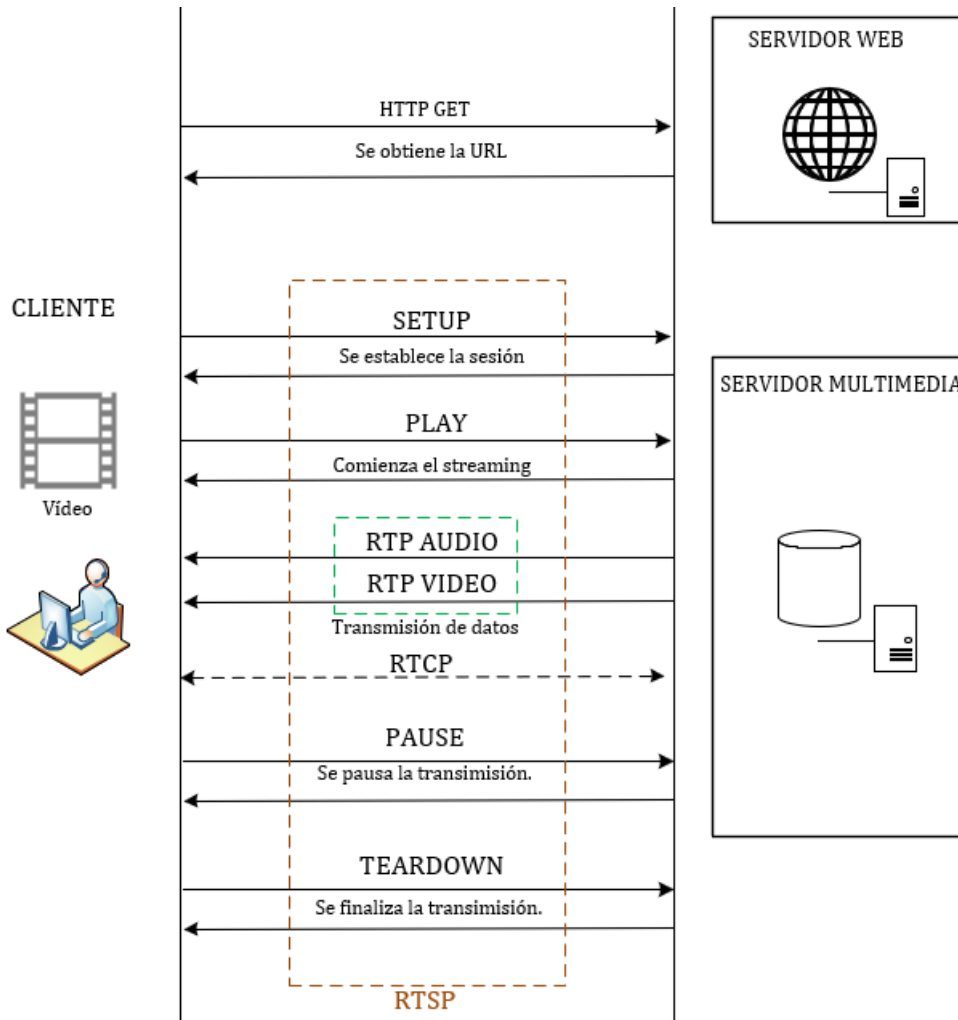


Figura 2. Comunicación streaming de video.

RTSP fragmenta los datos de transmisión en varios paquetes, ajustándose al ancho de banda disponible entre el cliente y el servidor. Su función principal es actuar como un control remoto para los servidores multimedia, permitiendo la gestión eficiente del streaming. Además, RTSP se beneficia de las optimizaciones de RTP, como la compresión de los encabezados, para mejorar el rendimiento de la transmisión, como lo menciona Kumar R et al. (2008).

Zingade et al, (2016) indica que para establecer una conexión RTSP, se siguen los siguientes pasos:

1. El Cliente envía una petición RTSP hacia una cámara IP, esperando establecer una conexión a través del comando “SETUP”.
2. La cámara responde a través de un protocolo de transporte, comúnmente RTP.
3. El cliente solicita la reproducción del contenido mediante el comando “PLAY”, lo que inicia la transmisión.
4. La cámara envía un paquete de datos de video en tiempo real, a través de una conexión TCP.
5. El cliente recibe y decodifica los paquetes de datos enviados en un formato de video.

Para comprender cómo se establece la comunicación a través del protocolo RTSP, se llevó a cabo una prueba utilizando la herramienta *Wireshark* para analizar el tráfico de red. Esta herramienta permite capturar y visualizar en detalle los paquetes de datos intercambiados durante la transmisión de video en tiempo real. En la figura 3, se puede observar la estructura de los componentes que forman parte de una transmisión RTSP, proporcionando una visión clara del flujo de datos y las interacciones entre los dispositivos implicados.

1184...	154.825543	10.2.	10.2.	RTSP	195 Reply: RTSP/1.0 200 OK
1184...	154.827465	10.2.	10.2.	RTSP	459 SETUP rtsp://10.2.:554/trackID=1 RTSP/1.0
1184...	154.856070	10.2.	10.2.	RTSP	195 Reply: RTSP/1.0 200 OK
1184...	154.860784	10.2.	10.2.	RTSP	421 PLAY rtsp://10.2.:554/ RTSP/1.0

Figura 3. Captura de paquetes de comandos RTSP.

En la anterior figura se destacan dos comandos de control:

SETUP: Solicita las opciones disponibles del servidor RTSP.

PLAY: Inicia la reproducción del flujo multimedia.

En la figura 4, se puede visualizar información correspondiente a la estructura de uno de estos paquetes, específicamente al comando de control “PLAY” y sus respectivas cabeceras.

```
▼ Real Time Streaming Protocol
  > Request: PLAY rtsp://10.2.:554/ RTSP/1.0\r\n
    CSeq: 10\r\n
    Authorization: Digest username="admin", realm="Login to ef78d5ce560897a48ba20ff8c180fe9a"
    User-Agent: LibVLC/3.0.20 (LIVE555 Streaming Media v2016.11.28)\r\n
    Session: 1332115746
    Range: npt=0.000-\r\n
```

Figura 4. Paquete de datos correspondiente al comando de control "PLAY" del protocolo RTSP.

## 2.1.6 Vulnerabilidades del protocolo RTSP

RTSP presenta varias vulnerabilidades que pueden comprometer la seguridad de los sistemas que lo utilizan. Los datos que se transmiten pueden ser interceptados o modificados, con el objetivo de monitorear, distorsionar y/o eliminar el contenido de una transmisión. RTSP tiene una baja confidencialidad para la transmisión en tiempo real, como lo menciona Watequlis Syaifudin et al. (2018).

En la sección 2.1.4, *Propiedades de RTSP*, se menciona que una de las características de este protocolo es su seguridad; no obstante, existen varios problemas en este aspecto que pueden comprometer la privacidad y la integridad del contenido transmitido.

Según Understanding RTSP: The Real-Time Streaming Protocol Explained (2023), en una transmisión RTSP se pueden presentar los siguientes problemas de seguridad:

- **Falta de cifrado:** El protocolo RTSP no implementa métodos de cifrado para proteger su contenido, lo que lo hace vulnerable a ataques que buscan interceptar la transmisión en tiempo real mediante accesos no autorizados.
- **Autenticación débil:** RTSP utiliza métodos de autenticación básica, lo que lo hace vulnerable a ataques de fuerza bruta, permitiendo que las credenciales de acceso puedan ser comprometidas.
- **Ataques de Inyección:** Los atacantes pueden inyectar paquetes maliciosos a través de comandos en los mensajes de RTSP, comprometiendo la integridad del contenido multimedia.

### 2.1.7 Problemas de seguridad en protocolos de streaming

Los problemas de seguridad en protocolos de streaming hacen referencia a ciertas fallas, debilidades y vulnerabilidades que pueden ser explotadas por un atacante para comprometer todo el flujo de transmisión, ya sea de audio o video.

Lian et al. (2009) menciona los siguientes problemas de seguridad:

- **Susceptibilidad a Intrusión**

Se refiere a los intentos no autorizados de acceso con el objetivo de manipular sistemas a través de una red de datos, estos intentos de intrusión pueden considerarse como ataques realizados por ciberdelincuentes y se clasifican en varios tipos, tales como: vulneración de servicios, inicios de sesión no autorizados, acceso a archivos confidenciales, malware, entre otros. Un ataque de intrusión se puede realizar a través de una debilidad en los servicios de streaming multimedia.

- **Falta de Encriptación**

La falta de encriptación puede exponer información sensible, comprometiendo la seguridad de un dispositivo o de todo el sistema. Esta vulnerabilidad surge principalmente del uso de algoritmos de cifrado obsoletos o débiles, que pueden ser explotados mediante técnicas de intrusión. En el caso del protocolo RTSP, no se soporta cifrado de extremo a extremo, lo que deja la transmisión de video expuesta a posibles interceptaciones o manipulación de datos durante su recorrido entre el dispositivo y el servidor. Esto plantea un riesgo considerable para la integridad y confidencialidad de la información transmitida.

- **Denegación de servicios**

Este tipo de vulnerabilidad busca interrumpir la disponibilidad de un servicio de transmisión de video o audio, un atacante puede inundar un servidor de streaming con grandes cantidades de tráfico o explotar vulnerabilidades específicas de los protocolos mediante el envío de paquetes malicioso o inyección de código.

### 2.1.8 Diferencias entre protocolos de streaming

Los protocolos de streaming definen reglas para la transmisión de datos multimedia a través de redes, cada protocolo posee características específicas que lo hacen adecuado para diferentes situaciones.

En la siguiente tabla se muestran los protocolos de streaming de audio y video en tiempo real más utilizados, analizando su funcionalidad, usos y características.

Protocolo	RTSP (Real Time Streaming Protocol)	RTMP (Real Time Messaging Protocol)	SRT (Secure Reliable Transport)	WebRTC (Web Real Time Communication)
Traducción	Protocolo de transmisión en tiempo real	Protocolo de mensajería en tiempo real	Transporte seguro y confiable	Comunicación web en tiempo real
Uso	Usado en transmisiones en vivo en redes locales, como cámaras de seguridad y video conferencias	Usado para enviar video y audio de alta calidad a servidores, entregando contenido a gran escala en internet	Usado por su baja latencia y transmisión segura de audio y video	Usado para transmisión en tiempo real de audio, video y datos
Descripción	Establece y controla sesiones multimedia entre dispositivos finales, se usa comúnmente en sistemas de videovigilancia y videoconferencias	Utiliza un modelo cliente-servidor, principalmente para la transmisión en vivo y la entrega de video bajo demanda	Usa UDP para el transporte e incluye mecanismos de recuperación de paquetes y control de congestión	Comúnmente utilizado para videoconferencias, juegos en línea y aplicaciones en tiempo real.

<b>Codificaciones</b>	Soporta codificaciones de video: H.265 <sup>6</sup> , H.264 <sup>7</sup> , VP9 <sup>8</sup> , VP8 <sup>9</sup>	Soporta codificaciones de video: H.264	Soporta las codificaciones de streaming RTMP, HLS <sup>10</sup> , etc.	Soporta las codificaciones de video: H.264
-----------------------	--	--	--	--

*Tabla 1. Protocolos de streaming de video.*

### 2.1.9 Vulnerabilidades sobre cámaras IP

Las cámaras IP son el punto de origen de las transmisiones en tiempo real, utilizando RTSP como el protocolo para gestionar y controlar el flujo de datos multimedia, por lo tanto, cualquier vulnerabilidad en las cámaras IP afecta directamente a la seguridad y confiabilidad del protocolo RTSP. A continuación, se detallan las principales vulnerabilidades identificadas en el uso de cámaras IP con transmisión RTSP:

- **Secuestros de sesión:** Un atacante puede interceptar una sesión establecida y tomar control del contenido multimedia, lo que se considera un acceso no autorizado, con la posibilidad de manipular el contenido.
- **Explotación de configuración predeterminada:** Existe la posibilidad de que los usuarios no cambien las credenciales por defecto de acceso a una cámara, lo que convierte a las cámaras en un objetivo fácil y vulnerable para que un atacante acceda al contenido, como lo menciona Understanding RTSP: The Real-Time Streaming Protocol Explained (2023).

---

<sup>6</sup> H.265: Estándar de compresión de video, permite transmitir video de alta calidad, como 4K y 8K usando menos ancho de banda.

<sup>7</sup> H.264: Estándar de compresión de video, usado ampliamente para la transmisión y almacenamiento de video en un menor tamaño.

<sup>8</sup> VP9: Códec de video diseñado para reducir el tamaño de los archivos manteniendo su calidad.

<sup>9</sup>VP8: Códec de video diseñado para ofrecer una compresión eficiente y permitir transmisión con menos datos.

<sup>10</sup> HLS: Protocolo de transmisión desarrollado por Apple, permite entregas contenido multimedia a través de internet.

### **2.1.10 Protocolo SRTP (Secure Real-Time Transport Protocol)**

El Protocolo de Transporte Seguro en Tiempo Real (SRTP) es una extensión del Protocolo RTP que añade mecanismos de seguridad para las transmisiones multimedia. Este protocolo fue definido en el RFC 3711 (publicado en 2004) y proporciona confidencialidad mediante la encriptación del contenido multimedia (audio y video), autenticación de los mensajes y protección contra ataques de repetición durante la transmisión de datos entre clientes y servidores. SRTP asegura que los flujos de medios transmitidos no sean interceptados ni manipulados por actores no autorizados, garantizando así la integridad y privacidad de la información audiovisual en sistemas de videovigilancia, como lo mencionan Dessai & Chaudhari (2015).

Iyyanar et al. (2012) destacan las siguientes mejoras de seguridad implementadas por SRTP:

- Confidencialidad para RTP y RTCP, cifrando su contenido.
- Integridad de todos los paquetes RTP y RTCP, garantizando que no sean modificados.
- Utilización de algoritmos de cifrado de datos para proteger el contenido multimedia.
- Prevención de ataques de repetición, utilizando identificadores únicos de paquetes para rechazar duplicados.
- Integración con TLS, asegurando el establecimiento seguro de la conexión.
- SRTP se puede utilizar como una capa de seguridad en la transmisión, permitiendo proteger el flujo de video contra accesos no autorizados.

## **2.2 Modelo de gestión del sistema de videovigilancia del SIS ECU 911 Zonal 6**

En el siguiente apartado se presentará el modelo general de gestión del sistema de videovigilancia del SIS ECU 911 Zonal 6, explicando su topología de red y los componentes involucrados.

### **2.2.1 Modelo de infraestructura del ECU 911 Zonal 6 para streaming de video**

La topología que se muestra en la figura 5 refleja el esquema actual de operación del streaming de video en el sistema de videovigilancia del SIS ECU 911 Zonal 6. Los

puntos de videovigilancia en la ciudad de Cuenca están conectados mediante enlaces dedicados de fibra óptica, lo que garantiza una conexión exclusiva y estable para cada cámara IP. Estos enlaces convergen en el router principal, que a su vez está interconectado con los servidores de streaming<sup>11</sup>, donde se gestionan y monitorean las transmisiones en tiempo real.

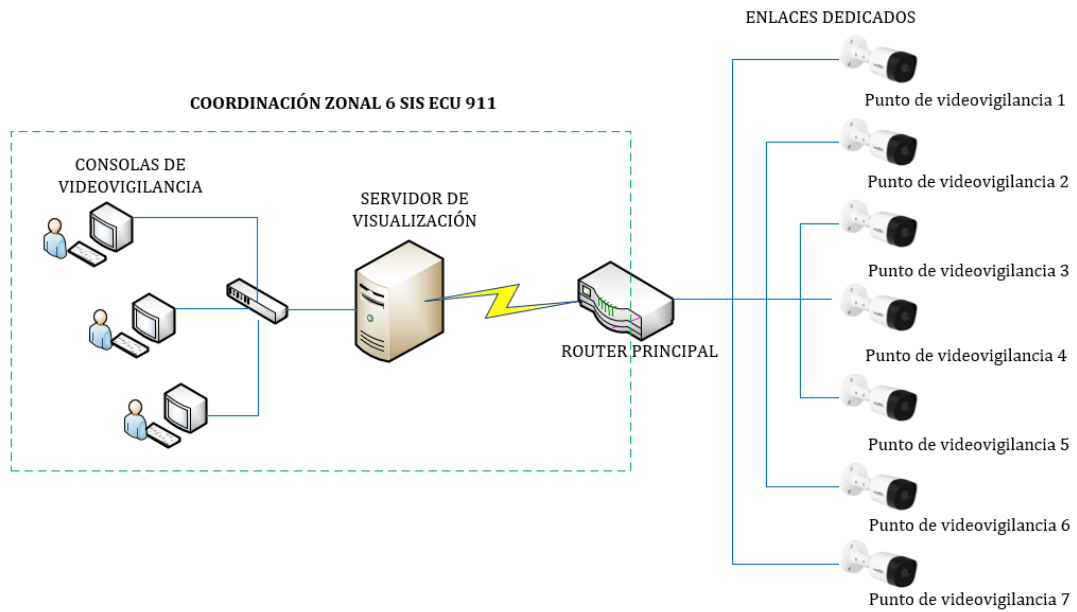


Figura 5. Topología del sistema de videovigilancia del SIS ECU 911.

### 2.2.2 Diagrama de red de los enlaces de datos utilizados

La Coordinación Zonal 6 del SIS ECU 911 tiene cobertura en las provincias de Azuay y Cañar, los proveedores de servicio de enlaces dedicados por fibra óptica son dos: ETAPA EP, que presta el servicio únicamente en la ciudad de Cuenca, y CNT EP, que provee el servicio para el resto de los cantones de la provincia de Azuay y para toda la provincia de Cañar. Todos los enlaces están enrutados hacia el Centro de Datos del SIS ECU 911 en Cuenca, como se muestra en la figura 6.

---

<sup>11</sup> Servidor de streaming: Es un sistema que permite la transmisión de contenido multimedia en tiempo real, recibe datos y los transmite a sus usuarios finales.



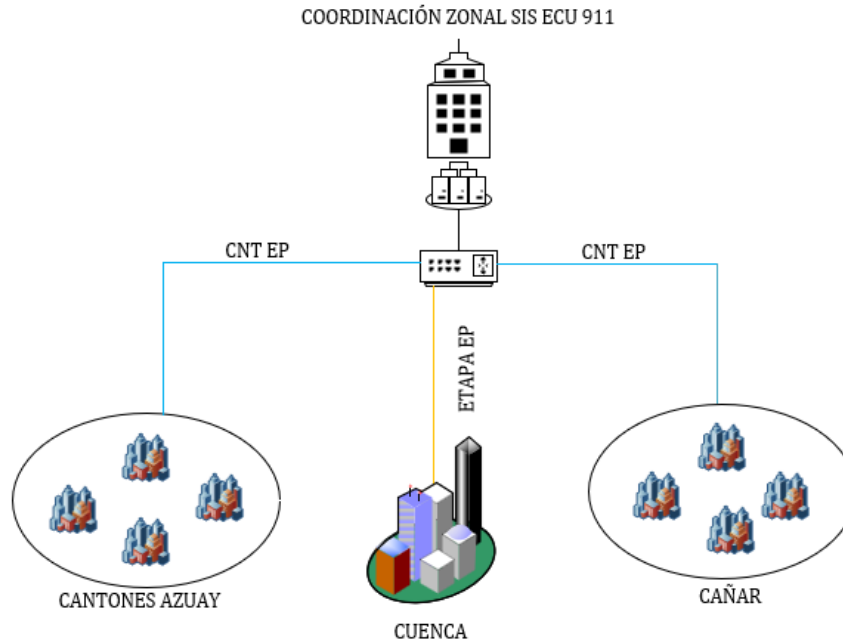


Figura 6. Diagrama de red de enlaces de datos con puntos de videovigilancia.

### 2.2.3 Puntos de videovigilancia

Un punto de videovigilancia es el lugar específico donde se instala una cámara IP, utilizada para el monitoreo de seguridad y el registro de actividades de una zona determinada. La ubicación de estos puntos de videovigilancia es de carácter estratégico y se define en función de la necesidad de vigilancia en un sitio específico.

### 2.2.4 Tipos de cámaras

En el territorio de la Coordinación Zonal 6 hay alrededor de 388 cámaras de videovigilancia de dos tipos: fijas y PTZ<sup>12</sup>. A cada punto de videovigilancia se le ha asignado un direccionamiento IP específico, junto con credenciales de acceso vía web para la configuración de parámetros como red, movilidad de la cámara, calidad de imagen, entre otros.

En la Coordinación Zonal 6 del SIS ECU 911 se utilizan cuatro marcas diferentes de cámaras IP, tanto fijas como PTZ. Los modelos y marcas de estas cámaras se detallan en la tabla 2.

---

<sup>12</sup> PTZ: Pan-Tilt-Zoom (Cámaras con capacidad de Paneo, Inclinación y Zoom).

Marca	Modelo	Tipo
Tiandy	TV-NH62331	PTZ
Tiandy	TC-NH6506S2	Fija
Cemax	CMX-IPDC-28A2-133-I0412-TD	PTZ
Hikvision	DS-2DE7A232IW-AEB(T5)	PTZ
Dahua	DH-SD6CE225DB	PTZ

Tabla 2. Tipos de cámaras utilizados en el SIS ECU 911 Zonal Cuenca.

Las cámaras fijas se usan para el monitoreo exclusivo de un lugar o infraestructura de interés, sin necesidad de cambiar su ángulo de enfoque.

Las cámaras PTZ se utilizan cuando es necesario cambiar el campo de visión, permitiendo movimientos horizontales y verticales sobre grandes áreas para obtener un campo visual más amplio.

### 2.2.5 Enlaces de datos

Como se mencionó anteriormente, la conexión entre los puntos de videovigilancia y el resto de la topología se realiza mediante enlaces de datos dedicados de fibra óptica. El ancho de banda asignado es de 2 Mbps para puntos de videovigilancia que poseen una sola cámara y 3 Mbps para puntos donde existen dos cámaras (fija y PTZ).

### 2.2.6 Direccionamiento IP

El direccionamiento IP utilizado para cada uno de los puntos de videovigilancia es de clase A, con una máscara de subred /29, lo que permite albergar hasta 6 hosts utilizables por subred.

Ciudad	Cámara	IP
Azogues	AZO-001-DOMO	10.2.X.X
Biblián	BIB-002-FIJA	10.2.X.X
Ponce Enríquez	CAM-001-DOMO	10.2.X.X
Ponce Enríquez	CAM-002-DOMO	10.2.X.X
Cañar	CAÑ-003-DOMO	10.2.X.X
Cañar	CAÑ-013-DOMO	10.2.X.X
Chordeleg	CHOR-002-DOMO	10.2.X.X
Cuenca	CUE-002-DOMO	10.2.X.X
Cuenca	CUE-005-DOMO	10.2.X.X
Déleg	DEL-001-DOMO	10.2.X.X
Girón	GIR-003-DOMO	10.2.X.X
Gualaceo	GUALA-002-DOMO	10.2.X.X

Gualaceo	GUALA-006-DOMO	10.2.X.X
Girón	LEN-312-FIJA	10.2.X.X
Nabón	NAB-001-DOMO	10.2.X.X
Oña	OÑA-001-DOMO	10.2.X.X
Paute	PAU-006-DOMO	10.2.X.X
Pucará	PUC-001-DOMO	10.2.X.X
Sevilla de Oro	SEV-001-DOMO	10.2.X.X
San Fernando	SFER-001-DOMO	10.2.X.X
Sigsig	SIGSIG-001-DOMO	10.2.X.X
Santa Isabel	STAISA-001-DOMO	10.2.X.X
Suscal	SUS-002-DOMO	10.2.X.X
El Tambo	TAM-001-DOMO	10.2.X.X
La Troncal	TRON-003-DOMO	10.2.X.X
Santa Isabel	UNI-009-DOMO	10.2.X.X

*Tabla 3. Ejemplos de direccionamiento IP.*

### **2.2.7 VMS (Video Management System)**

El Sistema de Gestión de Video (VMS) es una plataforma tecnológica que permite la gestión, monitoreo y supervisión de las cámaras instaladas en los diversos puntos de videovigilancia. Este sistema permite el monitoreo en tiempo real de todas las imágenes captada por las cámaras, además de la grabación y reproducción de video.

El VMS también permite la creación de usuarios y la asignación de perfiles de acceso para cada uno de los operadores de los puntos de videovigilancia, garantizando un control adecuado sobre quién puede visualizar o manipular las grabaciones y transmisiones en tiempo real.

### **2.2.8 IVS (Intelligent Video Surveillance)**

La Videovigilancia Inteligente (IVS) es el sistema de videovigilancia utilizado por el SIS ECU 911, esta es una solución integral desarrollada por Huawei que permite la integración de cámaras IP de diferentes marcas comerciales a través del protocolo ONVIF<sup>13</sup>, proporcionando soluciones de seguridad robustas para monitoreo de ciudades, infraestructura, vialidad, entre otros.

---

<sup>13</sup> ONVIF: Open Network Video Interface Forum, es un estándar global que facilita la interoperabilidad entre dispositivos de seguridad basados en IP, permitiendo que trabajen juntos sin problemas.

IVS permite la integración tanto de cámaras fijas como PTZ, y su interfaz de administración facilita la creación de usuarios para la visualización, asignación de dispositivos por usuario y grabación de los sistemas integrados; cabe destacar que esta solución permite la creación de usuarios con perfiles de acceso específicos, lo que garantiza un control adecuado sobre los permisos de visualización y operación.

## **2.3 Criterios generales de seguridad de la información aplicados en los sistemas de videovigilancia del SIS ECU 911**

El SIS ECU 911 maneja procedimientos, reglamentos y protocolos de seguridad de la información de uso interno exclusivamente, los cuáles no pueden ser compartidos con el público en general, por lo que no se pueden mostrar en el presente trabajo, sin embargo, el personal técnico del SIS ECU 911 compartió criterios generales de seguridad de la información que se pueden difundir públicamente, los cuáles se recogen a continuación.

### **2.3.1 Seguridad de redes para consolas de videovigilancia**

Cada puesto de trabajo de los operadores de videovigilancia tiene asignada una dirección IP estática, la cual se gestiona mediante permisos y reglas específicas aplicadas a través del firewall institucional. Estas estaciones de trabajo están aisladas en un segmento de red independiente, lo que garantiza que no puedan interactuar con otros segmentos dentro de la Coordinación Zonal, reforzando así la seguridad y el control sobre el acceso a los datos.

### **2.3.2 Seguridad Perimetral**

Dentro del centro de datos, existen equipos de seguridad perimetral que definen controles de acceso y segmentación de redes a través de VLAN, separando todo el tráfico en función de la operatividad y los servicios que se utilicen.

### **2.3.3 Seguridad Física**

En los puntos de videovigilancia ubicados en los cantones, los dispositivos de red están instalados en armarios de datos que contienen equipos como ONT (Terminal de Red Óptica) y transceptores de fibra óptica. Estos dispositivos cuentan con puertos Ethernet adicionales que permiten la conexión de más cámaras o dispositivos; sin embargo, es

responsabilidad del proveedor del servicio de datos bloquear los puertos no utilizados y habilitar solo los necesarios, garantizando la seguridad del sistema. Además, la altura de instalación de estos armarios, que supera los 7 metros, dificulta el acceso físico a los equipos, proporcionando una capa adicional de protección frente a posibles manipulaciones.

#### 2.3.4 Controles de acceso

El sistema de videovigilancia cuenta con tres niveles de acceso para el personal, definidos según los roles y funciones que desempeñan. Los accesos están estrictamente condicionados a las tareas asignadas a cada rol, asegurando que solo el personal autorizado pueda acceder a las funciones y datos correspondientes. En la siguiente tabla se detallan las actividades, roles y niveles de acceso permitidos para el personal de videovigilancia.

Rol	Nivel de Acceso	Actividades
Evaluador de videovigilancia	Perfil de visualización y monitoreo de video	Monitoreo y visualización de cámaras 24/7
Supervisor de videovigilancia	Perfil de administrador superior	Control sobre los evaluadores Accesos a registros de video Respuestas a peticiones jurídicas
Personal de tecnología	Perfil de acceso total	Administración general del sistema de videovigilancia

*Tabla 4. Roles usados para los usuarios que monitorean el sistema de videovigilancia.*

Como se evidencia en la tabla 4, brindar acceso total al personal de tecnología presenta un riesgo de seguridad. Aunque este personal es responsable de proporcionar soporte técnico en diversas áreas, esta práctica puede considerarse inadecuada y arriesgada.

## 2.4 Vulnerabilidades identificadas y reconocidas en el sistema de videovigilancia del SIS ECU 911

A lo largo de todos los años en el que el SIS ECU 911 se encuentra funcionando, específicamente desde el año 2012, se han detectado vulnerabilidades de seguridad en el

sistema de videovigilancia que el personal técnico ha ido tratando y documentando, este registro también es de uso interno, pero se ha podido obtener información general sobre estos eventos de seguridad.

#### **2.4.1 Registro histórico de vulnerabilidades encontradas sobre los sistemas de videovigilancia del SIS ECU 911**

Las vulnerabilidades que ha enfrentado el sistema de videovigilancia del SIS ECU 911 durante su funcionamiento se agrupan en las siguientes categorías:

- **Brechas de seguridad en credenciales**

La gestión de las 388 cámaras desplegadas en las provincias de Azuay y Cañar presenta un desafío significativo en cuanto al manejo de credenciales. Dado que cada dispositivo requeriría credenciales únicas, esto complicaría la vinculación con los servicios de visualización y grabación, aumentando el tiempo necesario para su implementación. Por esta razón, se ha decidido estandarizar una única credencial de acceso para todas las cámaras, simplificando el proceso y mejorando la eficiencia operativa, sin embargo, esta práctica presenta un riesgo considerable para la seguridad del sistema de videovigilancia, ya que compromete la individualidad de las credenciales y facilita posibles accesos no autorizados.

- **Configuraciones predeterminadas de los dispositivos**

Al configurar cámaras IP nuevas, muchos parámetros por defecto del equipo se mantienen sin modificaciones. No se realizan cambios específicos en cuanto a tipos de seguridad o encriptación de credenciales, priorizándose en su lugar configuraciones de red, giros automáticos, calidad de video y parámetros de visualización.

- **Reinicios fortuitos**

La energía eléctrica utilizada en los puntos de videovigilancia proviene del tendido eléctrico más cercano, generalmente postes de redes de distribución, sin embargo, los cortes de energía o sobrecargas de tensión pueden provocar que los equipos se apaguen y se restablezcan a sus configuraciones de fábrica. Cuando esto ocurre, las credenciales de los dispositivos se restablecen a valores predeterminados, los cuales son fácilmente accesibles mediante búsquedas en Internet. Esto representa un riesgo significativo para la seguridad del sistema, ya

que permite a personas no autorizadas acceder a las cámaras y comprometer potencialmente la integridad del sistema de videovigilancia.

## **2.5 Análisis de la seguridad del Protocolo RTSP en el sistema de video vigilancia del SIS ECU 911**

En esta sección se aborda la revisión práctica de la seguridad del protocolo RTSP en el sistema de videovigilancia del SIS ECU 911, así como las pruebas que fueron planificadas y ejecutadas. Dichas pruebas se enfocaron en las vulnerabilidades identificadas en el protocolo RTSP, las cuales han coincidido con los incidentes de seguridad registrados por el personal técnico del SIS ECU 911. Las pruebas realizadas durante la revisión de seguridad se clasifican en dos tipos:

- **Pruebas automatizadas:** Estas pruebas se centran en la identificación de vulnerabilidades presentes en las cámaras IP y en la configuración del protocolo RTSP. Su objetivo es detectar debilidades que puedan ser explotadas por un atacante. Para llevar a cabo estas pruebas, se emplearon herramientas especializadas como Nessus.
- **Pruebas manuales:** Estas pruebas están orientadas a evaluar las vulnerabilidades comunes del protocolo RTSP en las cámaras del SIS ECU 911, a través de estas pruebas, se busca analizar detalladamente los posibles riesgos que, en ocasiones, no son detectados por las herramientas automatizadas.

Las pruebas se llevaron a cabo durante un periodo de 30 días calendario, tiempo en el cual realizaron actividades como la captura del tráfico de red, la configuración de herramientas de análisis de vulnerabilidades, la ejecución de las pruebas planificadas y la revisión de hallazgos.

### **2.5.1 Herramientas utilizadas para análisis de vulnerabilidades**

En esta sección se mencionan las herramientas empleadas en las diferentes etapas de las pruebas realizadas durante la revisión:

- **Nmap:** Herramienta utilizada para el escaneo y la exploración de redes. Permite descubrir dispositivos, identificar puertos abiertos y servicios activos, así como ejecutar scripts que posibilitan un análisis de seguridad más detallado.

- **Wireshark:** Herramienta usada para capturar y examinar en tiempo real todo el tráfico que circula sobre una red específica, con Wireshark, es posible analizar los paquetes de datos que se envían y reciben, detectar problemas en la red, identificar vulnerabilidades y verificar el funcionamiento de los protocolos de red.
- **Nessus:** Herramienta automatizada de análisis de vulnerabilidades, empleada para identificar fallos de seguridad en sistemas, dispositivos, redes y aplicaciones. Nessus facilita la realización de pruebas de penetración y simulaciones de ataques, ayudando a identificar y mitigar riesgos de seguridad.

### **2.5.2 Escaneo de red, puertos abiertos y tráfico RTSP de los hosts de prueba**

Como punto de partida, se llevó a cabo un análisis de la topología de la red, complementado con la información proporcionada por el personal de tecnología del SIS ECU 911. Para este análisis se utilizó a la herramienta Nmap con el objetivo de escanear la red, identificar los puertos abiertos y detectar los dispositivos activos. Como criterio general en esta revisión, se buscó específicamente dispositivos que mantuvieran el puerto 554 abierto, que es el utilizado por el protocolo RTSP.

El análisis se realizó dentro de la red del SIS ECU 911 Zonal 6. En la figura 7, se puede observar que Nmap detectó un número considerable de dispositivos con el puerto 554 abierto, estos dispositivos coinciden con las direcciones IP de las cámaras que había informado previamente el personal de tecnología.



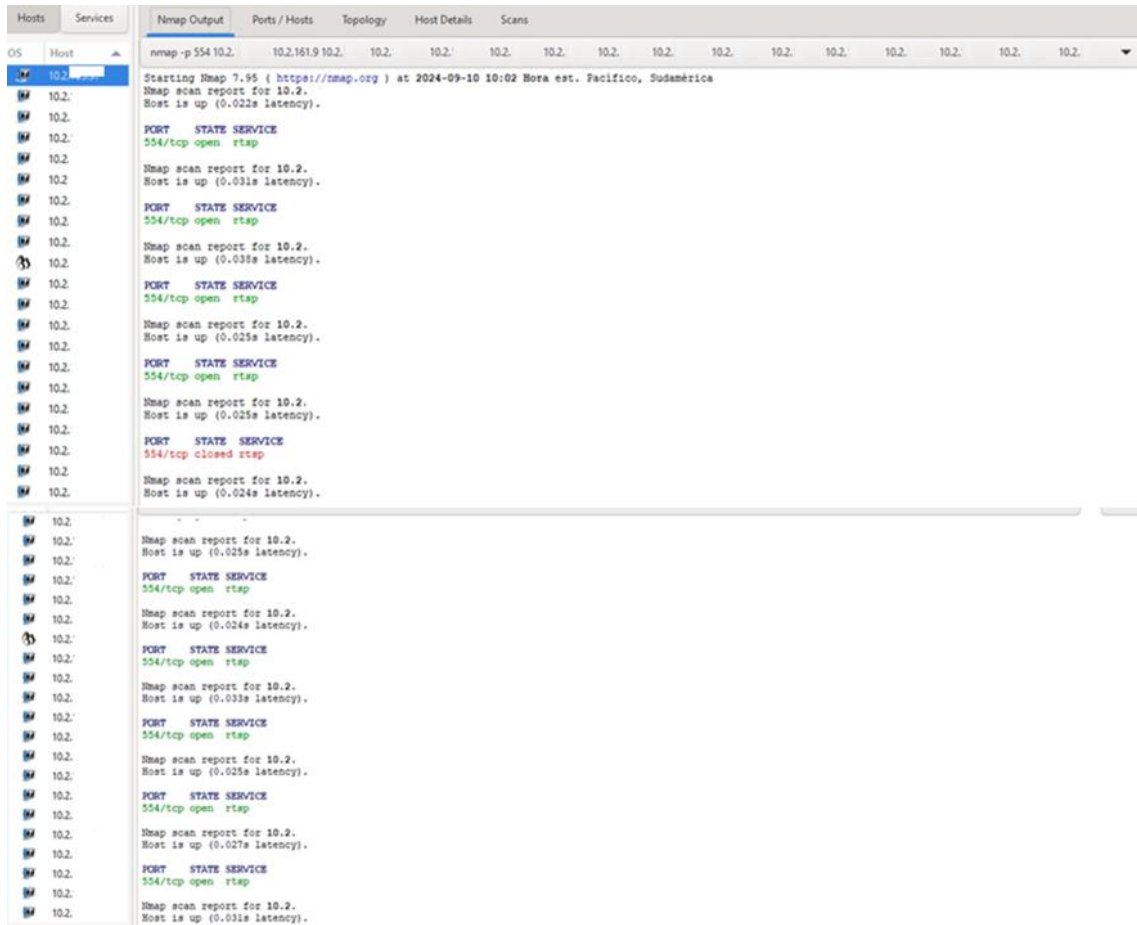


Figura 7. Escaneo de dispositivos que utilicen RTSP mediante Nmap.

Mediante la misma herramienta Nmap, se realizaron escaneos sobre los dispositivos detectados con el fin de obtener más información sobre ellos, como el sistema operativo y puertos adicionales abiertos. Una muestra de la información obtenida se observa en la figura 8.

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap-O 10.2.	10.2.	10.2.	10.2.	10.2.

```

Nmap scan report for 10.2
Host is up (0.0034s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
3001/tcp   open  nessus
Aggressive OS guesses: RGB Spectrum MediaWall 1500 video processor (98%), Lexmark X4530, X4650, 4800, or X9575 wireless printer (97%), Lexmark X4850 or X6570 printer (96%), Linux 2.6.10 - 2.6.13 (embedded) (96%), Lexmark X6650 printer (95%), DD-WRT v24 (Linux 2.6.22) (95%), Dell 2330dn printer (95%), Linux 2.6.9 - 2.6.33 (94%), Axis network camera (Linux 2.6.16 - 2.6.20) (94%), Roku HD1500 media player (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

Nmap scan report for 10.2.
Host is up (0.0032s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
8000/tcp  open  http-alt
8443/tcp  open  https-alt
Aggressive OS guesses: Linux 3.2 - 4.14 (96%), Linux 3.10 - 4.11 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (93%), Android 6 - 9 (Linux 3.18) (93%), Linux 3.2 - 3.16 (93%), Android 5.1 (92%), Linux 3.18 (92%), Linux 2.6.32 (91%), DD-WRT (Linux 3.18) (91%), Linux 4.4 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

Nmap scan report for 10.2.
Host is up (0.0058s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
8000/tcp  open  http-alt
8443/tcp  open  https-alt
Aggressive OS guesses: Linux 3.2 - 4.14 (96%), Linux 3.10 - 4.11 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (93%), Android 5.1 (93%), Android 6 - 9 (Linux 3.18) (93%), Linux 3.2 - 3.16 (93%), Linux 3.18 (92%), DD-WRT (Linux 3.18) (92%), Linux 4.4 (92%), Linux 2.6.32 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

Nmap scan report for 10.2.
Host is up (0.0054s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp
3001/tcp  open  nessus
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
9100/tcp  open  jetdirect
Device type: general purpose|printer|broadband router|media device|phone|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X (96%), Lexmark embedded (95%), Google embedded (92%), HP embedded (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:lexmark:cs410dn cpe:/o:google:android:4.2.2 cpe:/o:linux:linux_kernel:3.4 cpe:/o:google:android:2 cpe:/h:hp:storageworks_p2000_g3_msa_fc2fiscai_dual_combo_controller_1ff_array_system
Aggressive OS guesses: Linux 2.6.32 - 3.5 (96%), Lexmark CS410dn printer (95%), Linux 2.6.38 - 3.0 (94%), Linux 2.6.32 - 3.10 (93%), Vyatta (Linux 3.0.23) (92%), Linux 2.6.32 - 2.6.35 (92%), Google Home device (92%), Android 4.2.2 (Linux 3.4) (92%), Linux 2.6.32 - 3.13 (91%), Linux 2.6.38 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-17 10:40 Hora est. Pacifico, Sudamérica
Nmap scan report for 10.2.
Host is up (0.0051s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp
3001/tcp  open  nessus
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
9100/tcp  open  jetdirect
Device type: general purpose|printer|broadband router|phone|media device|storage-misc
Running (JUST GUESSING): Linux 2.6.X|3.X (96%), Lexmark embedded (95%), Google Android 4.2.X (92%), Google embedded (92%), HP embedded (91%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3 cpe:/h:lexmark:cs410dn cpe:/o:google:android:4.2.2 cpe:/o:linux:linux_kernel:3.4 cpe:/o:google:android:2 cpe:/h:hp:storageworks_p2000_g3_msa_fc2fiscai_dual_combo_controller_1ff_array_system
Aggressive OS guesses: Linux 2.6.32 - 3.5 (96%), Lexmark CS410dn printer (95%), Linux 2.6.38 - 3.0 (94%), Linux 2.6.32 - 3.10 (93%), Vyatta (Linux 3.0.23) (93%), Android 4.2.2 (Linux 3.4) (92%), Linux 2.6.32 - 2.6.35 (92%), Linux 3.1 (92%), Google Home device (92%), Linux 2.6.32 - 3.13 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

Nmap scan report for 10.2.
Host is up (0.0046s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp
3001/tcp  open  nessus
8080/tcp  open  http-proxy
9100/tcp  open  jetdirect
Aggressive OS guesses: RGB Spectrum MediaWall 1500 video processor (98%), Lexmark X4530, X4650, 4800, or X9575 wireless printer (97%), Lexmark X4850 or X6570 printer (96%), Lexmark X6650 printer (96%), Linux 2.6.10 - 2.6.13 (embedded) (96%), Axis network camera (Linux 2.6.16 - 2.6.20) (96%), Dell 2330dn printer (95%), DD-WRT v24

```

Figura 8. Escaneo para recabar información adicional de los dispositivos detectados.

En este punto, y aprovechando la revisión que ya se estaba llevando a cabo con Nmap, se realizó la primera evaluación de la seguridad en la configuración del protocolo RTSP mediante la búsqueda de URLs conocidas que podrían representar un riesgo si se encontraran desprotegidas en los dispositivos detectados. Una muestra de la información obtenida se observa en la figura 9.

```

PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| errors:
|   rtsp://10.2.   /PSIA/Streaming/channels/h264
|   rtsp://10.2.   /Streaming/Unicast/channels/101
|   rtsp://10.2.   /streaming/mjpeg
| other responses:
|   401:
|     rtsp://10.2.   1/
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| errors:
|   rtsp://10.2.   /PSIA/Streaming/channels/0?videoCodecType=H.264
|   rtsp://10.2.   /PSIA/Streaming/channels/h264
|   rtsp://10.2.   /Streaming/Unicast/channels/101
|   rtsp://10.2.   /streaming/mjpeg
| other responses:
|   401:
|     rtsp://10.2.   /1/stream1
|     rtsp://10.2.   /4
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| other responses:
|   401:
|     rtsp://10.2.   /4
|     rtsp://10.2.   /CAM_ID.password.mp2
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| other responses:
|   401:
|     rtsp://10.2.   /0
|     rtsp://10.2.   /12
|     rtsp://10.2.   /11
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| errors:
|   rtsp://10.2.   /12
|   rtsp://10.2.   /4
|   rtsp://10.2.   /11
| other responses:
|   401:
|     rtsp://10.2.   /1
|     rtsp://10.2.   /0/videol
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| errors:
|   rtsp://10.2.1   /4
|   rtsp://10.2.1   /11
|   rtsp://10.2.1   /12
| other responses:
|   401:
|     rtsp://10.2.   /
|     rtsp://10.2.   /0
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| other responses:
|   401:
|     rtsp://10.2.   1/
|     rtsp://10.2.   1/0
|     rtsp://10.2.   1/1/1:1/main
|     rtsp://10.2.   1/0/videol
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| other responses:
|   401:
|     rtsp://10.2.   /0/videol
|     rtsp://10.2.   /1
|     rtsp://10.2.   /1.AMF
|     rtsp://10.2.   /
|
PORT STATE SERVICE
554/tcp open  rtsp
| rtsp-url-brute:
| other responses:
|   401:
|     rtsp://10.2.   /12
|     rtsp://10.2.   /4
|     rtsp://10.2.   /CAM_ID.password.mp2
|     rtsp://10.2.   /CH001.sdp
|     rtsp://10.2.   /GetData.cgi
|

```

Figura 9. Identificación de URLs conocidas desprotegidas.

La revisión de las URLs conocidas no pudo identificar ninguna vulnerabilidad, ya que todas las pruebas realizadas sobre los hosts detectados arrojaron uno de los siguientes resultados: o bien las URLs no estaban presentes, o devolvían un código de error 401 (No autorizado), como se muestra en la imagen anterior.

Como resultado de la revisión realizada con Nmap, se pudo esquematizar la topología utilizada en el sistema de videovigilancia del SIS ECU 911 Zonal 6. En esta topología, los puntos de videovigilancia (equivalentes a una cámara IP) se consideran como nodos finales. En la figura 10, se muestra un diagrama básico de dicha topología.

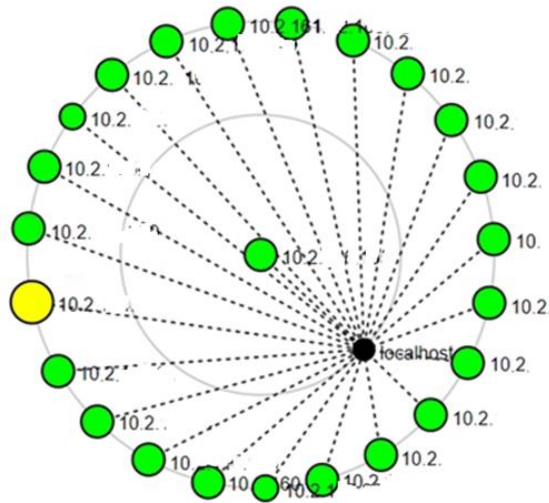


Figura 10. Diagrama de la topología de red del sistema de videovigilancia del SIS ECU 911 Zonal 6.

Con la topología de red identificada, se procedió a realizar un análisis del tráfico de paquetes utilizando Wireshark, filtrando específicamente todos los paquetes que utilizan el protocolo RTSP. En la figura 11, se puede observar parte de los paquetes capturados por Wireshark.

The screenshot shows the Wireshark interface with a filter set to 'rtsp'. The packet list pane displays several RTSP packets. The selected packet (No. 57455) is expanded to show its details, including TCP and RTSP headers and flags.

No.	Time	Source	Destination	Protocol	Length	Info
45743	49.057176	10.2.	10.2.	RTSP	397	Continuation
45751	49.069307	10.2.	10.2.	RTSP	98	Continuation
46762	51.072641	10.2.	10.2.	RTSP	303	Continuation
46777	51.088133	10.2.	10.2.	RTSP	98	Continuation
55682	71.274010	10.2.	10.2.	RTSP	361	Continuation
55684	71.279825	10.2.	10.2.	RTSP	98	Continuation
56468	74.311900	10.2.	10.2.	RTSP	373	Continuation
56470	74.319617	10.2.	10.2.	RTSP	98	Continuation
57449	76.883646	10.2.	10.2.	RTSP	359	Continuation
57455	76.908436	10.2.	10.2.	RTSP	98	Continuation
57830	77.071160	10.2.	10.2.	RTSP	360	Continuation

Transmission Control Protocol, Src Port: 554, Dst Port: 8434, Seq: 1, Ack: 306, Len: 44

- Source Port: 554
- Destination Port: 8434
- [Stream index: 349]
- [Stream Packet Number: 6]
- [Conversation completeness: Complete, WITH\_DATA (47)]
  - ...1. .... = RST: Present
  - ...0. .... = FIN: Absent
  - .... 1... = Data: Present
  - .... .1.. = ACK: Present
  - .... ..1. = SYN-ACK: Present
  - .... ...1 = SYN: Present
- [Completeness Flags: R·DASS]
- [TCP Segment Len: 44]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 1206606947
- [Next Sequence Number: 45 (relative sequence number)]
- Acknowledgment Number: 306 (relative ack number)
- Acknowledgment number (raw): 3968927058

Figura 11. Captura de paquetes RTSP mediante WireShark.

Se pueden evidenciar las capturas de paquetes RTSP al analizar el tráfico desde un punto de origen (SIS ECU 911 Cuenca) hacia los puntos de videovigilancia como destino, en la siguiente figura, se puede apreciar los componentes de una entrega RTSP.

No.	Time	Source	Destination	Protocol	Length	Info
9103	717.507863	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9210	728.166877	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9214	728.635047	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
9214	728.648842	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
9349	740.777061	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9349	740.824154	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
9394	744.642271	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9432	748.006496	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9552	758.244319	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9640	766.031319	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9679	769.421285	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
9679	769.437045	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
9818	781.632741	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
9828	782.455965	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
9828	782.478561	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
9887	787.661149	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
9887	787.676980	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
9958	793.970223	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
1028	821.847792	10.2.	10.2.	RTSP	76	OPTIONS * RTSP/1.0
1042	833.283744	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
1042	833.296244	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
1043	834.167877	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
1043	834.184864	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK
1043	834.256612	10.2.	10.2.	RTSP	85	OPTIONS * RTSP/1.0
1043	834.281339	10.2.	10.2.	RTSP	212	Reply: RTSP/1.0 200 OK

> Frame 964093: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF...  
 > Ethernet II, Src: HewlettPacka\_39:80:c0 (74:46:a0:39:80:c0), Dst: H3Ctechnology\_26:e8:61 (38:22:00:00:00:00)  
 > Internet Protocol Version 4, Src: 10.2., Dst: 10.2.:  
 > Transmission Control Protocol, Src Port: 33022, Dst Port: 554, Seq: 1, Ack: 1, Len: 22  
 > Real Time Streaming Protocol  
 > Request: OPTIONS \* RTSP/1.0\r\n\r\n

Figura 12. Componentes de una entrega RTSP.

## 2.6 Pruebas automatizadas en Nessus

En el siguiente apartado se detallan los pasos llevados a cabo para la ejecución de las pruebas automatizadas, que se realizaron utilizando la herramienta Nessus, y consistieron en dos pruebas separadas, cada una configurada con parámetros distintos y aplicadas sobre un número específico de hosts (cámaras IP). En la figura 13, se puede observar la configuración de la primera prueba a realizar.

rtsp 2 / Configuration  
 < Back to Scan Report

Settings	Credentials	Plugins
<b>BASIC</b> <ul style="list-style-type: none"> <li>General</li> <li>Schedule</li> <li>Notifications</li> </ul>		
<b>DISCOVERY</b>		
<b>ASSESSMENT</b>		
<b>REPORT</b>		
<b>ADVANCED</b>		
Name	rtsp 2	
Description	strp scan 2	
Folder	My Scans	
Targets	10.2.X.X, 10.2.X.X, 10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X, X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X,10.2.X.X, X,10.2.X.X,10.2.X.X	

Figura 13. Configuración de host para prueba.

En la figura 14, se muestra la configuración de los puertos a ser analizados, en este caso, el análisis se centrará en el puerto 554.

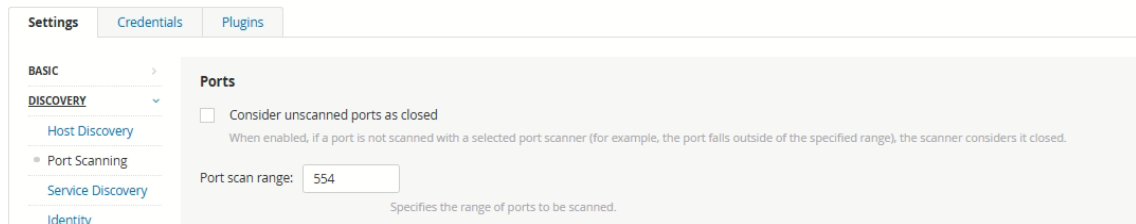


Figura 14. Configuración de los puertos a ser analizados.

En la figura 15, se muestra la selección del tipo de análisis que se desea realizar. Para esta prueba, se incluyó la detección de vulnerabilidades mediante ataques de fuerza bruta.

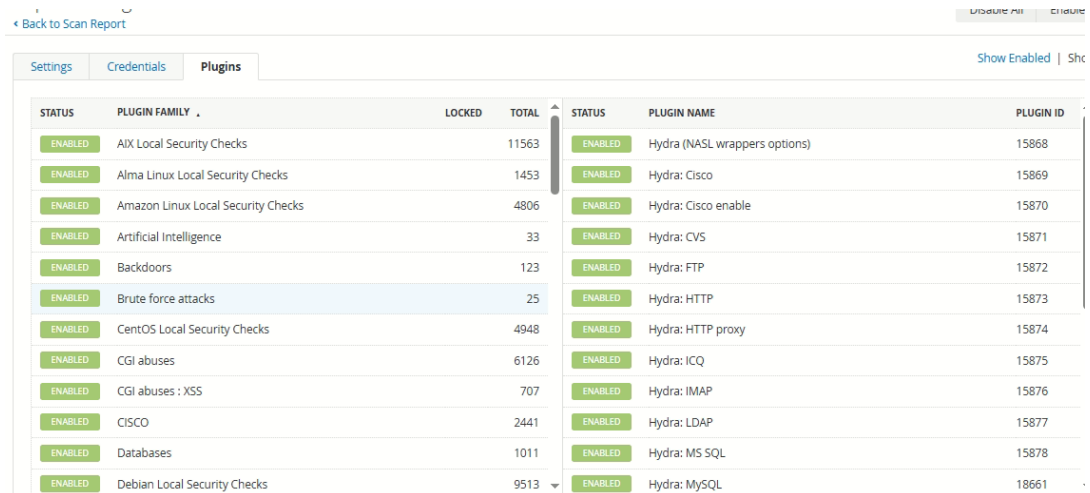


Figura 15. Configuración del tipo de ataque que se llevará a cabo.

La figura 16 muestra un resumen de los hallazgos obtenidos a partir de la prueba realizada sobre los hosts seleccionados.

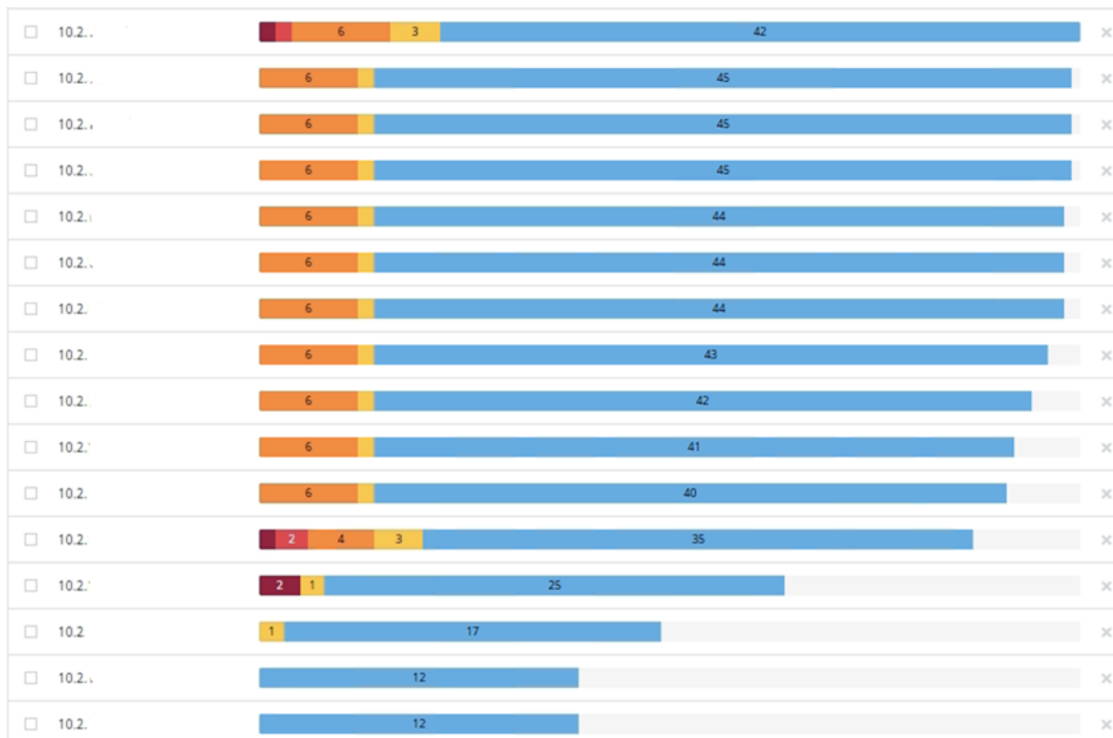


Figura 16. Resultados de la primera prueba obtenidos por Nessus.

El resultado que se muestra en la figura 16 corresponde a las vulnerabilidades encontradas en todos los hosts (cámaras IP) seleccionados. Los colores representados en el gráfico indican el nivel de criticidad de las vulnerabilidades: rojo oscuro (crítica), rojo (alta), anaranjado (media), amarillo (baja) y azul (informativa).

Para este análisis de vulnerabilidades, se ha puesto especial atención en aquellas clasificadas como críticas y altas, debido a su potencial impacto en el uso del protocolo RTSP y el correcto funcionamiento de las cámaras IP. Las vulnerabilidades críticas y altas presentan un mayor riesgo de ser explotadas por atacantes, ya que comprometen directamente la integridad, disponibilidad y confidencialidad de la transmisión de video.

En los resultados, también se observa un número considerable de vulnerabilidades clasificadas como informativas. Estas no han sido consideradas en el análisis, ya que no representan fallas de seguridad directas, sin embargo, proporcionan información adicional sobre la infraestructura de los hosts escaneados, como configuraciones, versiones de software o características de red. Cabe destacar que estas vulnerabilidades están descritas con mayor detalle en un informe generado por la herramienta Nessus, el cual se encuentra incluido en los anexos de este documento.





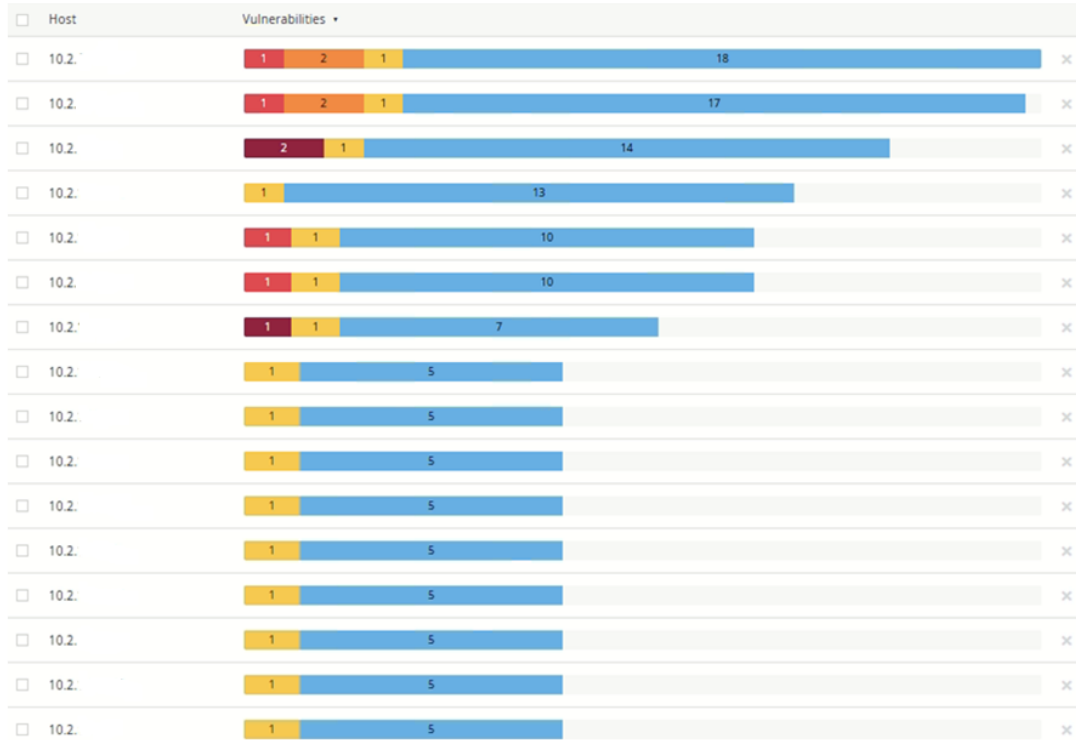


Figura 19. Resultados de la segunda prueba obtenidos por Nessus.

De manera similar, en esta prueba se obtuvieron resultados equivalentes en cuanto al tipo de vulnerabilidades encontradas y su nivel de criticidad. En la siguiente tabla se listan las vulnerabilidades detectadas en ambas pruebas automatizadas. Como se mencionó previamente, para el análisis se han considerado únicamente aquellas con mayor criticidad.

Tipo de vulnerabilidad	Criticidad
Detección de protocolo SSL 2 y 3	Crítico
Desbordamientos de buffer (UPnP)	Crítico
Vulnerabilidad Heartbleed	Alta
Algoritmos de hashing débiles	Alta
Múltiples vulnerabilidades Treck TCP/IP	Crítico
Nombre predeterminado público de SNMP	Alta

Tabla 5. Vulnerabilidades obtenidas de las pruebas automatizadas.

Para facilitar la comprensión de las vulnerabilidades identificadas, cada una de ellas será descrita en detalle en el Anexo 1 de este trabajo.

## 2.7 Pruebas manuales para identificación de vulnerabilidades

Para la realización de estas pruebas, se seleccionó una muestra de 10 cámaras en distintas ubicaciones, se utilizaron cada uno de los tipos de cámaras existentes con el fin de analizar sus configuraciones y vulnerabilidades. Estas pruebas se realizaron de forma manual, debido a que las cámaras IP pueden tener configuraciones particulares que requieren un análisis más detallado. El listado de las cámaras IP utilizadas para las pruebas manuales se encuentra en la tabla 6.

Ítem	Cámara	Marca	Tipo	Direccionamiento
1	AZO-002	Hikvision	PTZ	10.2.X.X
2	AZO-010	Tiandy	Fija	10.2.X.X
3	CAÑ-006	Hikvision	PTZ	10.2.X.X
4	CUE-123	Hikvision	PTZ	10.2.X.X
5	CUE-048	Tiandy	PTZ	10.2.X.X
6	CUE-135	Cemax	PTZ	10.2.X.X
7	CUE-050	Tiandy	Fija	10.2.X.X
8	GUALA-003	Hikvision	PTZ	10.2.X.X
9	TRON-004	Dahua	PTZ	10.2.X.X
10	GIR-001	Tiandy	PTZ	10.2.X.X

*Tabla 6. Muestra de cámaras para realización de pruebas.*

En primer lugar, se llevó a cabo una revisión específica de las configuraciones de autenticación y encriptación implementadas en cada una de las cámaras IP de la muestra seleccionada.



Figura 20. Configuración de autenticación de una cámara Hikvision.

La figura 20 muestra los parámetros de autenticación disponibles en la configuración de seguridad de las cámaras de la marca Hikvision, mientras que la figura 22 presenta configuraciones similares en las cámaras de la marca Dahua. En contraste, la figura 21 evidencia la ausencia de este tipo de configuraciones en las cámaras PTZ de la marca Tiandy, lo que representa un posible riesgo de seguridad al no contar con mecanismos adecuados de protección durante el proceso de autenticación.

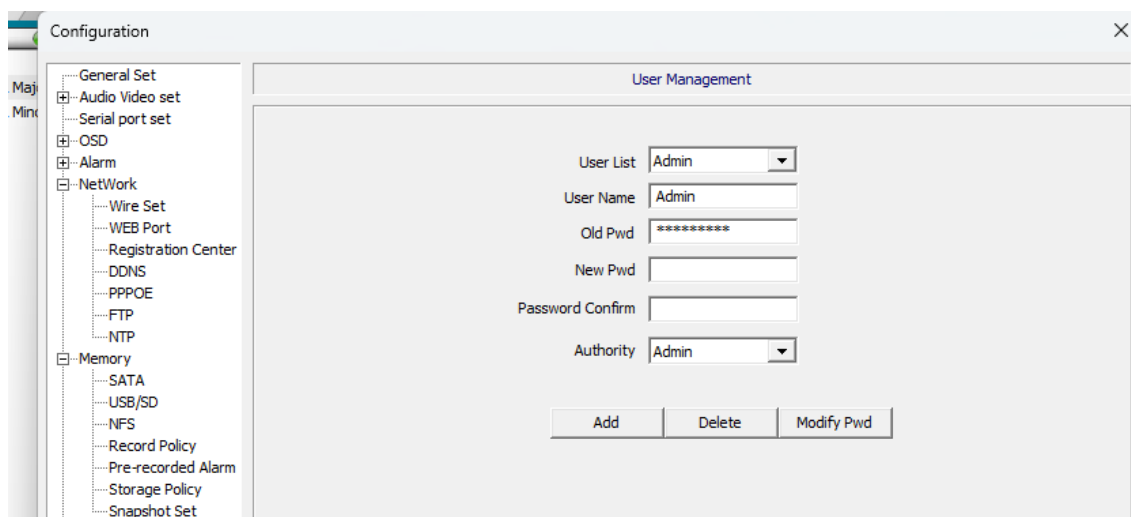


Figura 21. Parámetros de configuración de administración de usuario de una cámara Tiandy PTZ.

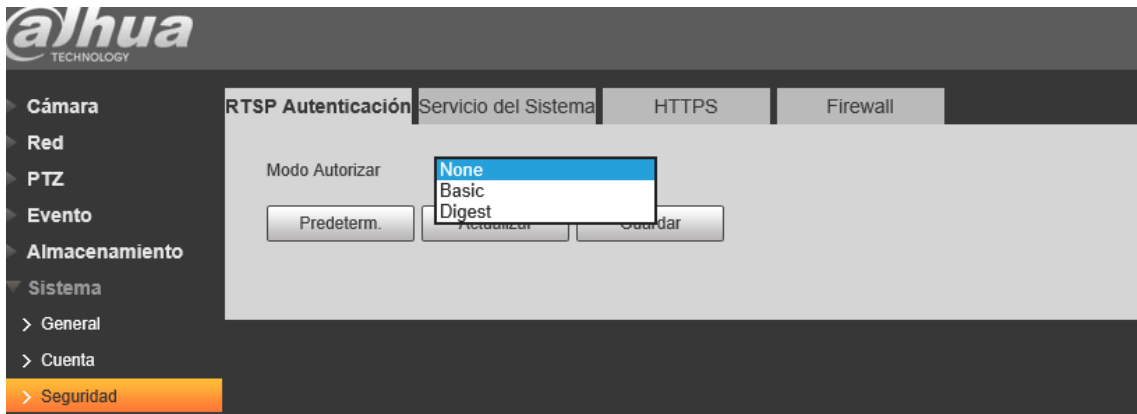


Figura 22. Configuración de autenticación de una cámara Dahua.

En las figuras 23 y 24, que muestran las configuraciones de las cámaras Cemax y Tiandy Fija, respectivamente, se puede observar que estas cámaras carecen de mecanismos de autenticación dentro de sus configuraciones.

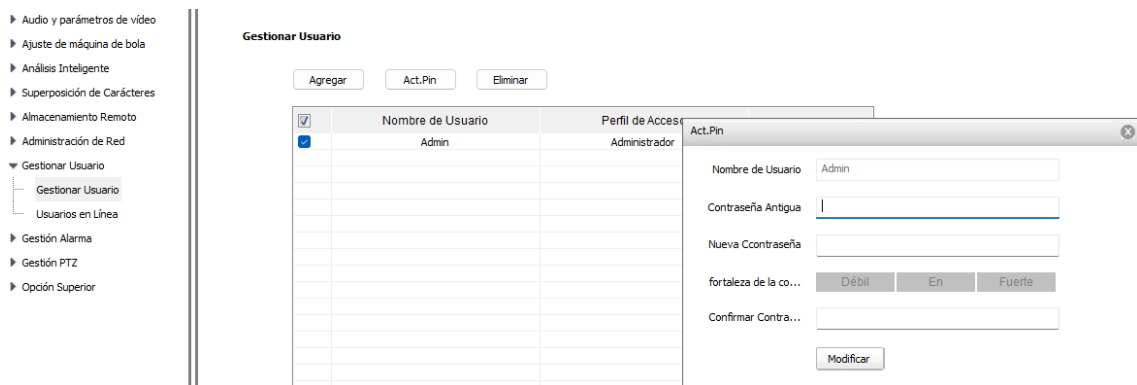


Figura 23. Parámetros de configuración de administración de usuario de una cámara CEMAX.

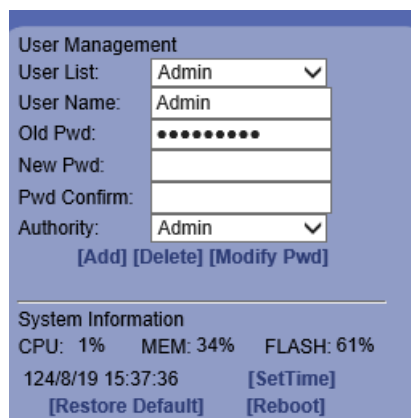


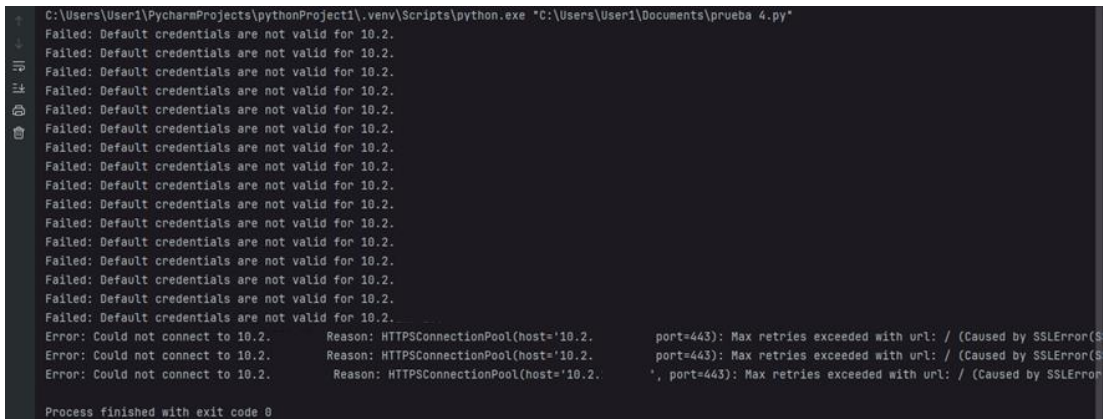
Figura 24. Parámetros de configuración de administración de usuario de una cámara TIANDY fija.

Se observó que los diferentes tipos de cámaras presentan parámetros de seguridad variables. Las cámaras de las marcas Dahua y Hikvision permiten la selección de

algoritmos de autenticación más avanzados, mientras que las cámaras Tiandy y Cemax solo ofrecen configuraciones de seguridad básicas. Esta diferencia se debe a que las cámaras Dahua y Hikvision corresponden a modelos más recientes y tecnológicamente avanzados, no siendo el caso de las cámaras Tiandy y Cemax, que han estado en operación por más de 10 años.

Adicionalmente, se llevó a cabo una serie de pruebas sobre la muestra de cámaras seleccionadas (en los casos donde la institución lo permitió, se amplió la muestra de análisis), estas pruebas se encuentran detalladas en el Anexo 1 del presente documento.

Es importante mencionar que, en algunas pruebas, una vez completado el proceso manual, se desarrollaron scripts para automatizar dichas pruebas. En la figura 25, se muestra la salida generada por uno de estos scripts.



```
C:\Users\User1\PycharmProjects\pythonProject1\.venv\Scripts\python.exe "C:\Users\User1\Documents\prueba 4.py"
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Failed: Default credentials are not valid for 10.2.
Error: Could not connect to 10.2. Reason: HTTPSConnectionPool(host='10.2. port=443): Max retries exceeded with url: / (Caused by SSLError(S
Error: Could not connect to 10.2. Reason: HTTPSConnectionPool(host='10.2. port=443): Max retries exceeded with url: / (Caused by SSLError(S
Error: Could not connect to 10.2. Reason: HTTPSConnectionPool(host='10.2. ', port=443): Max retries exceeded with url: / (Caused by SSLError(S
Process finished with exit code 0
```

Figura 25. Resultado de un script de uno de los scripts de pruebas utilizados.

## RESULTADOS Y CONCLUSIONES

En este último capítulo se revisarán los hallazgos encontrados durante la revisión y pruebas realizadas sobre el sistema de videovigilancia del SIS ECU 911 Zonal 6. Es importante señalar que las vulnerabilidades descritas complementan aquellas que se encuentran en el Anexo 1 del presente documento.

### 3.1 Vulnerabilidades identificadas

En la sección 2.6, *Pruebas automatizadas en Nessus*, se listaron las vulnerabilidades encontradas por la herramienta Nessus con un nivel de criticidad alto y crítico, las cuales se consideran de mayor impacto para la institución. A estas vulnerabilidades se deben sumar las identificadas mediante las pruebas manuales realizadas sobre las cámaras IP del sistema de videovigilancia, las cuales se detallan a continuación:

#### 3.1.1 Vulnerabilidades encontradas en cámaras Hikvision

El uso del algoritmo MD5 (ver figura 20) para la encriptación de contraseñas presenta un riesgo significativo, ya que permite que un atacante pueda descifrar contraseñas cortas mediante ataques de fuerza bruta, probando hasta encontrar un hash correspondiente. Cabe destacar que la obsolescencia de MD5 ha llevado a que sea considerado un algoritmo inseguro desde hace varios años.

#### 3.1.2 Vulnerabilidades encontradas en cámaras Dahua

Al revisar las configuraciones de las cámaras Dahua, se evidenció que cuentan con algoritmos de autenticación básicos, siendo la autenticación digest la opción más avanzada disponible (ver figura 22). Este mecanismo solo valida a los usuarios en entornos web y, aunque cifra las credenciales antes de transmitir las para evitar intercepciones, emplea el algoritmo MD5, el cual, como se mencionó anteriormente, es vulnerable.

#### 3.1.3 Vulnerabilidad en la integración de cámaras al sistema de visualización (IVS)

Si las cámaras IP no cuentan con un cifrado adecuado, los datos transmitidos al sistema de visualización pueden ser interceptados, lo que representa una vulnerabilidad que podría ser explotada por un atacante. En muchos casos, las credenciales de acceso utilizadas para la cámara y el servidor de streaming son las mismas, lo que incrementa el

riesgo de que la cámara sea comprometida a través de su proceso de autenticación. Por esta razón, es necesario implementar métodos más seguros de autenticación en el inicio de sesión, ya que éstos son un elemento clave en la vinculación de las cámaras IP con los servidores de videovigilancia.

En la revisión realizada, se identificaron algunos hallazgos vinculados al sistema IVS que es necesario resaltar:

- **Conexión mediante parámetros simples**

Los servicios de streaming suelen conectarse a las cámaras utilizando parámetros básicos, como la dirección IP, un ID y las credenciales de acceso. Esto resalta la importancia de proteger adecuadamente estos datos, ya que su exposición podría facilitar un acceso no autorizado y comprometer la seguridad del sistema.

The screenshot shows a configuration window titled "Agregar dispositivo". It contains the following fields and options:

- Nombre: CUE-XXX-DOMO
- Código: [Empty]
- Unidad de disco: ONVIF
- Nombre real: XXXXXX
- Contraseña: [Redacted]
- Confirmar contraseña: [Redacted]
- Servidor correspondiente: (Servidor predeterminado)
- Nota: Por seguridad, cambie la contraseña inicial de inmediato y recuerde cambiarla periódicamente.
- Opciones avanzadas -
- Dirección IP: 10.2.X.X (with a red warning icon)
- Puerto de dispositivo: 80
- Proveedor: [Empty]
- Modelo: [Empty]
- Buttons: Aceptar, Cancelar

Figura 26. Vinculación de dispositivos con servidor de streaming.

- **Vulnerabilidad en el sistema de visualización**

El sistema de visualización presenta una debilidad adicional, ya que permite visualizar la dirección IP de cualquier cámara que esté agregada. Si las credenciales de usuario han sido comprometidas, sería muy sencillo acceder a un dispositivo a través de un navegador web. Esta vulnerabilidad se muestra en la figura 27.

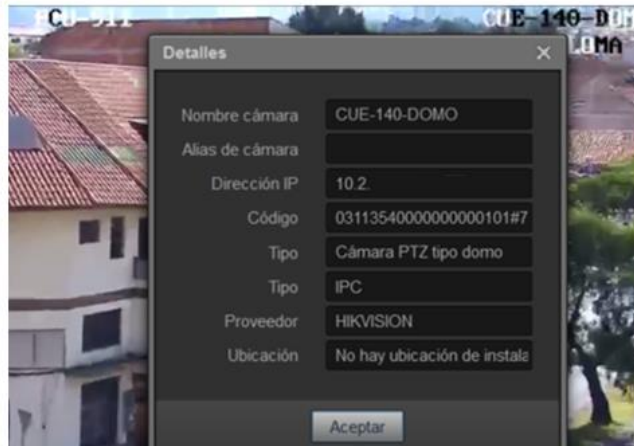


Figura 27. Detalles de una cámara IP agregada al IVS.

- **Acceso remoto a las cámaras**

También es posible acceder a las cámaras de manera remota a través de navegadores web o reproductores multimedia, como VLC Player. Este software permite conectarse a una cámara utilizando el protocolo RTSP y la dirección IP del dispositivo, facilitando la transmisión de video en tiempo real.

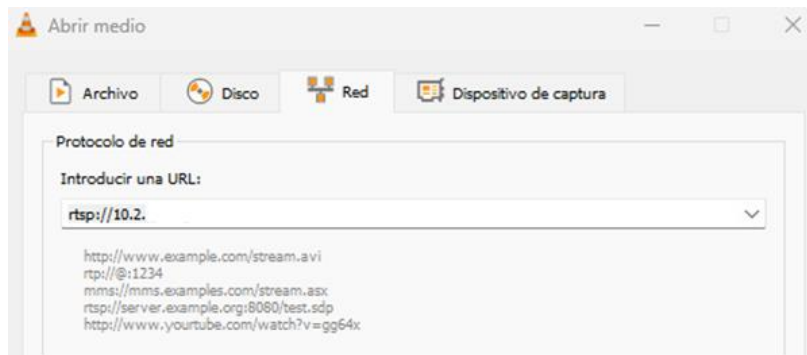


Figura 28. Acceso a una cámara IP a través de un reproductor de video.

### 3.1 Alternativas de mitigación

En este punto, se presentarán las alternativas de mitigación para las vulnerabilidades identificadas durante las pruebas de penetración, manuales y automatizadas, realizadas sobre el sistema de videovigilancia.

#### 3.1.1 Recomendaciones generales



Las siguientes recomendaciones se aplican a todo el sistema de videovigilancia y a los componentes que lo conforman:

**a. Cambio y fortalecimiento de credenciales**

Se recomienda modificar las credenciales predeterminadas por contraseñas seguras y únicas para cada dispositivo, utilizando combinaciones de caracteres fuertes. Esto incluye el uso de letras mayúsculas, minúsculas, números y caracteres especiales para aumentar la seguridad.

• **Implementación de autenticación robusta para RTSP**

Para mejorar la seguridad de las transmisiones mediante RTSP, se debe configurar el protocolo para requerir una autenticación fuerte antes de permitir el acceso al stream de video, esto se logra implementando métodos de autenticación más seguros que no sean fácilmente vulnerables, reforzando así la protección del sistema contra accesos no autorizados y previniendo potenciales ataques de interceptación o manipulación del contenido transmitido. Se recomienda evitar el uso de algoritmos vulnerables como MD5, y optar por opciones más seguras como SHA-256 o AES, que garantizan una encriptación más sólida de las credenciales y los datos transmitidos.

• **Uso de cifrado en la transmisión de RTSP**

Implementar cifrado en las transmisiones RTSP utilizando protocolos seguros como TLS o HTTPS, asegurando que los datos transmitidos estén protegidos contra la interceptación.

• **Actualización de firmware y configuración segura**

Mantener las cámaras IP actualizadas con el firmware más reciente proporcionado por el fabricante, siguiendo las mejores prácticas de seguridad, lo que incluye cerrar vulnerabilidades conocidas y aplicar configuraciones seguras recomendadas.

• **Monitoreo y auditoría**

Implementar sistemas de monitoreo y auditoría que registren accesos y actividades relacionadas con el protocolo RTSP. Establecer alertas para detectar

accesos no autorizados y realizar revisiones periódicas para asegurar el cumplimiento de las políticas de seguridad.

### 3.1.2 Recomendaciones específicas

Las siguientes recomendaciones se aplicarán sobre dispositivos específicos dentro del sistema de videovigilancia.

### 3.1.3 Configuración del mecanismo de autenticación en cámaras Hikvision

Una de las principales vulnerabilidades del protocolo RTSP es su mecanismo de autenticación. En las pruebas realizadas, se observó que las configuraciones simples y predeterminadas de las cámaras IP pueden ser explotadas para obtener credenciales de acceso. Para mitigar esta vulnerabilidad, se debe cambiar el algoritmo de cifrado utilizado para proteger las credenciales, garantizando una mayor seguridad en la transmisión de datos.

Se ha observado que, dentro de las configuraciones de los dispositivos, es posible modificar el tipo de algoritmo de encriptación utilizado para la autenticación, lo que permite optar por algoritmos más seguros que los predeterminados.



Figura 29. Algoritmos de autenticación RTSP.

Como se observa en la figura 29, dentro de la configuración de parámetros de la cámara IP, existen varios algoritmos de cifrado disponibles para la autenticación RTSP, entre ellos MD5, SHA-256 y una combinación de MD5/SHA-256, también se puede observar que para la autenticación web se utilizan algoritmos similares.

Se recomienda el uso de SHA-256, conocido por su robustez criptográfica, lo cual garantiza que los datos transmitidos a través del protocolo RTSP mantengan su integridad durante todo el proceso, reduciendo así el riesgo de accesos no autorizados y protegiendo la confidencialidad del sistema de videovigilancia.

### 3.1.4 Configuración del protocolo SRTP en cámaras Hikvision

Como se mencionó en el punto 2.1.10, el protocolo SRTP permite cifrar las transmisiones multimedia en tiempo real. Las cámaras IP utilizadas por el SIS ECU 911 permiten la configuración de este protocolo, lo que proporciona una capa adicional de protección durante una transmisión en tiempo real.

A continuación, se explicará cómo realizar la configuración del protocolo SRTP.



Figura 30. Configuración de protocolo SRTP.

Como se puede observar en la figura 30, existe un certificado creado por defecto, que forma parte de la configuración inicial de la cámara, no obstante, se planea generar un nuevo certificado, es recomendable utilizar un certificado emitido por una Autoridad de Certificación reconocida, pero para la presente explicación se utilizará el certificado autogenerated.

Para la creación de nuevos certificados, es necesario completar varios parámetros, entre ellos: la dirección IP del dispositivo, la validez del certificado, el nombre del certificado, el país, entre otros.

Crear certificado autofirmado

ID de certificado \* PRUEBA ✓

Longitud de clave pública 2048

País/Región \* CN ✓

IP/Nombre Dominio \* 10.2.1 ✓

Validez \* 365 Día(s) ✓

Contraseña

Estado o provincia

Localidad o municipio

Organización

Unidad organizativa

Email

OK Cancelar

Figura 31. Configuración del certificado digital para SRTP.

En la figura 31, se observa el procedimiento para la configuración del algoritmo, posteriormente, es necesario vincular el certificado con un algoritmo de encriptación para habilitar el uso de SRTP en la cámara IP, tal como se muestra a continuación.



Figura 32. Configuración de protocolo y certificado SRTP.

En la figura 32 se muestra que se ha configurado correctamente un algoritmo de cifrado, en este caso AES, este algoritmo ofrece un equilibrio entre rendimiento y seguridad, lo que lo convierte en una excelente opción para corregir debilidades en la seguridad de los sistemas de videovigilancia.

El certificado de servidor creado se utilizará para establecer conexiones más seguras, garantizando la integridad y confidencialidad de la información transmitida a través del protocolo RTSP.

Para verificar que la configuración ha sido exitosa, se puede utilizar un reproductor compatible con SRTP. Es necesario ingresar la URL de la cámara IP mediante una conexión RTSP, incluyendo el nombre de usuario, contraseña, puerto de acceso y el canal de streaming dentro de la URL.

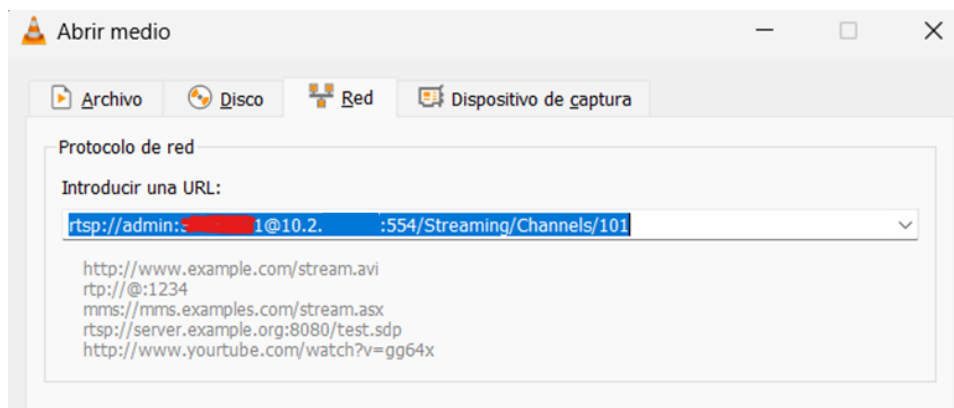


Figura 33. Establecimiento de conexión desde VLC hacia la cámara.

Después de ingresar todos los parámetros indicados, la configuración se considera exitosa cuando el video puede ser reproducido correctamente.

## CONCLUSIONES

El objetivo principal de este trabajo fue recopilar los avances recientes en cuanto a la seguridad del protocolo RTSP. No obstante, se observó que la cantidad de documentación disponible que demuestre mejoras significativas en los últimos años es limitada. A lo largo de este trabajo, se han presentado varias vulnerabilidades asociadas al protocolo, las cuales tienden a ser recurrentes. Esto sugiere una falta de evolución considerable en términos de seguridad.

El grado de seguridad en la implementación del protocolo RTSP depende en gran medida de las configuraciones realizadas en los dispositivos de la infraestructura de video. En el caso del sistema de videovigilancia del SIS ECU 911 Zonal 6, la implementación actual utiliza una versión obsoleta (RTSP 1.0) que no permite configuraciones de seguridad adecuadas. Debido a esto, se puede afirmar que el sistema de videovigilancia no es seguro, ya que, al usar dispositivos que no soportan configuraciones de seguridad avanzadas, se ven obligados a mantener dicha versión obsoleta.

A pesar de los avances tecnológicos en otros ámbitos, la evolución de la seguridad en el protocolo RTSP ha sido limitada. Vulnerabilidades recurrentes, como la falta de cifrado y la presencia de mecanismos de autenticación débiles, persisten y han sido documentadas. De todos los problemas identificados, el más preocupante es la debilidad en los mecanismos de autenticación, cuya configuración depende de las capacidades intrínsecas de las cámaras utilizadas en la infraestructura.

Una de las recomendaciones clave para la institución es mantener las versiones de firmware de los dispositivos siempre actualizadas. Sin embargo, esta solución tiene un límite, dado que la vida útil de los dispositivos y el soporte para los mismos eventualmente llegarán a su fin. En ese momento, el reemplazo de los equipos por dispositivos más modernos será la única opción viable, lo cual mejorará la seguridad general de la infraestructura.

Adicionalmente, se evidenció que varios dispositivos de la infraestructura del SIS ECU 911 Zonal 6, incluidas las cámaras, tienen puertos abiertos, lo que podría representar una vulnerabilidad. Es fundamental realizar una revisión exhaustiva de toda la infraestructura para identificar otros posibles puntos vulnerables.

En cuanto a la documentación utilizada en este trabajo, el RFC 2326 sigue siendo la fuente principal sobre el protocolo RTSP, ya que define su funcionamiento, propiedades y usos. No obstante, para una comprensión más profunda de las problemáticas de seguridad, el documento "Understanding RTSP: The Real-Time Streaming Protocol Explained" ha sido particularmente útil, junto con otras fuentes consultadas.

En relación con los objetivos planteados, se documentaron satisfactoriamente las vulnerabilidades encontradas en el sistema de videovigilancia del SIS ECU 911 y se propusieron posibles remediaciones. Estos hallazgos están recopilados en el anexo titulado "Reporte de Pruebas de Penetración: Vulnerabilidades del protocolo RTSP sobre cámaras IP en el Sistema de Videovigilancia del SIS ECU 911 Zonal 6", y las alternativas de mitigación fueron detalladas en la sección "Alternativas de Mitigación". En opinión del autor, la medida de seguridad más adecuada para la infraestructura actual es la implementación del protocolo SRTP, ya que ofrecería una mayor seguridad al añadir cifrado y mecanismos de autenticación robustos.

## RECOMENDACIONES

Se recomienda que el SIS ECU 911 Zonal 6 realice una actualización progresiva de las cámaras IP utilizadas en su sistema de videovigilancia, dado que los dispositivos más recientes cuentan con mejores características de seguridad, como el uso de algoritmos de encriptación más modernos y seguros. De las pruebas de seguridad realizadas, se ha concluido que las cámaras de la marca Hikvision presentan las mejores prestaciones.

Se sugiere al SIS ECU 911 Zonal 6 evaluar y aplicar las alternativas de mitigación presentadas en este documento, con el fin de resolver las vulnerabilidades identificadas en el sistema de videovigilancia. Una vez implementadas las medidas, se recomienda realizar una revisión del protocolo RTSP al menos dos veces al año, como parte de una evaluación de seguridad integral de toda la infraestructura. Durante el análisis, se detectaron posibles vulnerabilidades en otros componentes, como puertos abiertos innecesarios y configuraciones de red deficientes, que también deben ser abordadas.

Dentro de las alternativas de mitigación, se recomienda priorizar la implementación del protocolo SRTP en todos los dispositivos compatibles, ya que esto solucionaría el problema de la falta de cifrado que afecta al protocolo RTSP.

Basado en la experiencia obtenida en este trabajo, se aconseja realizar un análisis exhaustivo de todos los dispositivos del sistema de videovigilancia, o, en su defecto, utilizar una muestra más amplia que la utilizada en las pruebas. Para optimizar el proceso, es recomendable emplear herramientas de automatización que permitan evaluar una mayor cantidad de dispositivos en menos tiempo.

Se recomienda restringir el acceso total que posee el personal de tecnología del SIS ECU 911 Zonal 6 al contenido audiovisual transmitido por el sistema de videovigilancia. Esta práctica es inadecuada, ya que solo el personal autorizado debería tener acceso a dicha información, y únicamente para cumplir las funciones específicas de su rol.

Es fundamental capacitar al personal técnico, operativo y administrativo del SIS ECU 911 Zonal 6 en aspectos de seguridad de la información, con el objetivo de concientizar al personal y reducir la superficie de ataque del sistema. Asimismo, estas capacitaciones deberían ser gestionadas por un responsable de la seguridad de la información, quien también se encargaría de realizar las revisiones periódicas sugeridas.

Se recomienda revisar la metodología de integración de las cámaras IP con los sistemas de visualización, ya que actualmente se prioriza la funcionalidad y rapidez en el despliegue de los dispositivos, dejando de lado aspectos críticos de seguridad en la configuración.

Por último, durante las pruebas de seguridad realizadas en el sistema de videovigilancia, se observó una deficiencia en el manejo de herramientas de análisis de vulnerabilidades. Se sugiere que el tutor ofrezca un acompañamiento más cercano durante la ejecución de la parte práctica del trabajo de titulación. Además, sería conveniente aumentar el enfoque práctico en el currículo de las materias del programa de maestría.



## REFERENCIAS

- Apostolopoulos, J. G., Tan, W.-T., & Wee, S. J. (2002). *Video Streaming: Concepts, Algorithms, and Systems\**.
- Chu, D., Jiang, C. H., Hao, Z. B., & Jiang, W. (2013). The design and implementation of video surveillance system based on H.264, SIP, RTP/RTCP and RTSP. *Proceedings - 6th International Symposium on Computational Intelligence and Design, ISCID 2013*, 2, 39–43. <https://doi.org/10.1109/ISCID.2013.124>
- Cmpe. (2009). *RTSP Protocol Focus on SECURITY 2009 Samuel MONY-Philippe SAWADOGO*.
- Dessai, S., & Chaudhari, S. (2015). Design of Secure Transmission of Multimedia Data Using SRTP on Linux Platform. *International Journal of Reconfigurable and Embedded Systems (IJRES)*, 4(2), 71–81.
- Iyyanar, P., Chitra, M., & Sabarinath, P. (2012). Effective and Secure Scheme for Video Streaming Using SRTP. *International Journal of Machine Learning and Computing*, 855–859. <https://doi.org/10.7763/ijmlc.2012.v2.252>
- Kumar R, A. B., Reddy, L. C., & Hiremath, P. S. (2008). RTSP Audio and Video Streaming for QoS in Wireless Mobile Devices. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 8, Issue 1).
- Lian, S., Telecom, F., Kanellopoulos, D., & Ruffo, G. (2009). Recent Advances in Multimedia Information System Security. In *Informatica* (Vol. 33).
- Mateos Costilla, D., & Montoro, S. R. (n.d.). *Curs 2007/2008 enginy@eps Streaming de Audio/Video. Protocolo RTSP*.
- Schulzrinne, H. (2003). *Network Working Group RTP: A Transport Protocol for Real-Time Applications Status of this Memo*.
- Schulzrinne, H., Rao, A., Lanphier, R., Netscape, C. U. /, & Realnetworks, /. (1998). *Internet Engineering Task Force MMUSIC WG INTERNET-DRAFT Real Time Streaming Protocol (RTSP) Status of this Memo Copyright Notice*.

- Tejaswi, B., Mannan, M., & Youssef, A. (2023). All Your IoT Devices Are Belong to Us: Security Weaknesses in IoT Management Platforms. *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 245–250. <https://doi.org/10.1145/3577923.3583636>
- Turton William. (2021, March 9). *Hackers breach thousands of security cameras, exposing Tesla, jails, hospitals - Los Angeles Times*.
- Understanding RTSP: The Real-Time Streaming Protocol Explained | CQR*. (n.d.). Retrieved July 29, 2024, from <https://cqr.company/wiki/protocols/understanding-rtsp-the-real-time-streaming-protocol-explained/> Yan Liu, Guo-Hui Zhong, Yu Liu, Hua-Qiang He, & Fu-Rong Wang. (2008). *Wavelet Analysis and Pattern Recognition, 2008, ICWAPR '08, International Conference on*. IEEE Xplore.
- Zingade, S., Joshi, R., Shendkar, R., Arora, P., & Scholar, U. G. (2016). DREAM-A Data Streaming Application Using RTP/RTSP in a Local Area Network. *International Journal of Engineering Science and Computing*. <https://doi.org/10.4010/2016.693>

# ANEXOS

**Anexo 1:** Reporte de Pruebas de Penetración: Vulnerabilidades del protocolo RTSP sobre cámaras IP en el Sistema de Videovigilancia del SIS ECU 911 Zonal 6.

## Resumen ejecutivo

El presente informe expone los resultados del análisis de seguridad y las pruebas de penetración realizadas en cámaras IP que utilizan el protocolo RTSP para la transmisión de video en tiempo real en el sistema de videovigilancia del SIS ECU 911 Zonal 6. El objetivo principal fue identificar vulnerabilidades que pudieran comprometer la operación, confidencialidad e integridad del sistema de videovigilancia.

Las pruebas revelaron vulnerabilidades significativas, relacionadas principalmente con una autenticación débil y la exposición no autorizada de los streams de video, estos problemas se identificaron en cámaras Hikvision y Dahua, que constituyen un gran porcentaje de las cámaras analizadas y representan riesgos graves para la seguridad y privacidad de las transmisiones.

Las recomendaciones para mitigar estas vulnerabilidades incluyen la implementación de una autenticación robusta, el uso de cifrado en las transmisiones, y la actualización del firmware de los dispositivos involucrados.

## Alcance y duración

El análisis de seguridad se enfocó en el sistema de videovigilancia del SIS ECU 911, compuesto por 388 cámaras IP.

Las pruebas de penetración se realizaron durante 30 días, entre agosto y septiembre de 2024, utilizando una muestra representativa de cámaras distribuidas aleatoriamente para evaluar tanto dispositivos de reciente implementación como aquellos con mayor tiempo en uso.

## Resumen de vulnerabilidades encontradas

Durante la revisión de seguridad, se identificó un conjunto de vulnerabilidades, de las cuales se seleccionaron para el presente informe aquellas que pudieron ser demostradas o que podrían representar un impacto considerable para la organización. Al final, se seleccionaron 5 vulnerabilidades críticas y 3 de alto riesgo.

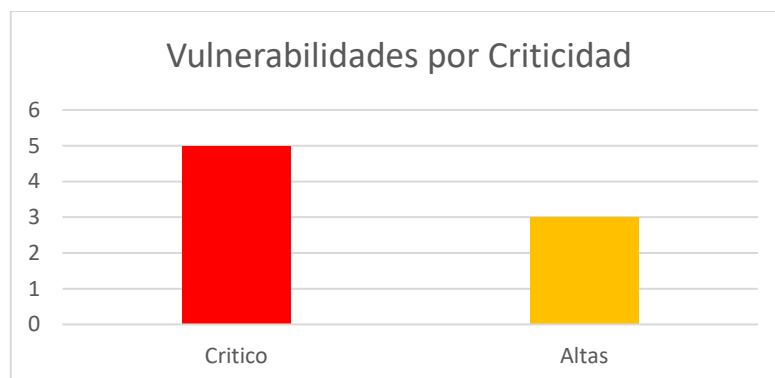


Figura 1. Vulnerabilidades encontradas sobre RTSP.

Las vulnerabilidades se dividieron según el tipo de prueba realizada, en primer lugar, se resumen las vulnerabilidades encontradas mediante pruebas manuales.

Vulnerabilidad	Criticidad
Exposición innecesaria de superficie de ataque por configuración de red errónea	Crítico
Configuraciones por defecto	Crítico

Tabla 1. Vulnerabilidades de RTSP obtenidas de pruebas manuales.

Asimismo, se realizaron pruebas utilizando herramientas de análisis automatizado, lo que dio como resultado la identificación de las siguientes vulnerabilidades:

Vulnerabilidad	Criticidad
Detección de protocolo SSL 2 y 3	Crítico
Desbordamientos de buffer (UPnP)	Crítico
Vulnerabilidad Heartbleed	Alto
Algoritmos de hashing débiles	Alto
Múltiples vulnerabilidades Treck TCP/IP	Crítico
Nombre predeterminado público de SNMP	Alto

Tabla 2. Vulnerabilidades de RTSP obtenidas de pruebas automatizadas.

## Metodología aplicada para realización de pruebas de penetración

Para evaluar la seguridad del sistema de videovigilancia, se realizaron pruebas técnicas tanto manuales como automatizadas, que incluyeron los siguientes procedimientos:

- **Escaneo de Red:** Se utilizó Nmap para identificar las cámaras IP activas en la red y determinar los puertos abiertos, con especial atención al puerto RTSP (554).
- **Pruebas de Acceso No Autenticado:** Se enviaron solicitudes RTSP a los puntos finales identificados para verificar si era posible acceder a los streams de video sin credenciales.
- **Evaluación de Mecanismos de Autenticación:** Se probaron combinaciones de credenciales predeterminadas y débiles para evaluar la efectividad de los mecanismos de autenticación en las cámaras.
- **Pruebas de Fuerza Bruta:** Utilizando scripts en lenguaje Python, se realizaron ataques de fuerza bruta sobre las credenciales de acceso a las cámaras.
- **Análisis de Tráfico:** Se monitoreó el tráfico de red para identificar transmisiones no cifradas y posibles vulnerabilidades en la comunicación.

## Detalles de vulnerabilidades

**Vulnerabilidad 1. Exposición innecesaria de superficie de ataque por configuración de red errónea**

**Criticidad:** **Crítico**

**Afectación:** Toda la muestra de cámaras IP verificadas

**Descripción:**

Las cámaras IP pueden ser accedidas desde un navegador web o un reproductor multimedia, como VLC. Debido a la simplicidad en el acceso a estos dispositivos, existe la posibilidad de que personal no autorizado, que opere dentro de la misma infraestructura del SIS ECU 911, pueda acceder a las cámaras sin consentimiento, comprometiendo la seguridad del sistema.

## Prueba (manual):

Al encontrarme en un segmento de red y una ubicación diferente de donde se encuentran los evaluadores de videovigilancia, puedo tener acceso hacia una cámara mediante un navegador web.

Paso 1: Probar conectividad hacia la cámara mediante la herramienta ping.

Paso 2: Abrir un navegador web e ingresar mediante la dirección IP de una cámara, desde una ubicación y un segmento de red diferente.

Paso 3: Verificar que el navegador devuelva un error de acceso (acceso no autorizado), en caso de que se permita el acceso:

Paso 3.1: Ingresar con las credenciales hacia la configuración y visualización de esta.

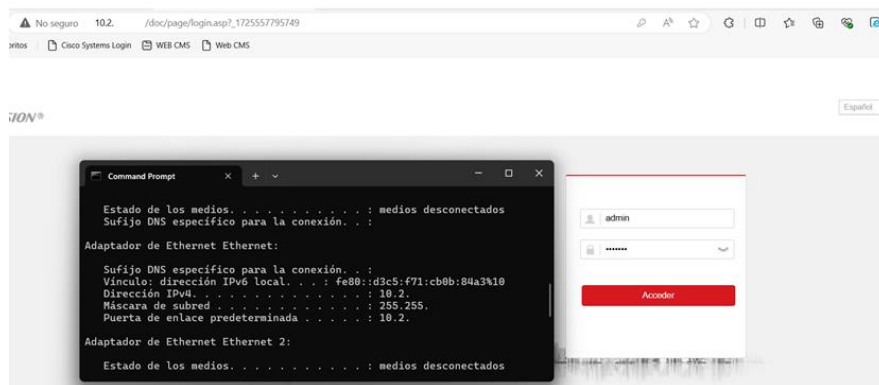


Figura 2. Verificación de conectividad entre PC de pruebas y la IP de la cámara.

## Remediación:

- Segmentar cada una de las redes, como una medida efectiva para prevenir un intrusión y filtrado de datos.
- Modificar la modalidad de autenticación de RTSP.
- Evitar el uso de credenciales predeterminadas y conocidas, tal es el caso de “admin”.

## Vulnerabilidad 2. Configuraciones por defecto

**Criticidad:** **Crítico**

**Afectación:** Toda la muestra de cámaras IP verificadas

**Descripción:**

Las cámaras IP están configuradas con ajustes predeterminados inseguros, priorizando únicamente los parámetros necesarios para su integración con los sistemas de videovigilancia, sin embargo, no se han implementado adecuadamente controles de seguridad adicionales, como la encriptación de datos o mecanismos de autenticación robustos.

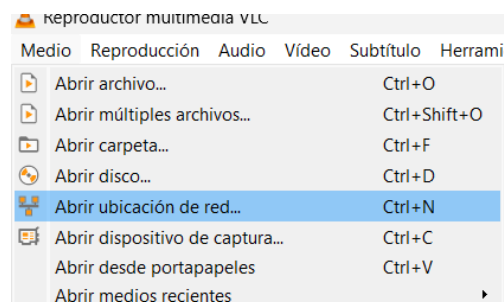
Esta falta de configuraciones de seguridad expone a las cámaras IP a riesgos como accesos no autorizados y posibles compromisos en la integridad y confidencialidad de los datos transmitidos.

### **Prueba (manual):**

Debido al gran número de dispositivos, no existe un control adecuado de configuración que garantice la seguridad de las cámaras que utilizan el protocolo RTSP. Los escenarios en los que se ha evidenciado esta vulnerabilidad incluyen accesos mediante reproductores multimedia.

Paso 1: Abrir el reproductor multimedia VLC.

Paso 2: Solicitar abrir una nueva unidad de red.



*Figura 3. Apertura de un nuevo stream.*

Paso 3: Colocar una URL a través de RTSP con las credenciales y dirección IP de la cámara, para obtener el acceso a visualización.

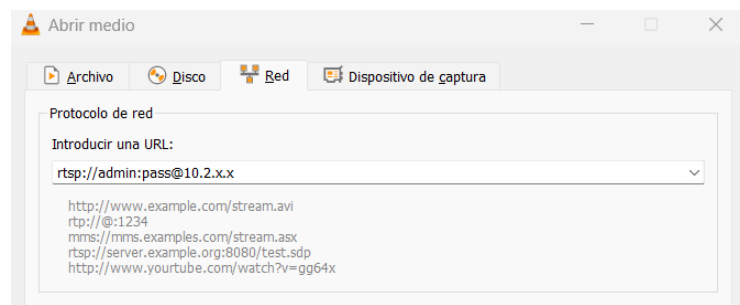


Figura 4. URL para inicio de sesión de un host a través de RTSP.

Paso 4: Realizar una prueba usando el puerto por defecto usado por RTSP.

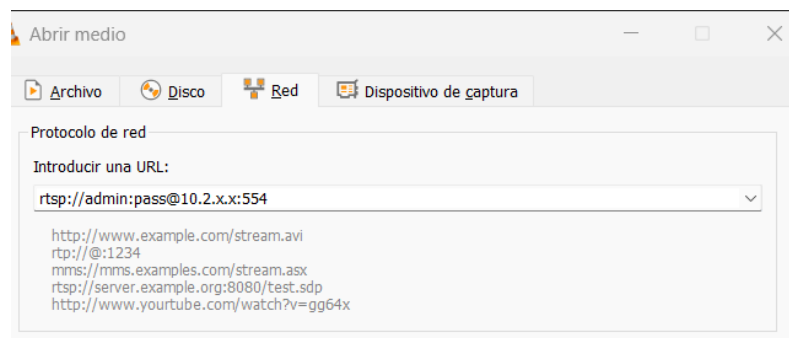


Figura 5. URL de inicio de sesión usando el número de protocolo.

### Remediación:

- Cambiar las credenciales predeterminadas por una combinación segura de usuario y contraseña.
- Configurar la autenticación para el acceso RTSP en la cámara, de modo que se requieran credenciales antes de permitir el acceso al stream.
- Asegurarse de que las cámaras estén actualizadas con el último firmware proporcionado por el fabricante.
- Modificar la configuración por defecto de los puertos de RTSP.

### Vulnerabilidad 3. Detección de protocolo SSL versión 2 y 3

**Criticidad:** **Crítico**

**Afectación:** 10.2.X.X – 10.2.X,X

**Prueba de carácter automatizada**

**Descripción:**



Se refiere a versiones de SSL que han sido afectadas por errores criptográficos, tales como; esquemas de reanudación de sesiones inseguras.

Un atacante puede aprovechar estas fallas para realizar ataques de intermediario (man in the middle) o para descifrar las comunicaciones entre el servicio afectado y los clientes.

**Remediación:**

- Deshabilitar las versiones de SSL 2.0 y 3.0.
- Usar TLS 1.2 o versiones superiores.
- Realiza pruebas con navegadores y clientes comunes para confirmar que no hay problemas de compatibilidad al deshabilitar SSLv2 y SSLv3.
- Realizar revisiones periódicas para asegurarse de que las configuraciones SSL/TLS estén actualizadas y seguras.

**Vulnerabilidad 4. Desbordamientos de buffer debido a versión anteriores de librería para dispositivos UPnP14**

**Criticidad:** **Crítico**

**Afectación:** 10.2.X.X – 10.2.X.X - 10.2.X.X

**Descripción:**

Existe una condición de desbordamiento de búfer basada en pila en la función `unique_service_name()` dentro del archivo `ssdp/ssdp_server.c`<sup>15</sup> cuando se manejan solicitudes del Protocolo simple de descubrimiento de servicios (SSDP). Un atacante remoto no autenticado puede aprovechar esto, a través de una solicitud SSDP especialmente diseñada, para ejecutar código arbitrario.

---

<sup>14</sup> UPnP: Universal Plug and Play, un conjunto de protocolos que permite a los dispositivos encontrarse entre si en una misma red local.

<sup>15</sup> `ssdp/ssdp_server.c`: Parte de una librería que permite implementar el protocolo UPnP, siendo importante para la interacción de dispositivos en red.



Figura 6. Configuración de librerías UPnP.

### Remediación:

- Actualizar las librerías libupnp.
- Aplicar los parches de seguridad.
- Implementar Sistemas de Detección y Prevención de Intrusiones para prevenir intentos de explotación basados en desbordamientos.

### Vulnerabilidad 5. Certificados SSL usando de Algoritmos de hashing débiles

**Criticidad:** **Alta**

**Afectación:** 10.2.X.X – 10.2.X.X - 10.2.X.X

### Prueba de carácter automatizada

### Descripción:

Utilización de algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Estos algoritmos de firma son vulnerables a ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado.



Figura 7. Algoritmos de hashing usados en las cámaras IP.

### Remediación:

- Mejorar hacia algoritmos de hash más eficientes.
- Reemplazar los certificados SSL existentes.
- Monitorear la vigencia de los certificados.

### Vulnerabilidad 6. Vulnerabilidad conocida como Heartbleed<sup>16</sup>, que afecta al protocolo de seguridad TLS (Transport Layer Security)

**Criticidad:** **Alta**

**Afectación:** 10.2.X.X – 10.2.X.X

### Prueba de carácter automatizada

### Descripción:

Esta falla podría permitir que un atacante remoto lea el contenido de hasta 64 KB de memoria del servidor, exponiendo potencialmente contraseñas, claves privadas y otros datos confidenciales.

---

<sup>16</sup> Heartbleed: Vulnerabilidad de seguridad crítica, sobre los protocolos (SSL/TLS) responsables de proteger las comunicaciones a través de internet

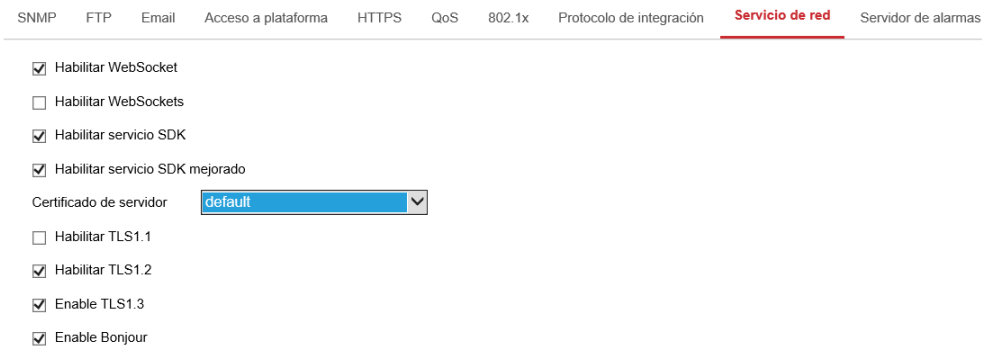


Figura 8. Versiones de protocolo TLS existentes.

## Remediación:

- Actualizar las versiones de Open SSL.
- Generar nuevos certificados SSL/TLS.
- Implementar una herramienta de detección de intrusos para monitorear cualquier acceso no autorizado.
- Establecer planes de mantenimiento y actualización de las bibliotecas de seguridad.
- Habilitar versiones más actualizadas de TLS.

## Vulnerabilidad 7. Múltiples vulnerabilidades de Treck TCP/IP

**Criticidad:** **Crítica**

**Afectación:** 10.2.X.X

### Prueba de carácter automatizada

### Descripción:

Se detecta el uso de una pila Treck TCP/IP<sup>17</sup> por parte del host afectado, siendo potencialmente vulnerable a Ripple 20.

Ripple es un conjunto de 19 vulnerabilidades encontradas sobre la pila Treck TCP/IP, las vulnerabilidades presentan un riesgo crítico debido a que una pila Treck está integrada por números dispositivos.

---

<sup>17</sup> Treck TCP/IP: Es una implementación de protocolos TCP /IP que fue desarrollada por la empresa Treck Inc. Especializada en software de redes embebidas.

## Remediación:

- Actualizar el firmware o software que utiliza Treck TCP/IP.
- Aplicar los parches de seguridad publicados por Treck para vulnerabilidades Ripple 20.
- Implementar una segmentación de red adecuada, aislando los dispositivos de la pila Treck TCP/IP.

## Vulnerabilidad 8. Nombre por defecto público de SNMP

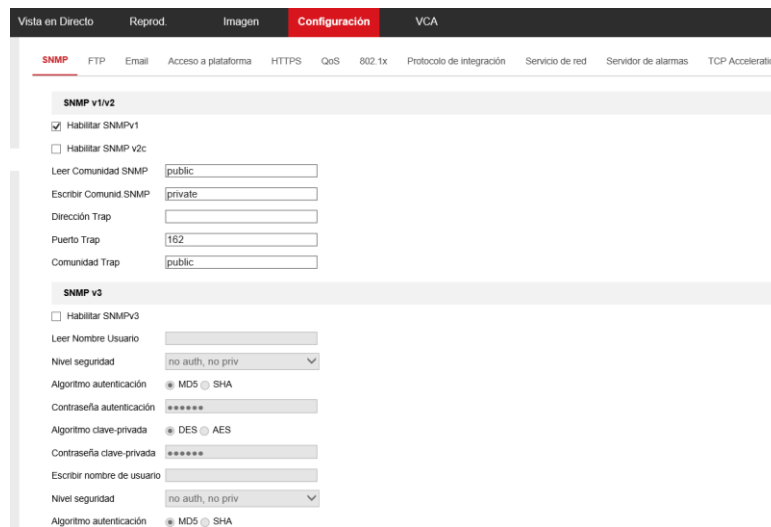
**Criticidad:** **Alta**

**Afectación:** 10.2.X.X – 10.2.X.X – 10.2.X.X

### Prueba de carácter automatizada

### Descripción:

Es posible obtener el nombre predeterminado de un servidor SNMP remoto, causando que un atacante pueda utilizar esta información para obtener más información sobre el host o para cambiar las configuraciones de este.



The image shows a configuration page for SNMP. At the top, there are tabs: 'Vista en Directo', 'Reprod.', 'Imagen', 'Configuración' (highlighted in red), and 'VCA'. Below the tabs is a navigation menu with items: 'SNMP', 'FTP', 'Email', 'Acceso a plataforma', 'HTTPS', 'QoS', '802.1x', 'Protocolo de Integración', 'Servicio de red', 'Servidor de alarmas', and 'TCP Acceleration'. The main content area is divided into two sections: 'SNMP v1/v2' and 'SNMP v3'. In the 'SNMP v1/v2' section, 'Habilitar SNMPv1' is checked, and 'Habilitar SNMP v2c' is unchecked. Below these are input fields for 'Leer Comunidad SNMP' (public), 'Escribir Comunidad SNMP' (private), 'Dirección Trap', 'Puerto Trap' (162), and 'Comunidad Trap' (public). The 'SNMP v3' section has 'Habilitar SNMPv3' unchecked. It includes fields for 'Leer Nombre Usuario', 'Nivel seguridad' (no auth, no priv), 'Algoritmo autenticación' (MD5), 'Contraseña autenticación' (\*\*\*\*\*), 'Algoritmo clave-privada' (DES), 'Contraseña clave-privada' (\*\*\*\*\*), 'Escribir nombre de usuario', 'Nivel seguridad' (no auth, no priv), and 'Algoritmo autenticación' (MD5).

Figura 9. Configuración por defecto de SNMP.

## Remediación:

- Desactivar el servicio de SNMP en todos los hosts.
- Cambiar los nombres predeterminados de la comunidad.
- Limita el acceso a SNMP solo a direcciones IP específicas de administradores o servidores de monitoreo confiables.

**Anexo 2:** Descripción de las pruebas de penetración manuales realizadas sobre las vulnerabilidades encontradas.

### **1. Accesos no Autorizados**

**Criticidad:** Crítico

**Afectación:** Toda la muestra de cámaras IP verificadas

**Descripción:**

Las cámaras IP pueden ser accedidas desde un navegador web o un reproductor la posibilidad de que personal no autorizado, que opere dentro de la misma infraestructura del SIS ECU 911, pueda acceder a las cámaras sin consentimiento, comprometiendo la seguridad del sistema.

**Remediación:**

- Segmentar cada una de las redes, como una medida efectiva para prevenir un intrusión y filtrado de datos.
- Modificar la modalidad de autenticación de RTSP.
- Evitar el uso de credenciales predeterminadas y conocidas, tal es el caso de “admin”.

### **2. Configuraciones por defecto**

**Criticidad:** Crítico

**Afectación:** Toda la muestra de cámaras IP verificadas

**Descripción:**

Las cámaras IP están configuradas con opciones predeterminadas, priorizando únicamente los ajustes necesarios para su integración con los sistemas de videovigilancia. Sin embargo, no se han implementado de manera adecuada controles de seguridad adicionales, como la encriptación de datos o mecanismos de autenticación. Esta falta de configuraciones de seguridad expone a las cámaras a riesgos significativos, como accesos no autorizados y posibles compromisos en la integridad y confidencialidad de los datos transmitidos

**Remediación:**

- Cambiar las credenciales predeterminadas a una combinación segura de usuario y contraseña.

- Configura la autenticación para el acceso RTSP en la cámara para requerir credenciales antes de permitir el acceso al stream.
- Asegurarse de que las cámaras están actualizadas con el último firmware proporcionado por el fabricante.
- Modificar la configuración por defecto de los puertos de RTSP.

### **3. Prueba de configuraciones por defecto**

**Criticidad:** Crítico

**Afectación:** Acceso a las cámaras IP, interceptar el flujo de video

**Descripción:**

Evaluar la seguridad de las cámaras Hikvision y Dahua en términos de posibles vulnerabilidades asociadas con el protocolo RTSP (Real-Time Streaming Protocol). En particular, se buscó identificar posibles vectores de ataque relacionados con la inyección de comandos a través de RTSP.

Durante la ejecución del script de pruebas, no se encontraron credenciales por defecto en las cámaras IP seleccionadas como parte de la muestra. Esto sugiere que las configuraciones iniciales de autenticación han sido modificadas adecuadamente, reduciendo la probabilidad de explotación de vulnerabilidades relacionadas con credenciales predeterminadas.

### Anexo 3: Script usado para verificar si las cámaras poseen credenciales por defecto.

```
import requests
from requests.auth import HTTPBasicAuth
import os

# Función que realiza la prueba sobre una cámara IP
def test_camera(camera_ip, username, password):
    # Define la URL para el endpoint de login de la cámara
    login_url = f'http://{camera_ip}/ISAPI/Security/userCheck'

    # Realiza la solicitud HTTP con las credenciales por defecto
    try:
        response = requests.get(login_url,
            auth=HTTPBasicAuth(username, password), timeout=5)
        if response.status_code == 200:
            print(f"Success: Default credentials are valid for
{camera_ip}")
            return True
        else:
            print(f"Failed: Default credentials are not valid for
{camera_ip}")
            return False
    except requests.RequestException as e:
        print(f"Error: Could not connect to {camera_ip}. Reason: {e}")
        return False

# Función para leer las direcciones IP desde un archivo
def read_camera_ips(file_path):
    try:
        with open(file_path, 'r') as file:
            # Leer cada línea del archivo, eliminando saltos de línea
            camera_ips = [line.strip() for line in file if
line.strip()]
            return camera_ips
    except FileNotFoundError:
        print("Error: The file was not found.")
        return []

# Definir las credenciales por defecto desde variables de entorno (más
seguro)
username = os.getenv('CAMERA_USER', '*****')
password = os.getenv('CAMERA_PASSWORD', '*****')

# Ruta al archivo de texto que contiene las IPs de las cámaras
file_path = 'cameras.txt'

# Leer las IPs desde el archivo
camera_ips = read_camera_ips(file_path)

# Ejecutar la prueba sobre cada cámara
for camera_ip in camera_ips:
    test_camera(camera_ip, username, password)
```



**Anexo 4:** Autorización por parte de la Coordinación Zonal 6 ECU 911, para la realización del presente trabajo de investigación.

**Anexo 5:** Reporte completo de las vulnerabilidades obtenidas de los escaneos automatizados en Nessus.

Nota: Debido a la extensión de los anexos 4 y 5, éstos se presentarán como documentos independientes.