UNIVERSIDAD JOSÉ ANTONIO PÁEZ

IMPLEMENTACIÓN DE UNA CAPA DE SEGURIDAD EN LA PLATAFORMA CISCO ISE EN LA EMPRESA AVÍCOLA LA GUÁSIMA, C.A.

Autor:

Yulihannys Pineda.

Urb. Yuma II, calle N.º 3. Municipio San Diego

Teléfono: (0241) 8714240 (master) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE UNA CAPA DE SEGURIDAD EN LA PLATAFORMA CISCO ISE EN LA EMPRESA AVÍCOLA LA GUÁSIMA, C.A.

Proyecto del Informe de Pasantías para optar al título de
INGENIERO EN TELECOMUNICACIONES

Autor:
Yulihannys Pineda.
Tutor:
Ing. José Villarroel.

San Diego, junio de 2023

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA [X]

TRABAJO DE GRADO [ ]

El jurado designado por la Facultad de Ingeniería para la evaluación del **Informe Final de Pasantía o Trabajo de Grado** titulado: Implementación de una capa de Seguridad en la Plataforma Cisco ISE en la Empresa, Avícola La Guasima

Realizado por el (la) Br. Yulihamys del Carmen Pinto Guedez

C.I. Nº 29727305 cursante de la carrera de Telecomunicaciones

hace constar después de analizar su contenido y oída la exposición oral, considera que el Informe Final o Trabajo de Grado ha obtenido la calificación de:

APROBADO [X] NO APROBADO [ ]

El Jurado

Tutor Académico (Coordinador)
Nombre: Jose Villalroel
C.I.: 24193852

Jurado
Nombre: Alex Barrios
C.I.: 8.667.378

Jurado
Nombre: Carlos Tarazo
C.I.: 24547369

Fecha: 03/07/2023

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE TELECOMUNICACIONES

CONSTANCIA DE APROBACIÓN PARA LA PRESENTACIÓN PÚBLICA DEL TRABAJO DE GRADO

Quien suscribe, José Villarroel, portador de la cédula de identidad N° 24.193.852, en mi carácter de tutor del trabajo de grado presentado por el ciudadano Yulihannys Pineda, portador de la cédula de identidad N° 29.727.305, titulado **IMPLEMENTACIÓN DE UNA CAPA DE SEGURIDAD EN LA PLATAFORMA CISCO ISE EN LA EMPRESA AVÍCOLA LA GUÁSIMA, C.A.**, presentado como requisito parcial para optar al título de Ingeniero en Telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los 05 días del mes de junio del año dos mil veintitrés.

José Villarroel
C.I: 24.193.852

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA

FI T 001 2022-3CR IP

Valencia, 14 de abril de 2023

Ciudadana:
PINEDA GUEDEZ, YULIHANNYS DEL CARMEN
29.727.305
Presente -

Cumplo con informarle que la comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **Nº 05-2023** de fecha **10/02/2023** aprobó el proyecto de grado tipo Informe de Pasantía titulado:

Implementación de una capa de seguridad en la plataforma CISCO ISE en la empresa Avícola la Guásima C.A.

Presentado por usted como requisito para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación del Tutor Académico que lo asesorará en el desarrollo de este proyecto a: Ing. José Rafael Villarroel García, titular de la cédula de identidad V- 24.193.852

Atentamente

Facultad de Ingeniería UJAP DECANATO

Dra. Laura Aurora Sáenz Palencia
Decana de la Facultad de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado de la Facultad de Ingeniería

DEDICATORIA

El presente trabajo, va dedicado a mis padres, Oscar y Dannalis, personas luchadoras que siempre están velando por mí y por mi educación, así como a mis dos hermanos, Roger y Oscari, quienes con su amor incondicional nunca dejan de apoyarme en mis estudios y proyectos de vida. A mis abuelos, Mami Lucy, Papi Sabi y Juliana, quienes siempre estarán orgullosos de mis logros y de mi persona. Mi familia, están ahí para extenderme una mano y ayudarme a crecer como persona. A mi madrina Nancy, una persona esencial para mi vida y mi crecimiento. A Sora y Lyroi, por iluminar mis días. Por último, a Luisito que me apoyó mucho durante el transcurso de la carrera.

Este trabajo igualmente, está dedicado a todos los profesionales y personas que ayudaron que este proyecto se haga realidad, ayudándome a formarme como profesional a través de enseñanzas, consejos y oportunidades.

AGRADECIMIENTOS

Quisiera agradecerle a mis padres y hermanos, debido a que gracias a sus consejos, apoyo incondicional y las oportunidades que me brindaron, me proporcionaron muchas maneras de salir adelante, en mis buenos y malos momentos. Quiero agradecer a los profesores de la universidad, que me permitieron formarme como futuro profesional de la universidad y me brindaron el conocimiento de mi carrera.

Así mismo, quiero agradecer a mis amigos y compañeros que tuve a lo largo de toda mi carrera universitaria ya que brindaron su apoyo, conocimiento y buenos momentos que recordaré siempre.

Muchas gracias a todos. Gracias Totales.

ÍNDICE GENERAL

CONTENIDO **pp.**

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

FIGURAS **DESCRIPCIÓN** **pp.**

ÍNDICE DE TABLAS

DESCRIPCIÓN

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE LA PLATAFORMA CISCO ISE PARA ADMINISTRAR POLÍTICAS DE SEGURIDAD DE LA RED EN LA EMPRESA AVÍCOLA LA GUÁSIMA, C.A.

Autor: Yulihannys Pineda
Tutor: Ing. José Villarroel
Fecha: junio 2023

RESUMEN INFORMATIVO

La presente investigación está titulada como **IMPLEMENTACIÓN DE LA PLATAFORMA CISCO ISE PARA ADMINISTRAR POLÍTICAS DE SEGURIDAD DE LA RED EN LA EMPRESA AVÍCOLA LA GUASIMA C.A**, la cual es una empresa ubicada en Tocuyito, Estado Carabobo, donde la misma explota la rama avícola y agrícola, así como, ofrece servicios de compra, venta y distribución de alimentos en Venezuela. Se realiza el presente estudio para la migración de tecnología del sistema de autenticación de usuarios a través de la implementación de un sistema de acceso para las políticas de seguridad, con la finalidad de proporcionar un control de acceso a los recursos corporativos, para la validación de usuarios y dispositivos finales, monitoreo y una gestión centralizada de la red. La metodología de la investigación posee un enfoque cualitativo, la investigación se plantea con la modalidad "proyecto especial", con diseño de campo y documental, y, por último, nivel descriptivo. Las técnicas de recolección de datos a utilizar son observación directa, entrevista y, por último, revisión documental. Así mismo, los instrumentos para la recolección de datos, se encuentra la guía de observación, guía de entrevista, registro fotográfico, tabla de actividades y diario de campo. Perteneciendo a la línea de investigación ciencias cognitivas y aplicadas de la Universidad José Antonio Páez. A través de esta investigación, se realizaron cinco (5) fases metodológicas donde se diagnosticó la situación actual de la empresa, se analizó la topología cableada e inalámbrica de la red empresarial y se analizó los requisitos mínimos para CISCO ISE, por lo que fue satisfactoria la implementación de la plataforma ya que demostró ser funcional y compatible a través de la evaluación de pruebas pilotos realizadas en la última fase metodológica.

Descriptores: Sistema de acceso, Políticas de seguridad, Seguridad de la Información

INTRODUCCIÓN

El constante desarrollo tecnológico que existe en la actualidad, provoca que exista un gran crecimiento en las redes a nivel mundial. De este modo, provocando que las organizaciones y compañías se preocupen en la mejora de la seguridad de su información, incorporando sistemas posean este cometido, como son las políticas de acceso, normas, protocolos, de esta manera, creando una barrera ante posibles vulnerabilidades. La aplicación de este tipo de control de acceso a la red empresarial, permite mayor visibilidad a los usuarios, así como el monitoreo de quiénes, cuándo y cómo se están conectando a la red, así actuar rápidamente ante cualquier tipo de amenaza.

Por lo que, la empresa Avícola La Guásima, C.A, se encuentra en un sector industrial que consta de una operación diaria a través de su red empresarial, siendo una de las principales razones de por qué implementar una plataforma centralizada para gestión de políticas de seguridad, es una migración de tecnología ideal para resultados óptimos y seguros. De este modo, CISCO ISE (Identity Services Engine), se conoce por ser una plataforma que administra la red, permitiendo la creación y aplicación de políticas de seguridad y acceso. Siendo un enfoque dinámico y automatizado para la toma de decisiones en toda la infraestructura de la red empresarial.

En el presente trabajo, se desarrollarán cinco (5) fases metodológicas para el objetivo principal propuesto, cuales se describirán en el desarrollo de la investigación.

Se destaca de esta manera, la descripción de cada capítulo. **El Capítulo I**, denominado La empresa, describe la empresa donde se realiza la pasantía, su enfoque, conjunto a su ubicación, misión y visión, así como la estructura interna considerando todas las gerencias que posee. En el **Capítulo II,** se denomina El Problema, se explica la problemática a estudiar que presenta la red empresarial, así mismo como el impacto que genera en la empresa, como la necesidad que existe de solucionarlo. Se redactan los objetivos generales y específicos, la justificación, alcance y límites que tendrá.

En el **Capítulo III,** se denomina Marco Teórico, se exponen los antecedentes que sirvieron de guía a lo largo del presente estudio, las bases legales que apoyan la investigación, así como teoría que sustenta las bases de la investigación, así como la definición de los términos que ayudan al entendimiento de siglas o términos utilizados en el trabajo.

Con lo que respecta del **Capítulo IV**, denominado Marco Metodológico, se enfoca a la explicación del tipo, diseño y nivel de investigación. Por consecuente, la población y muestra

a estudiar, técnicas e instrumentos de recolección de datos utilizados, así técnicas para el análisis de los datos, y por último las fases metodológicas.

Por último, el **Capítulo V**, denominado Resultados, se mostrarán las fases metodológicas y cada una de las actividades que se llevaron a cabo, así mismo como las conclusiones y recomendaciones del presente trabajo.

CAPÍTULO I

LA EMPRESA

1.1 Descripción de la empresa

La empresa Setrys se describe como una empresa de soluciones tecnológicas dirigida a las telecomunicaciones, en redes y la ciberseguridad. Realizan consultaría especializada a clientes y empresas, así como la compra, venta y distribución de equipos para satisfacer la demanda de los usuarios que consumen sus servicios.

1.1.1 Ubicación de la empresa

Setrys C.A posee diferentes sucursales, a nivel nacional se encuentran dos sucursales ubicadas en Caracas y Valencia, a nivel internacional en Colombia, Chile y República Dominicana. La pasantía en cuestión, se desarrolla en Valencia, en la urbanización, La Trigaleña, en el Centro Comercial Trigaleña Plaza.

1.1.2 Razón Social

La razón social de la empresa se resume en "Setrys C.A".

1.1.3 Reseña histórica

Setrys C.A fue creada en el año 2009, sin embargo, cesó operaciones hasta el año 2017, donde ha servido a diferentes clientes como Farmatodo, Coca-Cola, Cisco, etc.

1.1.4 Estructura Organizativa

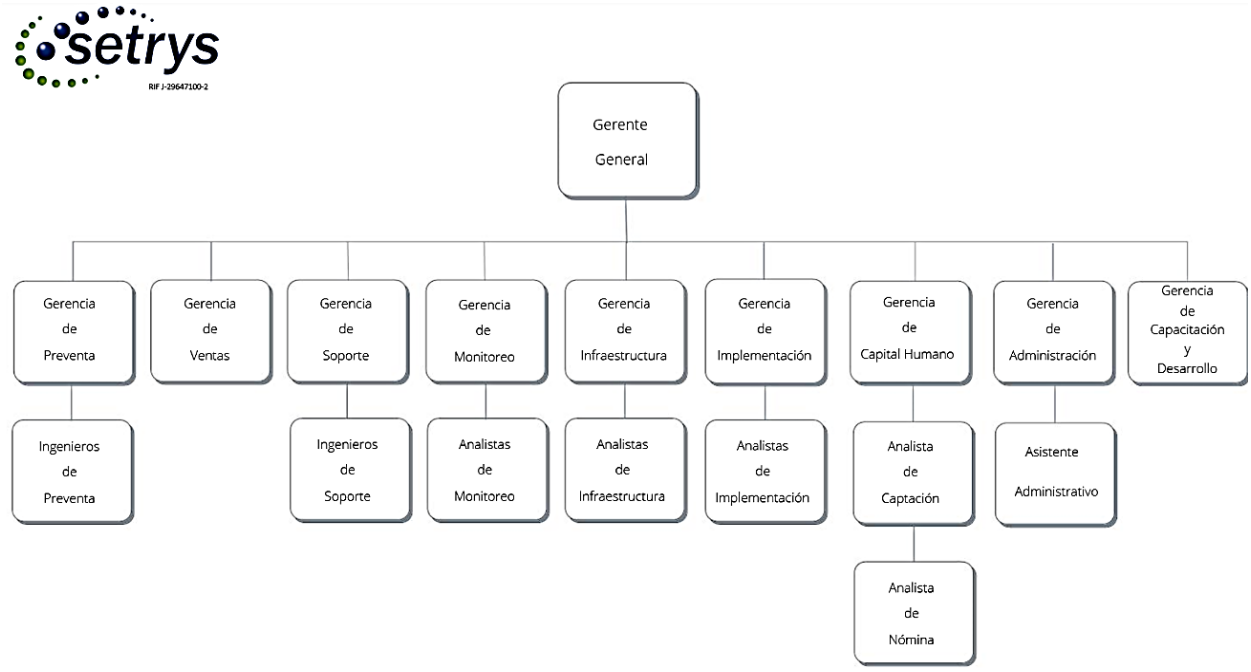


Figura 1. Organigrama de la organización de gerencias en la empresa
Fuente: Setrys, C.A. (2022)

El organigrama de la empresa presenta nueve gerencias en total, resumiéndose en Gerencia de Preventa, Gerencia de Ventas, Gerencia de soporte, Gerencia de Monitoreo, Gerencia de Infraestructura, Gerencia de Infraestructura, Gerencia de Implementación, Gerencia de Capital Humano, Gerencia de Administración y por último Gerencia de Capacitación y Desarrollo.

1.2 Misión, Visión, Objetivos y Valores de la empresa

1.2.1 Misión

"Entender el ecosistema tecnológico de nuestros clientes empresariales para entregar soluciones de vanguardia a su medida. Garantizando un acompañamiento cercano de nuestro equipo de profesionales especializados con pasión de servicio, contando con infraestructura y tecnología de punta en constante evolución." (Setrys C.A)

1.2.2 Visión

"Ser reconocida como una de las empresas líder a nivel nacional e internacional en el ramo de las tecnologías de la información, especializándonos en los servicios de redes y sistemas, dando cumplimiento a nuestro principio corporativo que busca el permanente crecimiento de nuestra empresa, impulsando la innovación y el desarrollo de nuevas oportunidades de negocios." (Setrys C.A)

1.2.3 Objetivos

Los objetivos de la empresa Setrys C.A es ser la empresa líder en los servicios de telecomunicaciones, soluciones tecnológicas y redes. Así como ser un servicio de calidad para empresas en diferentes localidades.

1.2.4 Valores

"Los principios y valores de conducta empresarial con los que Setrys C.A está comprometido al más alto nivel, son los siguientes:

- Innovación: Invertimos en investigación, capacitación y desarrollo, ofreciendo nuevos productos y servicios, que se adecuan a dar solución a cada empresa, persona y momento. Asimismo, nuestro personal está altamente calificado y certificado por nuestros aliados comerciales, ofreciendo sus habilidades prácticas en el monitoreo, diagnóstico y solución de cualquier evento.
- Integridad: Nos caracterizamos por nuestra honradez y por hacer lo correcto frente a las diversas situaciones, a nuestros clientes le transmitimos siempre las ventajas sin ocultar los riesgos en la toma de decisión, y se garantiza un comportamiento integro y ético en todas nuestras actuaciones por parte de todo el personal de Setrys.

- Responsabilidad: Nos involucramos al máximo en cada proyecto y trabajamos con el compromiso de crear una relación a largo plazo basada en la eficacia y eficiencia de nuestro Equipo de Trabajo.
- Excelencia: Nos basamos en un control operativo que nos permite visualizar los procesos de atención al cliente, mejora continua, máxima eficiencia en la gestión de procesos y finalmente trabajar orientados en alcanzar los mejores resultados.
- Confianza: Nos caracterizamos por trabajar bajo principios éticos, consistencia y lealtad en nuestro actuar, manteniendo una comunicación constante con nuestros clientes para obtener resultados positivos." (Setrys C.A)

1.3 Descripción del Departamento donde se desarrolla la pasantía.

La pasantía se realiza en la Gerencia de Implementación, describiéndose como:

"Unidad encargada de la ejecución de los procesos de implementación desde lo técnico hasta administrativo en los diversos proyectos de Setrys, cumpliendo con los requerimientos funcionales y de rendimiento, asegurando los estándares de calidad requeridos y a su vez garantizando eficientemente los diversos recursos con base en las metas de Setrys C.A" (Setrys C.A)

1.3.1 Proceso de Producción

La producción de Setrys C.A está basado en la realización de proyectos por cliente, por lo que el proyecto es transferido a diferentes gerencias, siguiendo diferentes fases como, de gerencia de ventas, gerencia de implementación y gerencia de soporte.

CAPÍTULO II

EL PROBLEMA

2.1 Planteamiento del problema

En los inicios de los años 60, las redes tomaron un papel muy importante en el desarrollo tecnológico a nivel mundial, provocando su crecimiento de forma exponencial, la seguridad en la red y las políticas de seguridad no se consideraban un factor importante debido al desconocimiento que existía para atacar una red. Hasta el año 1988, se tomó con importancia la seguridad en la red debido al auge del internet, ya que no era dirigido únicamente a organizaciones sino para el público de manera general. En el mismo año, existió un incidente llamado *worm* (gusano) provocando que distintas empresas fueran afectadas a nivel económico y a nivel de red, sin embargo, fue un motivo de por qué es necesario crear mecanismos de protección de los datos, abriendo puerta una gran área que es indispensable para una red actual. Hoy en día, existe un gran desarrollo de nuevas tecnologías donde se encuentra una extensa diversificación de equipos que tienen la posibilidad de acceder a la red, provocando que las organizaciones necesiten controlar y monitorear los dispositivos conectados. Sin embargo, es una tarea difícil gestionar cuántos usuarios ingresan a la red, dónde ingresan y qué tipos de permisos de accesos poseen. En una red genérica, normalmente no cuenta con métodos de autenticación en puntos de red, una autorización para acceder a un servidor y un tipo de registro a donde se está accediendo.

Por lo tanto, las vulnerabilidades de las redes van incrementando cada día, requiriendo más exigencia a la hora de establecer parámetros para las políticas de seguridad, ya que se afrontan a peligros como malwares, provocando daños perjudiciales para una red, dando mal uso de la información disponible e incluso llegando a corromper o eliminar la misma, de igual manera pueden provocar ataques dirigidos a la red que no puedan ser afrontados a tiempo.

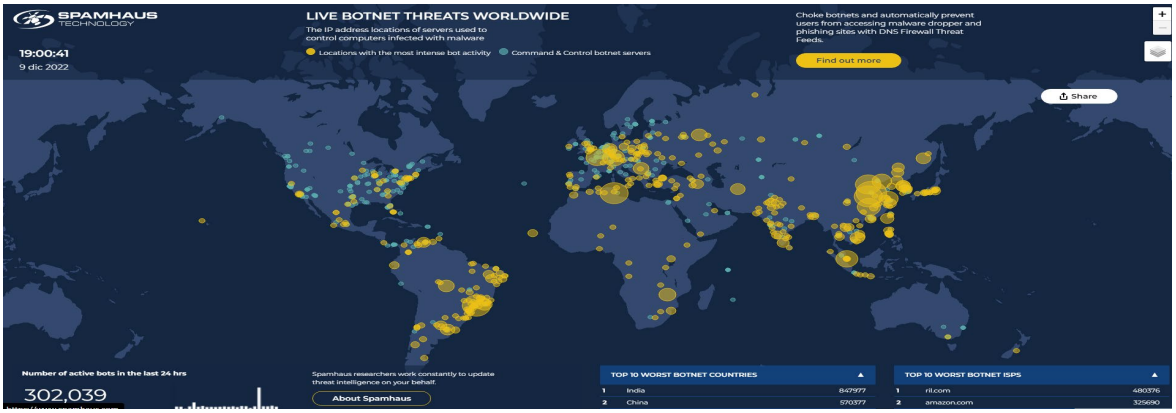


Figura 2: Ataques a nivel mundial de IP infectadas de malwares en tiempo real
Fuente: Spamhaus. (2023)

Se destaca de esta manera, que los ataques globales se han vuelto el centro de atención en los últimos años debido al constante crecimiento de los dispositivos, así como las conexiones, siendo un factor importante para estadísticas y estimados para la consideración del manejo de la seguridad de usuarios y dispositivos conectados en cada red. Según CISCO SYSTEMS (Cisco Visual Networking Index: Forecast and Trends, 2017–2022), proyecta el crecimiento de los dispositivos entre 2017 al 2022, entre ellos contando M2M (machine to machine), teléfonos inteligentes y entre otros.

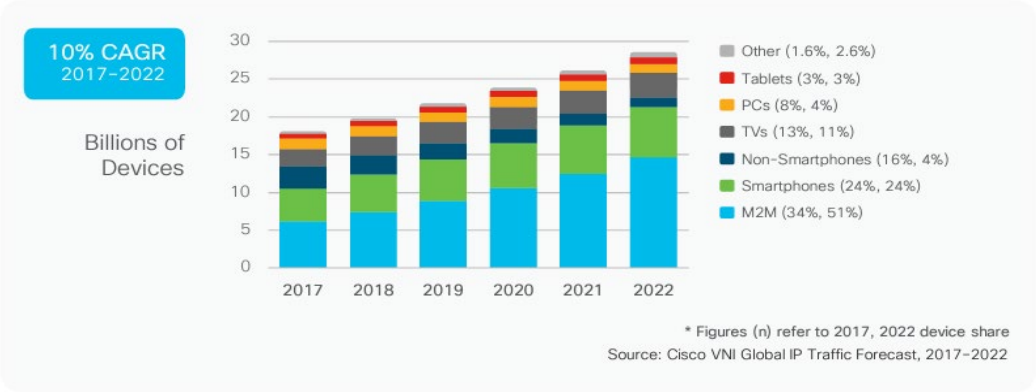


Figura 3. Crecimiento global de dispositivos y conexiones
Fuente: CISCO VNI Global IP Traffic Forecast 2017-2022

En el caso de Latino América, CISCO SYSTEMS (Cisco Visual Networking Index (VNI): Forecast Highlights, 2017–2022), ilustra el crecimiento exponencial del continente a través de estadísticas como el aumento de la población de usuarios de internet, dispositivos, conexiones per cápita y velocidades de internet que ayudan a proveedores y empresas alrededor del mundo a prepararse y tomar medidas para el crecimiento de enlaces y estructuras.

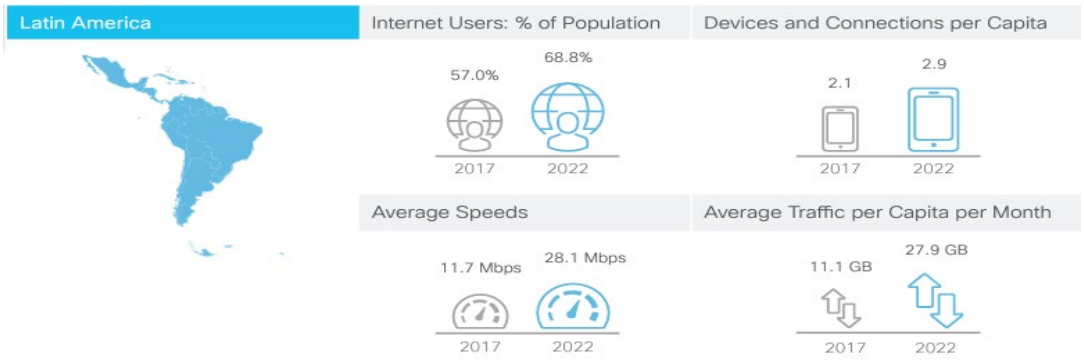


Figura 4. Estadísticas de crecimiento de dispositivos en Latino América 2017-2022.
Fuente: VNI Forecast Highlights Tool - Cisco System

Por otra parte, Latino América es uno de los continentes que recibe amenazas de forma constante, en el caso de las empresas, resulta ser un problema preocupante debido a que la red empresarial es un puente para el flujo de la información necesaria para el funcionamiento diario de las operaciones que se realizan todos los días, ya que ésta permite el acceso a usuarios

internos y externos a los recursos y datos, así como los permisos que se les otorga a los destinarios correspondientes, precisamente siendo una vulnerabilidad que puede ser atacada por algún tipo de agente externo a la empresa.

Por lo mismo, la compañía ESET especializada en ciberseguridad presenta a través de un reporte anual (Security Report, Latinoamérica 2022), una encuesta a empresas situadas en el continente sobre incidentes con respecto a la seguridad de sus redes, apreciado en la **figura** 5. Los incidentes más señalados se dividen en infección de malware, ataques de ingeniería social y accesos no autorizados, además, la mitad de las empresas encuestadas afirma no tener incidentes de seguridad significando que pudieron haber o no incidentes que no fueron reconocidos en las organizaciones, dado que es inevitable que un porcentaje de los mismos no puedan ser detectados, sin embargo, las capacidades de detección van incrementando hoy en día por los avances tecnológicos a través de la ciberseguridad.

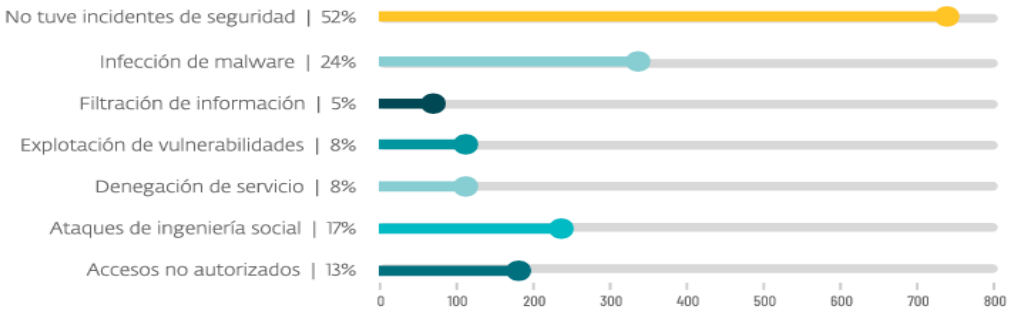


Figura 5. Incidentes de seguridad reportados por empresas en América Latina en 2021.
Fuente: ESET Security Report 2022 Latino América

En los datos ofrecidos por ESET, la empresa destaca a Venezuela en el año 2018 por ser uno de los países con un mayor índice a infecciones de "malware", conocidos como códigos maliciosos comunes, sin embargo, una de las mayores preocupaciones son los "ransomware" siendo un tipo de malware perjudicial a los datos empresariales de estas organizaciones. En este caso, Venezuela no cuenta con una estrategia de seguridad nacional que permita confiabilidad a las redes empresariales. Se tiene como evidencia la creación de un sistema llamado Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), con el objetivo de proporcionar mayor calidad de ciberseguridad, enfocándose en el desarrollo y promoción de los Sistemas Nacionales de Seguridad de Información, Certificación Electrónica y entre otros, siendo necesario resaltar que tiene un enfoque para las plataformas nacionales que posee el país. Debido a la necesidad por la ciberseguridad y la administración de las redes, se ha convertido en un negocio rentable para el sector privado que ofrecen servicios relacionado a la seguridad de la información, para así apoyar a las empresas a tener protocolos necesarios para la operación diaria de las mismas.

Jaén (2015), en su investigación metodológica “Diseño e Implementación del control de Acceso a la Red”, explica cómo llevar a cabo una estrategia de seguridad de la información para el beneficio de la red empresarial:

> “Una estrategia de seguridad de la información es disponer de elementos de red que permitan habilitar un control de acceso perimetral, como son los firewalls y hoy es crítico implementar una solución de control de acceso a recursos de red basados en contexto, es decir que permita a los administradores de red, establecer políticas para el acceso, que identifiquen al usuario, dispositivos mediante los cuales se accede a la red, lugar y hora de ingreso a la red institucional y que los recursos habilitados sean los adecuados.” (p.4)

La empresa “Avícola La Guásima C.A”, situada en la ciudad Tocuyito, estado Carabobo, se dedica a la explotación de rama avícola y agrícola, especialmente en la compra, venta, cría de aves, ganado y varias especies de animales, de este modo llevando a cabo la producción y distribución de alimentos en Venezuela. Actualmente, no posee ningún sistema centralizado de seguridad que controle el acceso, autenticación o monitoreo de los usuarios y dispositivos en su red empresarial, únicamente recurren al uso de un sistema de Pre Shared Key (PSK) que logra autenticar al usuario que desee acceder, siendo hoy en día, en comparación con otros métodos, un sistema simple para las vulnerabilidades que pueden afectar a las operaciones de la empresa día a día. Uno de los problemas radica en la divulgación de la clave de un Service Set Identifier (SSID) en la empresa, provocando que el manejo de los usuarios finales y los dispositivos se realice de una forma desorganizada y a la misma vez, descontrolada; al manejar redes empresariales, cambiar la clave no es una solución factible debido que no resuelve el problema desde la raíz, necesitando de esta forma una herramienta que pueda manejar, así como facilitar el control y autorización que se le proporciona a cada dispositivo que se conecta a la red empresarial.

En la actualidad, para poder acceder a la red empresarial y los recursos que ésta ofrece, en las diferentes áreas de la empresa, se puede realizar de forma cableada o inalámbrica. En el caso de la red cableada, no se puede distinguir un control o autorización al usuario y dispositivo que se está conectando, siendo un riesgo debido al tipo de usuario que pueda tener acceso físico a los puntos de red o switches. Por su parte, en la forma inalámbrica igualmente no posee un estricto control quién se conecta a ella, siendo la sede principal y sitios foráneos de la empresa, tal cual como son las granjas y diferentes sucursales de producción, generando la necesidad de establecer diferentes roles y tipos de privilegios a cada usuario que se conecte en la red, dividiéndose en: nodos de administración, de monitoreo y de personas.

Hoy en día, la operación de la empresa "Avícola La Guásima, C.A", cuenta con el recurso de Umbrella, un producto de ciberseguridad proporcionado por Cisco Systems, éste mismo permite visualizar servicios de nube, básicamente permitiendo que bloquee destinos que puedan ser maliciosos y amenazantes antes de establecer una conexión, negando de esta manera las solicitudes a destinos maliciosos que puedan aportar *phishing* e infecciones de malware. Este tipo de servicio está dirigido hacia los recursos en la red, utiliza las herramientas del Domain Name System (DNS) para el tráfico de la plataforma de nube y seguridad. Por lo que es importante resaltar que los puntos de acceso físicos y las conexiones inalámbricas permanecen vulnerables ante cierto ataque, debido a que Umbrella posee otro enfoque como es la seguridad a causa de las constantes amenazas que posee el internet a través del navegador.

Es importante destacar que la empresa posee una red fundamentada a partir de elementos de la empresa Cisco Systems, por lo que favorece la implementación de una plataforma que facilite el control de acceso y manejo de las políticas de seguridad de la red que sea del mismo fabricante, de esta manera creando una red homogénea para el mayor rendimiento de las funciones, así como reducir el tiempo de implementación de la plataforma.

2.2 Formulación del problema

¿Cómo mejorar la administración de políticas de seguridad en la red corporativa de la empresa Avícola La Guásima, C.A.?

2.3 Objetivos de la investigación

2.3.1 Objetivo general

Implementar una capa de seguridad en la plataforma CISCO ISE en la empresa Avícola La Guásima, C.A.

2.3.2 Objetivos específicos

- Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.
- Analizar la estructura actual de la topología de la interconexión de la red empresarial y las configuraciones disponibles a través del medio/plataforma para el proceso de seguridad de datos y usuarios.
- Analizar los requisitos mínimos que se necesitan para la implementación de CISCO ISE.
- Desplegar los componentes y estructuras lógicas y funcionales de la capa de seguridad en la red empresarial.

- Evaluar el desempeño de la nueva capa de seguridad de la plataforma CISCO ISE, así como la efectividad de las nuevas políticas de seguridad en la empresa Avícola La Guásima, C.A.

2.4 Justificación de la investigación

La tecnología del control de políticas de seguridad tiene el propósito de proporcionar control y visibilidad a la configuración de la red y la actividad de los usuarios, internos y externos, lográndose a través de un sistema eficiente, como lo es el servidor de CISCO ISE, para gestionar las políticas de seguridad. Algunos de los beneficios que puede proveer este sistema, es la visibilidad de todas las interacciones de la red, como la autenticación, autorización y accounting (AAA) integradas, perfiles, servicios para usuarios temporales y permanentes, por su parte también una total integración con el sistema para su gestión, con el objetivo de mostrar toda la información compilada de forma estadística de la red en una sola consola.

A diferencia de NAC, siendo un producto igualmente de CISCO, se limita únicamente al control de acceso que permite a los usuarios obtener acceso seguro a los recursos de la red, por su parte, ISE ofrece una mayor seguridad y protección para la red empresarial ya que proporciona varias funciones como herramientas de autenticación de usuarios, ancho de banda y controles de filtrado de tráfico en la interfaz de usuario y asegurar un entorno de red alámbrico o inalámbrico.

La empresa Avícola La Guásima, C.A. demuestra la necesidad para la implementación de este servidor para controlar y monitorear efectivamente la red empresarial, con la intención de garantizar la seguridad del usuario y la empresa ante amenazas y vulnerabilidades que puedan afectar sus operaciones diarias.

2.5 Alcance y Limitaciones

Se busca satisfacer completamente las medidas de seguridad necesarias para la red empresarial a través de la implementación de una instancia CISCO ISE a través de la creación de una máquina virtual (VM) ubicada en la red local de la empresa. Se aplicará el protocolo AAA (Authentication, Authorization, Accounting), de esta manera, los protocolos RADIUS y TACACS+, garantizando la seguridad de la red y de los dispositivos. Se busca estudiar y evaluar la topología cableada e inalámbrica de la red empresarial a través de protocolos de descubrimiento como los protocolos CDP, LLDP y EIGRP, así mismo CISCO ISE ser la plataforma que gestione y monitoree los accesos cableados e inalámbricos a la red de empresa “Avícola La Guásima C.A” con la creación de políticas de seguridad y roles administración.

Las limitaciones que se deben tomar en cuenta para la implementación del CISCO ISE, abarca un estudio considerando un pequeño estimado de usuarios finales que permitan realizar un plan piloto y poder garantizar los resultados finales. Su aplicación y análisis comprende la seguridad a nivel lógico, exceptuando la manipulación de la capa física o la topológica de los elementos que se encuentren en la red empresarial (control de acceso físico a las instalaciones, equipos, cableado, dispositivos). De esta misma manera, en los nodos no se integrará el pxGrid.

CAPÍTULO III

MARCO TEÓRICO

Según Santa Palella Stracuzzi y Feliberto Martins Pestana (2012), el marco teórico se define como: "La elección de teorías o soportes teóricos que permitan abordar el objeto de estudio. Explica que establece la teoría y por qué se considera pertinente y aplicable a lo que se investiga." (p.194). Por lo que, podemos afirmar que en el marco teórico se hace la investigación y recopilación de teorías en forma documental, expuesta por varios autores y profesionales del área. De esta forma, sustentando las bases teóricas para la solución de la problemática.

3.1 Antecedentes

En la investigación de Silvera (2022), titulada "**Implementación de un sistema de acceso a la red de datos para mejorar el control de acceso de los dispositivos microinformáticos en una empresa de fabricación y comercialización de alimentos de consumo masivo**", para optar al título de Ingeniero de Sistemas e Informática en la Universidad Tecnológica del Perú, se tuvo como objetivo principal, implementar un sistema de acceso a la red de datos para mejorar el control de acceso de los dispositivos microinformáticos en una empresa de fabricación y comercialización de alimentos de consumo masivo, utilizando un enfoque cualitativo, diseño pre experimental de preprueba-posprueba y diagnóstico, tipo de investigación aplicada. Como muestra, se escogieron 30 dispositivos microinformáticos fueron evaluados en la pre prueba y post prueba con el estímulo aplicado, haciendo uso de la guía de observación como instrumento para la recolección de datos.

En las conclusiones de la investigación, se confirmó que la implementación de un sistema de acceso a la red de datos permite mejorar el control de accesos de los dispositivos microinformáticos. Guarda una gran cercanía con el presente trabajo debido a que ambas investigaciones están dirigidas a una empresa de alimentos, así como tienen el objetivo común de la implementación de un sistema eficiente para el sistema de acceso a la red empresarial.

Así mismo, de Merino (2021**),** titulada "**Desarrollo de Plan de Actividades y políticas de acceso AAA para plataforma de red inalámbrica en entorno productivo para Farmatodo en Venezuela**", para optar al título de Ingeniero de Telecomunicaciones en la Universidad Católica Andrés Bello, el objetivo principal de implementar CISCO ISE para mejorar las políticas de seguridad en la empresa Farmatodo C.A. Con un diseño de proyecto factible, y tipo de investigación de campo. El antecedente citado, posee una población de la

empresa Farmatodo C.A, y así mismo, utilizando una muestra del Departamento de Telecomunicaciones.

Por lo que, las conclusiones de esta investigación mencionada dieron con la mejora de las políticas de seguridad de la empresa estudiada, logrando implementar la plataforma CISCO ISE en toda la red empresarial, en las diferentes sucursales en el país. El trabajo mencionado posee una relación estricta con la presente, debido a que ambos trabajos trabajan con la plataforma CISCO ISE, para la implementación de un sistema de monitoreo y manejo de políticas de seguridad para ambas empresas.

De igual forma, Noguera (2019), desarrolló un trabajo de investigación llamado "**Implementación de un sistema de detección de intrusos para Venezolana del Vidrio C.A**", para optar el título de Especialista en Telecomunicaciones Digitales, en la Universidad Central de Venezuela, teniendo como objetivo principal diseño e implantación de una solución que incremente la seguridad de los datos de la empresa Venezolana del Vidrio C.A., a fin de resguardar sus operaciones, transacciones, e información corporativa, utilizando un enfoque cuantitativo, con un tipo de investigación de proyecto factible. La población se tuvo a la empresa Venezolana del Vidrio C.A.

Al finalizar la investigación, se concluyó que la herramienta para detectar y alertar sobre el tráfico malicioso, se incrementó la integridad, disponibilidad y resguardo de la información empresarial. Resaltó la importancia de detectar ataques mientras suceden en tiempo real, para ser detenidos en cuestión de minutos, por lo que su NIDS requiere un monitoreo constante, debido a que lamentablemente no es una herramienta capaz de reaccionar ante una intrusión. Así mismo, recomienda el uso de detección de malware de cliente/servidor. La investigación de Noguera, se encuentra relacionada con los objetivos de la presente investigación, debido a la intención de implementar una plataforma que ayude a la seguridad de la red empresarial, llevando a cabo procedimientos imprescindibles para este tipo de sistemas como son el diagnóstico, definir el tipo de sistema a implementar y su configuración e integración en la red de la organización.

Así mismo, Peña (2016), realizó un trabajo de investigación por nombre "**Diseño e implementación de una red privada virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada**", para optar por el título Especialista en Comunicaciones y Redes de Comunicaciones de Datos, en la Universidad Central de Venezuela. Con el objetivo general de Diseñar e implementar una Red Privada Virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada. Una investigación de tipo cuantitativo, con un tipo de investigación de proyecto factible. Se utilizó la técnica de

observación documental y arqueo bibliográfico. Se llevó a cabo en una población como es la empresa privada.

A través de la investigación, se concluye que la arquitectura escogida permite una redundancia en la conexión vía SSL-VPN, cual garantiza de esta manera el manejo de la misma desde cualquier ubicación geográfica y así mismo garantiza el uso de credenciales de inicio de sesión a los usuarios VPN. Se destaca entonces, la similitud que posee esta investigación con la presente ya que busca crear políticas de acceso a los usuarios que se deseen conectar en la red.

Por último, Vargas (2016), presenta su trabajo llamado **"Modelo de Madurez de Seguridad de la Información para el Monitoreo y Análisis del tráfico de redes en la Administración Pública Nacional de Venezuela."** Optando por el Título de Magíster en Sistema de Información en la Universidad Católica Andrés Bello. Posee el objetivo general de Proponer un Modelo de Madurez de Seguridad de la Información para el Monitoreo y Análisis del Tráfico de redes en la Administración Pública Nacional de Venezuela. Con un tipo de investigación de proyecto factible, así como un diseño de tipo documental y de campo. Utiliza instrumentos como entrevista y cuestionarios. La investigación está compuesta por una población de entes e instituciones de Administración Pública Nacional. En el caso de la muestra, se procedió en personal seleccionado de diferentes instituciones del estado.

La investigación, por ende, concluye que es un sistema que busca de ser guía de un diagnóstico y evaluación de la seguridad informática, de esta manera minimizando el impacto a eventos relacionados con la misma. El software aplicado no tiene una parametrización necesaria para poder determinar valores adecuados para el tráfico de red, y uno de los puntos a resaltar, es la centralización del sistema de monitoreo de seguridad. El trabajo citado, guarda relación con el presente debido a la necesidad que posee cada red de seguridad para establecer sistemas para la seguridad de la información de algún ente o institución.

3.2 Teoría central de la Investigación

La teoría central de la presente investigación se basa en la Seguridad de la Información. Según Fortra, explica que la seguridad de la información "es la práctica que consiste en identificar y proteger la información confidencial, y garantizar que los datos estarán seguros durante todo su ciclo de vida" (Fotra, 2022, p.1)

3.3 Bases Teóricas

3.3.1 Redes

Según Etecé, las redes se definen "como interconexión de un número determinado de computadores (…) mediante dispositivos alámbricos o inalámbricos que, mediante impulsos eléctricos, ondas electromagnéticas u otros medios físicos, les permiten enviar y recibir información en paquetes de datos, compartir sus recursos". (Etecé, 2021, p.1)

3.3.1.1 Sistemas de acceso a la red

Los sistemas de acceso se definen como una tecnología que permite el monitoreo y visibilidad de la red, así como la administración de acceso para el control de forma efectiva de dispositivos que acceden dependiendo de las políticas de gestión propuestas para la gestión de dispositivos microinformáticos. Según Helfrich (2006), describe que establece reglas o políticas de acceso y cuenta con una consola centralizada que permite a los dispositivos el acceso total, acceso limitado o la imposibilidad de acceder a la red.

3.3.1.2 Tipos de peligro en la red y malwares

Se define al virus informático, como un programa desarrollado en un determinado lenguaje de programación, infectando uno o varios sistemas informáticos, utilizando varios mecanismos de propagación o autorreplicación, el cual trata de reproducirse de forma acelerada para extender su alcance. (Vieites, 2013, p.42)

Desde eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. De esta misma forma, Vieites (2013), define diferentes tipos de amenazas como virus de sector de arranque (BOOT), virus de archivos ejecutables, virus de macros, virus de lenguajes de Script, Malware, Gusanos, Troyanos, Spyware, Keyloggers, Adwares, Dialers. Backdoors, Otros, etc. (p.44)

3.3.1.3 Seguridad en la red

La seguridad en la red se define como un conjunto de estrategias, procesos y tecnologías para la protección de una empresa ante ataques y accesos no autorizados. En las investigaciones de Bejarano, (2017) explica que la seguridad en la red se define como "garantizar que se mantenga la información (de una empresa, entidad gubernamental, etc.) de manera íntegra, privada (confidencial), controlada, autentificada y disponible (solo para el personal autorizado), mediante políticas de seguridad informática (PSI)." (p.10)

- **Seguridad Física**

Según Huerta (2002) explica que la seguridad física es: "la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial." (p.22) Por lo que la seguridad física se refiere a

controles y mecanismos de seguridad dentro de la red empresarial, de esta manera, implementado para proteger el hardware y almacenamientos.

- **Seguridad Lógica**

El Instituto Superior de Estudios ISED (2018), en su artículo por nombre "¿Qué es la seguridad lógica?", define el término de la misma:

> ".. Un conjunto de procesos destinados a garantizar la seguridad en el uso de los sistemas y los programas destinados a gestionar los datos y procesos de cualquier empresa. Del mismo modo, también hace referencia al acceso autorizado y ordenado de los usuarios a la información almacenada por la compañía". (p.1)

3.3.2 Política de seguridad

Consisten en una serie de normas que permiten asegurar la confidencialidad, debe ser cumplido por todo el personal relacionado a la empresa. Por lo que, es conjunto de reglas que implementan una serie de mecanismos para garantizar un nivel de seguridad adecuado sobre los recursos informáticos en una organización. Según IBM (2021), las políticas de seguridad "define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema." Así como en el mismo documento en su portal de internet, menciona que "proporciona una base para la planificación de la seguridad al diseñar nuevas aplicaciones o ampliar la red actual, describe responsabilidades del usuario como las de proteger información confidencial." (p.1)

3.3.3 Identity Stores (bases de datos)

Cisco Systems en su guía oficial de CCPN Security Identity Management (2021), lo describe como una base de datos que guarda todas las credenciales de los usuarios o endpoints (usuarios finales). Es utilizado para autenticar la identidad, puede encontrarse en una base de datos interna que reside en un servidor AAA o una base de datos externa que almacena las identidades. Pueden existir usuarios internos, para un grupo limitado de usuarios, dedicado a un control interno de la red, así como existen usuarios externos, utilizado como la base principal de todas las credenciales de los usuarios, aquí se incluye el Active Directory (AD), Lightweight Directory Access Protocol (LDAP), RADIUS token server, etc.

3.3.3.1 Active Directory (AD)

El Active Directory es un producto de Microsoft, donde cumple la función de servicio de directorio en una red. Utiliza protocolos como LDAF, DNS y DHCP. Permite a los administradores establecer políticas en la empresa, así como desplegar programas en varios ordenadores. Por lo que el AD, almacena toda la información en una base de datos centralizada,

organizada y accesible a los administradores. Según Microsoft (2022), explica en su portal de internet:

> "Active Directory almacena información acerca de los objetos de una red y facilita su búsqueda y uso por parte de los usuarios y administradores. Active Directory usa un almacén de datos estructurado como base para una organización jerárquica lógica de la información del directorio." (p.1)

3.3.4 Protocolos de Autenticación

3.3.4.1 Protocolo AAA

El protocolo AAA contiene la autenticación, autorización y contabilidad. Normalmente se utiliza para el diseño de sistemas de control de acceso a redes de datos, de forma centralizada en un mismo nodo o red.

- **Autenticación**

La autenticación viene del término en inglés *Authentication*, considerándose una de las primeras A's. A través de su trabajo de investigación, Corredera (2020) lo define como, "…verificar la identidad de un usuario antes de permitir que acceda a un recurso de red o servicio. Esto se consigue haciendo coincidir las credenciales proporcionadas … (por ejemplo, Nombre – contraseña) con las credenciales almacenadas en un servidor AAA." (p.12)

- **Autorización**

La autorización, del inglés *Authorization*, se refiere a los permisos que se le provee al usuario en el momento de autenticar sus credenciales, concretamente se envía una solicitud al servidor que contiene la información del usuario. Greyrat (2022) define la función de la autorización a través de que "determina el alcance del acceso a la red y qué tipo de servicios y recursos son accesibles para el usuario autenticado. La autorización es el método para hacer cumplir las políticas." (p.1)

- **Contabilidad**

La contabilidad, del término en inglés *Accounting*, se entiende cómo la última de las tres A's. Se ve incluida en el Modelo y *framework* de Red de Gestión de Telecomunicaciones ISO/ITU-T para la gestión de redes. Según Corredera (2020), la contabilidad está basada en "medir la cantidad de recursos que consume un usuario durante su acceso, incluyendo información como la cantidad de tiempo que ha usado del sistema o la cantidad de datos enviados y/o recibidos durante una sesión" (p.22)

Así mismo, se define que la contabilidad posee un proceso donde se mantiene un registro de estadísticas de la sesión del usuario, por el almacenamiento conectado en la red (NAS) al servidor.

3.3.4.2 Protocolo RADIUS

Sus siglas indican Remote Authentication Dial-In User Server, posee acceso a la información de las cuentas de usuario y comprueba las credenciales de autenticación de los accesos a la red. Hassel (2003), en su obra llamada RADIUS, afirma que:

> Es un protocolo para el control de acceso a la red, implementado en dispositivos como routers, switch y servidores, provee autenticación centralizada, autorización y manejo o contabilización de cuentas (AAA). Es un sistema de seguridad distribuido que garantiza el acceso remoto a redes y servicios de la red contra el acceso no autorizado". (p.34)

De esta manera, RADIUS se describe como un protocolo que se basa en un modelo cliente-servidor, donde el servicio de AAA son administrados por un proveedor de recursos cual es el servidor RADIUS. Consta de un servidor de autenticación, un autenticador y por último un suplicante o cliente.

- **Funcionamiento de RADIUS**

Cuando un usuario o equipo envía una solicitud a un servidor de acceso a la red (NAS) para obtener acceso a un recurso de red particular, envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere al dispositivo NAS a través de los protocolos de la capa de enlace, por ejemplo, PPP quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS solicitando el acceso a la red. El servidor RADIUS comprueba que la información es correcta utilizando algunos de los esquemas de autenticación (esto dependen del propio servidor RADIUS).

3.3.4.3 Protocolo TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) es un protocolo de seguridad desarrollado por Cisco Systems Inc. Debido que RADIUS no abarcaba ciertas áreas que eran necesarias tomar en cuenta. Mañas (2016), en su obra "Guía de Seguridad CCN-STIC-401)", posee un glosario donde explica que TACACS+ consiste en:

> Un protocolo basado en TCP que mejora el TACACS al separar las funciones de autenticación, autorización y contabilidad y al cifrar todo el tráfico entre el servidor de acceso a la red y el servidor de autenticación. TACACS+ es extensible para permitir el uso de cualquier mecanismo de autenticación con clientes TACACS+. (p.977)

Por lo que, TACACS+ provee una validación centralizada de usuarios que intentan acceder a un recurso en la red, cifra el cuerpo de los paquetes a enviar, en el encabezado del paquete, indica si se encuentra cifrado o no. De esta manera, TACACS+ implementa los servicios de AA separando cada uno de estos procesos.

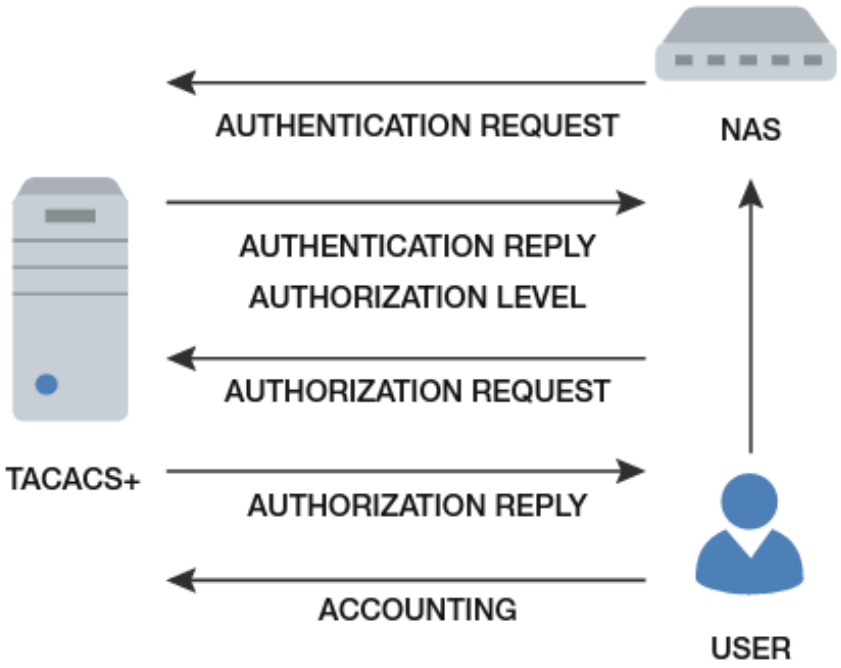


Figura 6. Secuencia de mensajes TACACS+.
Fuente: tacacs.net (2011)

3.3.5 Protocolos de descubrimiento

3.3.5.1 Protocolo CDP

Según CISCO (s.f), "El Cisco Discovery Protocol (CDP) es un protocolo de propietario de Cisco de la capa de link que permite que los dispositivos de Cisco comuniquen sin importar la conectividad de capas de red." (p.1)

Por lo que, se conoce como un protocolo de capa 2 para recopilar información sobre dispositivos conectados físicamente entre sí, por lo que a través de este protocolo se puede obtener información de los equipos vecinos y se ejecuta exclusivamente en equipos del fabricante CISCO, como routers, switches y servidores de acceso. Se ejecuta en todos los medios LAN y WAN. De esta manera, cuando un dispositivo vecino recibe un mensaje CDP, puede utilizar esa información para construir una tabla de vecinos que muestra qué dispositivos están directamente conectados. Además, los dispositivos pueden intercambiar información sobre la capacidad de la interfaz, como el tipo de medios soportados. La información proporcionada por CDP es la siguiente: Nombre del dispositivo, Plataforma, Versión del software del equipo, Dirección IP, Interfaz remota, nombre dominio VTP, VLAN nativa y estado del dúplex.

3.3.5.2 Protocolos LLDP

Según CISCO (s.f) “El protocolo LLDP (Link Layer Discovery Protocol) es un protocolo de detección de capa de enlace definido en el estándar IEEE 802.1AB. LLDP permite a los dispositivos de red anunciar información sobre ellos mismos a otros dispositivos de la red.” (p.1)

De esta manera, su objetivo principal es permitir que los dispositivos en una red se descubran mutuamente y compartan información sobre sí mismos, ya que este protocolo permite a dispositivos de diferentes fabricantes comunicarse entre sí. Existen “paquetes de anuncio” a través de estos enlaces que contienen información como su identidad, capacidades y configuración. Por lo que, este protocolo facilita la gestión de la red y el mantenimiento, para obtener información sobre los dispositivos vecinos en una red local.

3.3.5.3 Protocolo EIGRP

El Protocolo de Enrutamiento de Gateway Interior Mejorado es un protocolo de enrutamiento avanzado desarrollado por Cisco Systems. Según los autores Mier y Mier (2008) en su obra “PROTOCOLOS DE ENRUTAMIENTO RIP, OSPF Y EIGRP” explican que:

> EIGRP es un protocolo avanzado basado en las características asociadas con los protocolos del estado de enlace. Es independiente, no confía en TCP/IP para intercambiar información de enrutamiento; para esto utiliza el Protocolo de transporte fiable a fin de garantizar la entrega de la información de enrutamiento. (p. 52-53)

De esta manera, es importante destacar que el protocolo EIGRP combina características de enrutamiento de vector de distancia y enrutamiento de estado de enlace, lo que lo convierte en un protocolo híbrido de enrutamiento.

3.3.6 Estándar IEEE 802.1X

El estándar de autenticación IEEE 802.1X permite controlar el acceso a los servicios de red a través de sus puertos, opera en la capa dos del modelo OSI, asegura el intercambio de las credenciales de usuario o dispositivo evitando cualquier acceso no autorizado a la red. Arias, Carrillo (2017) explican en su obra de “Rediseño del sistema de Autenticación de usuarios de una red corporativa”, una infraestructura de red 802.1x que requiere de tres elementos para operar: suplicante, equipos autenticadores y servidor de autenticación:

- Suplicante: Es el cliente por medio de un software solicita tener acceso a los recursos de la red.

- Autenticador: Puede ser un switch, un punto de acceso, componente que a través los usuarios acceden a los servicios de red, su función es forzar el proceso de autenticación y enrutar el tráfico.
- Servidor de autenticación: Se encarga de procesar la autenticación de las credenciales del usuario
- Por lo general se emplean bases de datos para realizar este proceso tales como: SQL, Microsoft AD, LDAP, entre otros. (p.18)

3.3.6.1 Funcionamiento del Estándar IEEE 802.1X

Consiste en cinco procedimientos a través de los elementos: clientes, autenticador, y servidor. Primeramente, el cliente inicia comunicación, enviando un mensaje en un paquete EAP. El autenticador responde con un EAP. La respuesta de identidad es enviada a través de un puerto, pidiendo las credenciales, el cliente le responde al autenticador con credenciales, y por último el autenticador reenvía las credenciales al servidor.

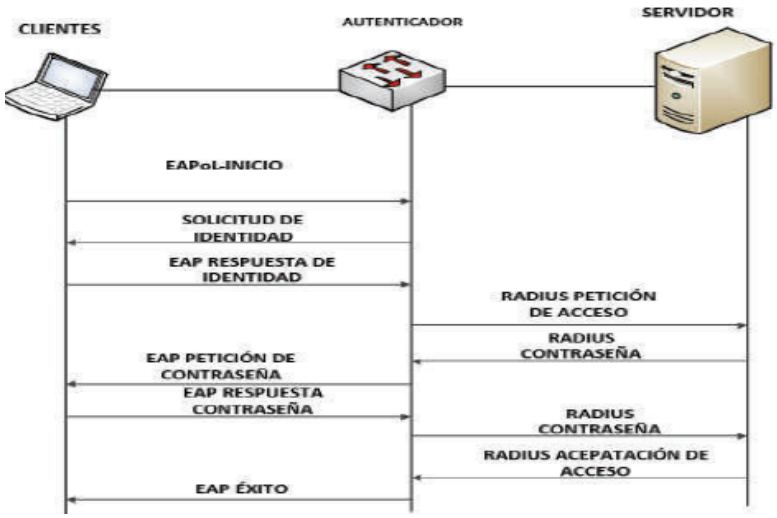


Figura 7. Funcionamiento del estándar IEEE 802.1X.
Fuente: Paredes M., Urbina W., Espinosa N. (2014)

3.3.6.2 Protocolo EAP

El protocolo EAP usa un controlador de acceso "autenticador", cual permite o niega el acceso del usuario en la red. Consistiendo en tres elementos como es el usuario, quien es validado a través de credenciales. Luego el controlador de acceso, conociéndose como un firewall actuando entre el usuario y el servidor de autenticación. Por último, el servidor de autenticación, a través de NAS se comprueba la identidad del usuario por el controlador de la red y otorgar acceso al usuario.

- **EAP TLS**

Se define como "…un sistema de autenticación fuerte que se basa en certificados digitales, tanto del cliente como el servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos." (Arias, Carillo, 2017, p. 21)

- **EAP TTLS**

Arias, Carillo (2017), lo define como "…un sistema de autenticación que se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS." (p.22)

3.3.7 ISO 27000

La ISO 27000 es conocido como un conjunto de estándares que proporcionan un marco teórico para la gestión de seguridad de la información. Son publicadas por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional.

3.3.7.1 ISO 27001

Según Corletti, la norma ISO 27001, está basada en aspectos fundamentales que cubren una visión de consideración para cualquier empresa que desee la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Por lo que, es la normativa que define la calidad con que se adopta y gestionan medidas de seguridad.

3.3.7.2 ISO 27002

Según el autor anteriormente citado, la norma ISO 27002, es una recopilación mejorada para la Gestión de Seguridad de la Información (SGSI). Luego de la determinación de requerimientos para la seguridad, se seleccionan controles apropiados que se deben implementar para reducir riesgos. Contiene un total de 133 controles.

3.3.8 CISCO

3.3.8.1 CISCO ISE

La empresa Cisco Systems Inc. Incorporó las soluciones de autenticación de Access Control Server (ACS) con las soluciones NAC, por lo que ofrece la plataforma ISE. Según Cisco Systems (2014) "permite cumplir las políticas de seguridad de acceso en forma confiable. Es una plataforma contextual, basada en identidad, que recolecta información en tiempo real de la red, usuarios y dispositivos."

Hoy en día es utilizado como un producto para la administración de la red, permitiendo la creación y aplicación de políticas de seguridad y acceso para dispositivos finales (*endpoints*), conectados a *routers* y *switches* de la empresa. CISCO ISE realiza una verificación rigurosa y reconocimiento automático del perfil del dispositivo, permite realizar reconocimiento automático de las características de los equipos añadidos, así como permite tener control total

de la visibilidad de la red. Posee un estricto cumplimiento de políticas de seguridad, definiendo políticas de acceso que cumpla con los requisitos. Es una plataforma dinámica debido a que presenta una interfaz de estadísticas en forma de gráficos, así como creación, visibilidad y generación de reportes de la red empresarial.

- **Características CISCO ISE**
  - Aplicación uniforme de políticas contextuales en las redes fijas e inalámbricas.
  - Visibilidad de todo el sistema para saber qué y quién está en la red fija, inalámbrica o VPN.
  - Servicios de AAA integrados, perfiles (profiling), estado (posture) y usuarios temporales.
  - Identificación automática y precisa de dispositivos mediante sondas basadas en ISE.
  - Integración BYOD simplificada mediante registro de autoservicio.
  - Automatiza la aplicación de políticas y configuración de dispositivos de acceso.
- **Arquitectura CISCO ISE**
  - **Administration Persona (PAN)**

El nodo de administración permite realizar todas las acciones y operaciones administrativas de la red. Tiene acceso a todas las configuraciones del sistema y el funcionamiento de la autenticación, autorización y auditoría.

  - **Monitoring Persona (MnT)**

El nodo de monitoreo permite a CISCO ISE ser colector de información como mensajes de registro, repositorio de información de administración creada para usuarios, grupos y dispositivos. De esta manera, igualmente tiene la función de ser un repositorio de información de las políticas de servicio para el nodo PSN.

  - **Policy Services Persona (PSN)**

El nodo de políticas de servicio, proporciona las políticas de acceso a la red, acceso de invitados, clientes y perfiles de servicio. De esta manera, este rol evalúa las políticas y toma las decisiones hacia los usuarios de la red a través de una solicitud al nodo. Por lo que, el PSN se encarga del tráfico entre los dispositivos de la red y el CISCO ISE.

3.3.8.2 AnyConnect

Siendo un producto de CISCO, la empresa afirma que es un: "… agente unificado de terminales de seguridad que ofrece diversos servicios de seguridad para proteger la empresa. También proporciona la visibilidad y el control que necesita para identificar qué usuarios y dispositivos acceden a la empresa extendida." (Cisco Systems, 2017, p.1). Incluye funciones como acceso remoto, acceso VPN a través de protocolos Secure Sockets Layer (SSL) e Ipsec IKEv2.

3.4 Bases Legales.

3.4.1 Constitución de la República Bolivariana de Venezuela.

Con relación a las bases legales, la Constitución de Venezuela no posee leyes que sustenten las amenazas que pueden perjudicar la red empresarial de una empresa, sin embargo, el Artículo 60 actúa como soporte legal en la presente investigación, adscrito a la Constitución de la República Bolivariana de Venezuela (1999).

> **Artículo 60**: Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

3.4.2 Ley Especial contra Delitos Informáticos (2001)

De igual modo, en Venezuela existe un organismo llamado Comisión Nacional de Telecomunicaciones (CONATEL), cual regula la calidad de los servicios prestados en el país y elaborar planes y políticas nacionales de telecomunicaciones. Creando la Ley Especial contra Delitos Informáticos, publicado el 30 de octubre de 2001 en la Gaceta Oficial Nº 37.313. Así mismo, presentando los artículos que rigen la presente investigación:

> **Artículo 6:** Acceso indebido. Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

> **Artículo 7**: Sabotaje o daño a sistemas. Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes

que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias**.**

Artículo 9: Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 11: Espionaje informático. Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

Artículo 20: Violación de la privacidad de la data o información de carácter personal. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

3.5 Definición de términos

NAC: Network Access Control. Es un método para reforzar la seguridad, la visibilidad y la gestión de acceso de una red propietaria.

Device Administration AAA: Controla el acceso de los dispositivos de red. Es un usuario que inicia sesión en los dispositivos de red, para configurar y mantener los dispositivos administrados. Utiliza el protocolo TACACS+.

Network Access AAA. El servidor AAA interactúa con servidores de puerta de enlace y de acceso a la red con credenciales. El servidor AAA utiliza RADIUS.

DNS: Servicio de nombres de dominio que permite la administración de los nombres de ordenadores. Este servicio constituye el mecanismo de asignación y resolución de nombres (traducción de nombres simbólicos a direcciones IP) en Internet.

SSID: Es el nombre público que identifica una red local inalámbrica, es decir, una WLAN. Son las siglas de Service Set Identifier.

AV PAIRS: AV en AV-Pair significa valor de atributo. Algunos tipos de ejemplos incluyen pares TACACS+ y RADIUS AV. Estos pares AV se pueden utilizar para definir elementos específicos de autenticación, autorización y contabilidad para cada sesión individual.

IP address; Dirección del Protocolo de Internet. Este protocolo es un conjunto de reglas para la comunicación a través de Internet. Una dirección IP identifica una red o dispositivo en Internet.

VPN: Virtual Private Network, o red privada virtual. Establece una conexión segura y cifrada entre su ordenador e Internet y proporciona un túnel privado para sus datos y comunicaciones mientras utiliza las redes públicas.

SSH: Secure Shell, es un protocol de red destinado principalmente a la conexión con máquinas a las que accedemos por línea de comandos. Se puede conectar con servidores, usando la red internet como vía para comunicaciones.

TELNET: Es un protocolo de red de aplicación que permite la comunicación de usuario con un computador remoto a través de una interfaz basa den texto. Crea una conexón de terminal virtual, permitiendo a los usuarios acceder a las aplicaciones en un equipo remoto.

CAPÍTULO IV

MARCO METODOLÓGICO

La investigación presente está dirigida a realizar la implementación de una plataforma de sistema de acceso con políticas de seguridad para la empresa Avícola La Guásima C.A, para este cometido, se definirá el tipo de investigación, diseño de investigación, nivel de investigación, población y muestra, técnicas e instrumentos para la recolección de datos, las fases metodológicas, y la confiabilidad de la investigación.

Según Palella y Martins (2012) "se refiere a la clase de estudio que se va a realizar. Orienta sobre la finalidad general del estudio y sobre la manera de recoger las informaciones o datos necesarios". (p.88) Por lo que, lo podemos definir como el tipo de metodología que incluye cómo se realizará el estudio para el problema planteado. Se destaca de esta manera, el Trabajo de Grado que se está desarrollando se dirige a un enfoque cualitativo. Según Hernández, Fernández y Baptista (2010), definen el enfoque cualitativo como "utiliza recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación y puede o no probar hipótesis en su proceso de interpretación." (p. 7). De esta manera, se estudiará la naturaleza de nuestras variables y cómo se desempeñan cualitativamente en la investigación.

4.1 Tipo de Investigación

Se entiende tipo de investigación como la comprensión de cómo se desarrollará el estudio, añadiendo información sobre el propósito de la misma y la forma de recolectar datos. En las investigaciones de Palella y Martins (2012), explican que. "El tipo de investigación se refiere a la clase de estudio que se va a realizar. Orienta sobre la finalidad general del estudio y sobre la manera de recoger las informaciones o datos necesarios."

Por lo que, el tipo de esta investigación es proyecto especial. Es caracterizado por un proceso estricto de investigación, con el diagnóstico del problema, con la elaboración de una solución y una implementación factible para resolver una problemática. En este sentido, en el Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales UPEL (2016) define el proyecto especial como un estudio que: "incluye la demostración de la necesidad de la creación o de la importancia del aporte, según el caso, la fundamentación teórica, la descripción de la metodología utilizada y el resultado concreto del trabajo en forma acabada" (p.22). Siendo así el caso de la presente investigación, cual busca elaborar una propuesta

factible para la empresa Avícola La Guásima C.A. con las políticas de seguridad de la red empresarial.

4.2 Diseño de la Investigación

El diseño de la investigación está basado en el modelo metodológico que se asume en la investigación para dar respuesta a la problemática señalada. Los autores Altuve y Rivas (1998) asegura que el diseño de una investigación, “es una estrategia general que adopta el investigador como forma de abordar un problema determinado, que permite identificar los pasos que deben seguir para efectuar su estudio” (p. 231)

En cuando a la investigación, existen dos tipos de diseño de investigación a tomar en cuenta. La investigación documental, se describe como una revisión sistemática del material a considerar y análisis de los datos que provienen del mismo. En la investigación de Arias (1997) señala que "es aquella que se basa en la obtención y análisis de datos provenientes de materiales impresos u otros tipos de documentos" (p.47). Por otro lado, se encuentra la investigación de campo, el mismo autor define su concepto como: “Consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna”. Por lo que, el investigador procede a recolectar datos necesarios sin ser alterados por un agente externo. Por consiguiente, la presente investigación presentará dos diseños como son la investigación documental y de campo, garantizando obtener la información necesaria para el avance de la investigación.

4.3 Nivel de la Investigación

En relación con el nivel de la investigación, indica si la investigación se basa en un acercamiento superficial o si el investigador profundizará el tema tratado. Según Arias (1999) “El nivel de investigación se refiere al grado de profundidad con que se aborda un objeto fenómeno. Aquí se indicará si se trata de una investigación exploratoria, descriptiva, explicativa” (p. 19).

Por lo que, se define el nivel de la investigación como descriptivo, puesto que se interpreta la realidad de la problemática, conjunto a una descripción registro, análisis e interpretar los fenómenos. Se dedica a construir conclusiones sobre el tema de investigación y cómo funciona en la actualidad. Según el mismo autor, Arias (1997), define que este nivel de investigación consiste en “la caracterización de un hecho, fenómeno o grupo con el fin de

establecer su estructura o comportamiento (...) mide (n) de forma independiente las variables (p.48).

4.4 Población y muestra

La población se define como el conjunto de unidades, personas u objetos cual se dirige el objeto de estudio, para obtener información de la misma, de modo que una conclusión sea generada. Los autores Palella y Martins (2012), definen la población como: "La población puede ser definida como el conjunto finito o infinito de elementos, personas o cosas pertinentes a una investigación y que generalmente suele ser inaccesible" (p.105). De modo que, la población de la presente investigación está conformado por la red de datos de la empresa Avícola La Guásima, C.A, como la sede principal y los sitios foráneos como son las granjas y sitios de producción.

En el mismo orden de ideas, la muestra se refiere al porcentaje seleccionado de la población que permite concretar características y comportamientos de la población escogida en general. Los autores mencionados anteriormente la definen como "la escogencia de una parte representativa de una población, cuyas características reproduce de la manera más exacta posible." (p.106). La muestra de la presente investigación se enfocará en la red de datos del Departamento de Telecomunicaciones ubicado en la sede principal de la empresa Avícola La Guásima, C.A.

4.5 Técnicas e Instrumentos de recolección de datos.

4.5.1 Técnicas de Recolección de Datos.

Con respecto a las técnicas de recolección de datos, se refiere a las diferentes formas para obtener datos de la problemática a tratar. Según, Arias (2006), "las técnicas de recolección de datos son las distintas formas o maneras de obtener la información". (p.53) En la presente investigación, se hará uso de la observación directa, la entrevista y la encuesta.

Observación Directa.

En la presente técnica de recolección de datos, la observación directa se enfoca en el área de estudio y utiliza la observación para recaudar información crítica para la investigación y organizarla de forma intelectual. Fernández y Baptista (2006), expresan que: "la observación directa consiste en el registro sistemático, válido y confiable de comportamientos o conducta manifiesta" (p.316). Con esta técnica, la problemática de Avícola La Guásima, C.A podrá ser

observada directamente y al mismo tiempo, será un recurso importante para la resolución de la misma.

Entrevista.

Palella y Martins (2012) definen esta técnica de recolección de datos como “Una técnica que permite obtener datos mediante un diálogo que se realiza entre dos personas cara a cara: el entrevistador "investigador" y el entrevistado; la intención es obtener información que posea este último.” (p. 119) Es una técnica por donde se obtiene información concisa y detallada a partir de personas involucradas en el área de estudio. Es un recurso importante ya que, en esta, se consigue la opinión, críticas, información y datos que serán recompilados para su uso en la presente investigación. Se destaca entonces, la entrevista directa con el gerente del Departamento de Telecomunicaciones debido al nivel de autoridad que posee en la empresa y coordinador de las operaciones diarias de la misma.

Revisión documental.

Machuca (2022) en su investigación, explica que la revisión documental “consiste en realizar una investigación y recopilación de información a través de la revisión de diferentes fuentes documentales”. Por lo que, se refiere a la búsqueda e investigación de información en diferentes medios disponibles, sirviendo como base para el presente estudio.

4.5.2 Instrumentos de Recolección de Datos.

Los instrumentos son definidos por Palella y Martins (2006), como “un instrumento de recolección de datos es, en principio, cualquier recurso del cual pueda valerse el investigador para acercarse a los fenómenos y extraer de ellos información.” (p. 137) Para el presente trabajo, se hará uso de la guía de observación y entrevista estructurada.

Guía de observación.

La guía de observación se conoce como un instrumento con la funcionabilidad de enlistar información importante al momento de estudio, útil para el análisis de la misma. Según Ortiz (2004), en su obra Métodos y Técnicas de Investigación Documental Y De Campo, explica que la guía de observación es:

> Es un instrumento de la técnica de observación; su estructura corresponde con la sistematicidad de los aspectos que se prevé registrar acerca del objeto. Este instrumento permite registrar los datos con un orden cronológico, práctico y

> concreto para derivar de ellos el análisis de una situación o problema determinado. (p.75)

Guía de entrevista.

Según Feria, Matilla y Mantecón (2020), explican que "la guía de la entrevista constituye el instrumento metodológico que permite la aplicación del método en la práctica." (p.69) Por lo que, la guía de entrevista se aplica a los individuos para obtener datos sobre el objeto de estudio, a través de diferentes preguntas.

Diario de campo.

Según Bonilla y Rodríguez (1997), explican que el diario de campo "debe permitirle al investigador un monitoreo permanente del pfroceso de observación. Puede ser especialmente útil [...] al investigador en él se toma nota de aspectos que considere importantes para organizar, analizar e interpretar la información que está recogiendo". (p.129) Permitiendo de esta manera, sistematizar las prácticas investigativas del estudio, enriqueciendo la teoría-práctica del cometido.

Registro Fotográfico.

Augustowsky, G. (s. f.) explica en su obra que "Las tomas fotográficas se emplean para el relevamiento sistemático de aquellos aspectos o cuestiones en los que los registros clásicos –como la transcripción escrita de lo observado– resultan insuficientes". Por lo que, se trata de reflejar a través de fotografía prueba y registros sobre material resaltante para la presente investigación.

Tabla de actividades.

Para el cometido de la investigación, se realizaron tablas de actividades para enumerar y resumir las diferentes actividades, así como tareas para cada fase metodológica de esta investigación. Contarán con un cuadro de actividades, descripción de cada actividad, las tareas de cada actividad y así mismo el responsable de la actividad. Es utilizado para favorecer el orden y explicar con claridad los procedimientos llevados a cabo en cada fase de esta investigación.

4.6 Técnicas de análisis de resultado

Luego de los datos recolectados, son procesados para el estudio y aplicados en el proyecto. Hurtado (2012) "son las técnicas de análisis que se ocupan de relacionar, interpretar y buscar significado a la información expresada en códigos verbales e icónicos". (p.181).

Diagrama Causa-Efecto

Se conoce como una técnica para relacionar las causas que pueden estar creando una consecuencia en el área a investigar, permitiendo determinar el tipo de origen que pueda presentar la problemática. Según Gutiérrez (2005), el diagrama causa-efecto o diagrama de Ishikawa es un método grafico que refleja la relación entre una característica de calidad (muchas veces en el área problemática) y los factores que posiblemente contribuyen a que existan. (p.165)

Matriz FODA

Thompson y Strickland (1998) establecen que el análisis FODA estima el hecho que una estrategia tiene que lograr un equilibrio o ajuste entre la capacidad interna de la organización y su situación de carácter externo; es decir, las oportunidades y amenazas. Por lo que, resulta una herramienta muy efectiva para analizar las fortalezas y debilidades (internas en la empresa investigada) y oportunidades y amenazas (externas a la empresa investigada), a través se pueden generar estrategias para las condiciones observadas.

4.7 Fases metodológicas

Fase I: Diagnóstico de las condiciones de la empresa con respecto a la eficiencia de las políticas de seguridad del sistema de acceso de Avícola La Guásima C.A.

En la primera fase, se observará la situación actual de la impresa. Se recogerá información con referente a las políticas de seguridad actuales y el manejo de la seguridad en la red empresarial. El investigador se encargará de realizar una visita a la empresa para la observación directa de la misma y documentar datos primarios sobre el estudio a realizar, por medio del uso de la guía de observación, detectando la problemática y las causas que la origina. En esta fase, se hace uso de la tabla de actividades y la entrevista formal a través de la guía de entrevista. Se aplicarán las técnicas de análisis de datos obtenidos de la entrevista formal, utilizando diagrama de Causa-Efecto y Matriz FODA.

Fase II: Análisis de la estructura actual de la topología de la interconexión de la red empresarial y las configuraciones disponibles a través del medio/plataforma para el proceso de seguridad de datos y usuarios.

En la segunda fase del presente trabajo, se realizará el estudio de la topología de la red empresarial, como es la sede principal y los sitios foráneos. Se realizará el estudio de la red corporativa proporcionada por el cliente a partir de una máquina virtual. Se basará igualmente, en el estudio de las configuraciones que posee la topología previamente investigada, como las

redes disponibles, que existen en la red empresarial a través de la topología investigada. Se asignarán los recursos que son más relevantes para la plataforma CISCO ISE. Por lo tanto, el instrumento de esta fase será la guía de observación.

Fase III: Análisis de los requerimientos proporcionados por el cliente para su implementación en la red empresarial.

La tercera fase de la investigación, está dedicada al análisis de lo que se va a implementar en la red empresarial. El investigador ubicará recursos físicos/lógicos, realizar actualizaciones si lo amerita. Se definirán características, requerimientos mínimos y recomendados, equipamiento para el desarrollo del proyecto para realizar la planificación. El investigador recaudará información para que la implementación se realice de forma óptima y sin complicaciones. Así como, se determinará con exactitud qué versiones, requerimientos se utilizarán. Para esta tercera fase, se aplicará tabla de actividades.

Fase IV: Despliegue de los componentes y estructura lógicas y funcionales de la capa de seguridad.

En esta cuarta fase, se ejecutará la implementación del sistema de acceso a la red de datos, con tecnología CISCO ISE, en la red cableada e inalámbrica. Se creará la máquina virtual facilitada por la empresa Avícola La Guásima, C.A para la instalación del sistema CISCO ISE, a través de la máquina virtual. Se establecerán credenciales, políticas de seguridad para la autenticación, autorización y políticas AAA. Así como roles y administración para el sistema. Así mismo, también se verifica que CISCO ISE está operando en toda la red de Avícola La Guásima, C.A. Se monitorearán y se administrarán los dispositivos finales, así de este modo observando el rendimiento de la misma, mediante la plataforma centralizada del CISCO ISE. Para esta fase, se utilizará la tabla de actividades.

Fase V: Evaluación de la eficiencia de la plataforma de sistema de acceso a la red a través de plan piloto.

En la última fase, se evaluará el rendimiento de la implementación de CISCO ISE en Avícola La Guásima, C.A, se realizará el desarrollo de pruebas de aceptación para el personal TI que se encuentra en el Departamento de Telecomunicaciones. Se contará con la presencia de la gerencia del Departamento de Telecomunicaciones para aceptar el producto y decidir si necesita un tipo de optimización o nuevas políticas que consideren necesarias. Al final de esta

fase, el investigador valorará la factibilidad de la plataforma implementada, y generar recomendaciones para futuras implementaciones.

4.8 Cuadro de Operacionalización de Variables

OBJETIVO ESPECÍFICO 1	VARIABLE	DIMENSIÓN	INDICADORES	ÍTEMS	FUENTE DE INFORMACIÓN
Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.	Sistema de acceso	Políticas de seguridad	Tipos de políticas	1	Técnica: Entrevista
		Políticas AAA (authentication, authorization, accounting)	Validación	2	
		Medios de acceso a la red	Identificación de dispositivos	3 y 4	
			Tipos de dispositivos conectados	5	

Fuente: Pineda, Y. (2023)

4.9 Confiabilidad de la investigación

Según el Manual para la Elaboración y Presentación de los Anteproyectos, Proyectos de Trabajos de Grado, Trabajos de Grado, Tesis doctoral e Informe De Pasantía y Extramuros de la Universidad José Antonio Páez (2020), la confiabilidad se define como: "refiere al nivel de exactitud y consistencia de los resultados obtenidos al aplicar el instrumento por segunda vez en condiciones tan parecida como sea posible." (p.25) La confiabilidad de la presente investigación se basa en la revisión continua de los resultados obtenidos por los instrumentos, así mismo como la utilización de diferentes métodos como es diagrama causa-efecto, matriz FODA y técnica de grupo nominal.

4.10 Validación de instrumento.

Según lo indican Palella y Martins (2012), “La validez se define como la ausencia de sesgos. Representa la relación entre lo que se mide y aquello que realmente se quiere medir” (p. 160). Por lo que, permite la validación del instrumento para asegurar su eficiencia en la presente investigación.

CAPÍTULO V

RESULTADOS DE LA INVESTIGACIÓN

Para el desarrollo del presente trabajo de grado, se describen cada uno de los objetivos específicos planteados, donde toman lugar las cinco (5) fases para establecer los resultados. En este capítulo igualmente se hablará de diferentes recomendaciones, así como las conclusiones de este trabajo de investigación.

5.1 Fase I: Diagnóstico de las condiciones de la empresa con respecto a la eficiencia de las políticas de seguridad del sistema de acceso de Avícola La Guásima C.A.

La empresa "Avícola La Guásima C.A" se encuentra ubicada en Tocuyito, ubicado en el estado Carabobo, en la **figura 8** se puede apreciar que se encuentra en el sector La Guásima, Carretera vieja de Tocuyito, Edif. Que pollo Piso 2 frente a la urb. Villa Jardín. Dicho lugar, cuenta con diferentes edificios, así como lugares remotos como son las granjas.

Figura 8. Sector La Guásima.
Fuente: Google Maps. (2023)

Para el cometido de esta fase, a través de la guía de observación se despliegan diferentes actividades para el diagnóstico de las condiciones de la empresa con relación a las políticas de seguridad y sus causas. En esta primera fase, se evaluó todo lo referente al diagnóstico del lugar de trabajo, así como se recolectó información con respecto a la situación actual de la red empresarial de "Avícola La Guásima C.A".

Tabla 1.
Actividades: Fase 1.

Actividad	Descripción	Tareas	Responsables
1.Realizar checklist (guía de observación)	En esta actividad se procede a realizar y llenar la guía de observación	Aplicar instrumento de recolección de datos: guía de observación	Autor de trabajo de grado
2. Validación de la entrevista formal y presentación de los resultados obtenidos.	En esta actividad se muestra las respuestas obtenidas en la entrevista.	Presentar los resultados obtenidos por la entrevista.	Autor de trabajo de grado
3.Aplicar diferentes técnicas de análisis de resultados.	En esta actividad se analizarán con técnicas los resultados obtenidos.	Realizar Matriz FODA Realizar un esquema Causa – Efecto	Autor de trabajo de grado

Fuente: Pineda, Y. (2023)

- **Actividad Nro. 1: Realizar y completar la guía de observación (checklist).**

En el siguiente apartado se muestra guía de observación a realizar, conformado por ocho (8) preguntas que tienen como objetivo identificar y diagnosticar la condición actual del sistema de acceso de la red corporativa a través de la observación.

Cuadro 2.
Guía de observación.

N°	CHECKLIST	SI	NO	OBSERVACIONES
1	En la red empresarial, ¿existe un programa centralizado que ayude la gestión de control de acceso?		X	
2	¿Los trabajadores se pueden conectar directamente desde los puntos de red?	X		
3	¿Se cuenta con información relativa a los planos de la topología local o inalámbrica de la red empresarial?		X	Poseen listas de Excel con esa información, sin embargo, no planos.

4	¿Existen medidas de seguridad de inspeccionar quién se conecta o cómo a la red empresarial?	X		A través de un filtrado de MAC.
5	¿La infraestructura de la red empresarial posee recursos que puedan ayudar a implementar un nuevo sistema de gestión de acceso?	X		Poseen una red basada en productos CISCO.
6	¿Se controla moderadamente quién se conecta inalámbricamente a la red empresarial?		X	
7	¿Se cumple el protocolo AAA en la red empresarial?		X	
8	¿Las políticas de seguridad son lo suficientemente eficientes para velar la seguridad de los datos de la red empresarial?		X	No se siguen con claridad las políticas de seguridad.
	TOTAL	3	5	
	% POR ITEMS	**37.5 %**	**62.5 %**	

Autor: Pineda, Y (2023)

- **Actividad Nro. 2: Validación de la entrevista formal y presentación de los resultados obtenidos.**

La siguiente actividad presenta la entrevista y los resultados obtenidos por ella. La función dentro de la empresa de los diferentes expertos entrevistados es presentado en el cuadro ##, donde desempeñan el control y supervisión de la red corporativa en la empresa "Avícola La Guásima C.A".

Cuadro 3.

Expertos a entrevistar.

N.º	CARGO
1	Gerente del Departamento de Telecomunicaciones
2	Supervisor de Telecomunicaciones
3	Analista de Telecomunicaciones

Autor: Pineda, Y (2023)

Cuadro 4.

Entrevista estructurada Nro.1.

RESULTADOS DE LA ENTREVISTA		
N.º	**Experto: 1**	**Fecha: 30/1/2023**
	PREGUNTAS	**RESPUESTAS**
1	En la red empresarial, ¿puede usted mencionar las políticas de seguridad en la red y por cuáles medios son implementadas?	Si, efectivamente se pueden mencionar. El planteamiento interno es simple. Existe un control aplicado al acceso a la red Wifi Corporativa (control aplicado en el WLC), también existe un control de tráfico interno entre redes (control aplicado en el NUCLEO de la red) y por último existe un control de tráfico proveniente desde internet (control aplicado en dispositivos perimetrales).
2	Desde su experiencia, ¿qué tipos de procesos se utilizan para validar las credenciales de usuarios en la red?	Las credenciales de usuarios son creadas dentro del "Directorio Activo" empresarial, por lo tanto, el control de credenciales está sujeto a las políticas diseñadas y aplicadas por este. En resumen, la política asigna un tiempo de vigencias de las credenciales, alcances y constitución de la misma.
3	¿Qué tipos de métodos se utilizan para identificar los dispositivos conectados?	Los dispositivos deben ser presentados hasta el equipo técnico de "Soporte de Usuarios", y si el usuario pertenece al grupo exclusivo y autorizado, entonces las direcciones físicas (mac address) del equipo son tomadas y registradas en la BD correspondiente.
4	Desde el departamento de telecomunicaciones, ¿cuáles son los métodos que se utilizan para monitorear a los usuarios conectados a la red?	El proceso es simple, solo se monitorean cuáles son los usuarios conectados a la red wifi corporativa, y ese proceso se lleva a cabo dentro del WLC. El protocolo AAA se podría implementar de una mejor forma en la red empresarial, debido a que posibles ataques podrían provocar una interrupción de operaciones diarias en la empresa, provocando pérdidas.
5	En el ámbito de trabajo, ¿puede usted mencionar los diferentes medios para conectarse en la red empresarial?	Solo dos métodos, alámbrico (solo equipos pertenecientes a la empresa) e inalámbrico (equipos mixtos, es decir, equipos pertenecientes a la empresa y equipo personales, ambos deben pertenecer a un grupo definido, exclusivo y autorizado).

Autor: Pineda, Y (2023)

Cuadro 5.
Entrevista estructurada Nro. 2.

RESULTADOS DE LA ENTREVISTA		
N.°	**Experto: 2**	**Fecha: 30/1/2023**
	PREGUNTAS	**RESPUESTAS**
1	En la red empresarial, ¿puede usted mencionar las políticas de seguridad en la red y por cuáles medios son implementadas?	Una de las políticas de seguridad que se poseen en la red empresarial son el filtrado web para la seguridad de la empresa, bloqueo de IP publicadas no deseadas, así mismo como el bloqueo de cualquier tipo de malware, entre otro tipo de amenaza a la empresa. Una de las cosas que me concierne en las políticas de seguridad son los cambios de contraseña, chequeo de quién se encuentra conectado a la red, etc, puede ser un peligro potencial a nuestra información como la usurpación de identidad, etc.
2	Desde su experiencia, ¿qué tipos de procesos se utilizan para validar las credenciales de usuarios en la red?	Los procesos que se utilizan hoy en día aquí en la empresa para validar credenciales es el user local, es decir, tenemos un Active Directory que ayuda a validar credenciales.
3	¿Qué tipos de métodos se utilizan para identificar los dispositivos conectados?	Se utilizan comandos para identificar los dispositivos conectados, sin embargo, normalmente se registran las direcciones MAC de los dispositivos para que sean ya reconocidos por la red.
4	Desde el departamento de telecomunicaciones, ¿cuáles son los métodos que se utilizan para monitorear a los usuarios conectados a la red?	En la red inalámbrica que se tiene aquí en la empresa se realiza únicamente por el WLC que es el controlador de red inalámbrica, básicamente gestiona puntos de acceso a la red, pero nos gustaría tener más métodos para monitorear usuarios conectados en nuestra red. Nos parece que podríamos utilizar tecnología más innovadora para poder monitorear a los usuarios y dispositivos conectados a la red y complementarla con la tecnología que poseemos ahora mismo.
5	En el ámbito de trabajo, ¿puede usted mencionar los diferentes medios para conectarse en la red empresarial?	Actualmente se tienen los medios locales, es decir, LAN como ejemplo puntos de acceso que están distribuidos en la empresa, y por el medio inalámbrico, donde se pueden conectar teléfonos, laptops, computadoras, etc, por lo que me parece importante tener un control de esa área.

Autor: Pineda, Y (2023)

Cuadro 6.

Entrevista estructurada Nro.3.

RESULTADOS DE LA ENTREVISTA		
N.º	**Experto: 3**	**Fecha: 30/1/2023**
	PREGUNTAS	**RESPUESTAS**
1	En la red empresarial, ¿puede usted mencionar las políticas de seguridad en la red y por cuáles medios son implementadas?	En la empresa existen diferentes tipos de políticas de seguridad, se tienen políticas para filtrar información potencialmente peligrosa a nuestra red, así como bloqueos de páginas, se tiene el uso de CISCO Umbrella en la red. Así mismo se cuenta con el WLC que es un controlador de acceso a la red wifi, igualmente se controla gran parte del tráfico de datos interno, sin embargo, sería más apropiado tener un sistema centralizado que se pueda administrar todo por ese medio.
2	Desde su experiencia, ¿qué tipos de procesos se utilizan para validar las credenciales de usuarios en la red?	Las credenciales de los usuarios que están registrados en la empresa son validadas a partir de una base de datos llamada "Directorio Activo", en ese mismo se aplican políticas a los usuarios, básicamente son usuarios locales y tienen diferentes grupos donde pertenecen.
3	¿Qué tipos de métodos se utilizan para identificar los dispositivos conectados?	Actualmente tengo entendido que los métodos utilizados para identificar los dispositivos conectados se realizan a partir del registro de los mismos con las identificaciones como son el MAC address, no obstante, creo que sería mejor si se pudiera automatizar este procedimiento.
4	Desde el departamento de telecomunicaciones, ¿cuáles son los métodos que se utilizan para monitorear a los usuarios conectados a la red?	El método que se utiliza es a través del control de tráfico de la red inalámbrica, donde se gestiona la cantidad de usuarios conectados. Se utiliza el Meraki que es un Firewall.
5	En el ámbito de trabajo, ¿puede usted mencionar los diferentes medios para conectarse en la red empresarial?	Tengo entendido que son dos medios, alámbrico, es decir por cableado, estos equipos solo son de la empresa únicamente por políticas de seguridad. Y por otra parte se encuentra el inalámbrico, pueden ser personales o pertenecientes de la empresa, me temo que en lugares remotos existe una gran cantidad de endpoints debido a que entre los usuarios se comparten las claves del SSID y puede

		ser preocupante debido a que no se escanea ni se registran a los usuarios que se conectan por este medio.

Autor: Pineda, Y. (2023)

Cuadro 7.

Análisis de las entrevistas estructuradas.

RESULTADOS DE LAS ENTREVISTAS REALIZADAS		
N.º	**Experto: 3**	**Fecha:5/2/2023**
	PREGUNTAS	**RESPUESTAS**
1	En la red empresarial, ¿puede usted mencionar las políticas de seguridad en la red y por cuáles medios son implementadas?	Todos los expertos coincidieron que existen políticas de seguridad que rigen el control y seguridad a la red empresarial, sin embargo, no poseen un sistema centralizado que administre este tipo de políticas además de los recursos que son CISCO UMBRELLA, el WLC y configuraciones de Active Directory que obliga a los usuarios cambiar su contraseña en un plazo de tiempo. Es decir, que están muy distribuidos los recursos utilizados en la red empresarial.
2	Desde su experiencia, ¿qué tipos de procesos se utilizan para validar las credenciales de usuarios en la red?	Los expertos entrevistados estuvieron de acuerdo que todos los usuarios y grupos son registrados a través de un correspondiente "Directorio Activo" donde son validadas las credenciales y se aplican ciertas políticas de seguridad a ellos. Así mismo, el tipo de privilegios que posee en la red empresarial.
3	¿Qué tipos de métodos se utilizan para identificar los dispositivos conectados?	Todos los expertos mencionaron que la dirección MAC de los dispositivos es indispensable para identificar a los dispositivos conectados, sin embargo, algunos coincidieron que este proceso podría estar más automatizado.
4	Desde el departamento de telecomunicaciones, ¿cuáles son los métodos que se utilizan para monitorear a los usuarios conectados a la red?	Los tres expertos entrevistados coinciden que el monitoreo es realizado a partir de la red inalámbrica WLC, donde controla routers, switches, firewalls, gateways, etc. Se utiliza el Meraki que es un Firewall. Así mismo, es posible monitorearlos, sin embargo, comentaron que esta tecnología podría ser complementada con recursos más innovadores y centralizados. Sin embargo, comentaron sobre la mejora de las políticas AAA y cómo podría existir el riesgo de que ataques interrumpan el servicio.

5	En el ámbito de trabajo, ¿puede usted mencionar los diferentes medios para conectarse en la red empresarial?	Las respuestas de los tres expertos se basaron en dos partes, el cableado o alámbrico que son pertenecientes a la empresa y así mismo, el inalámbrico que pueden ingresar dispositivos personales o de la empresa. Uno de los expertos mencionó que le preocupaba una divulgación de la clave del SSID y podría ser un peligro ya que no se escanea apropiadamente quién podría ingresar.

Autor: Pineda, Y (2023)

- **Actividad Nro. 3: Aplicar diferentes técnicas de análisis de resultados.**

En esta última actividad de la primera fase del presente trabajo de grado, se ponen en práctica las técnicas de análisis de resultados anteriormente expuestos en el apartado metodológico, como son el diagrama de causa-efecto y matriz FODA.

Diagrama de Causa-Efecto.

A continuación, se presenta en la **figura 9**, el diagrama de Causa-Efecto o mejor llamado Diagrama de Ishikawa, a través de las entrevistas estructuradas se resumieron las causas explican cómo se puede mejorar la administración de políticas de seguridad de una red corporativa. El Diagrama de Ishikawa consiste identificar raíces de un problema, por lo que se analiza todos los factores involucrados en el proceso y se puede apreciar el problema o efecto, siendo el comportamiento o resultado que se desea cambiar y mejorar.

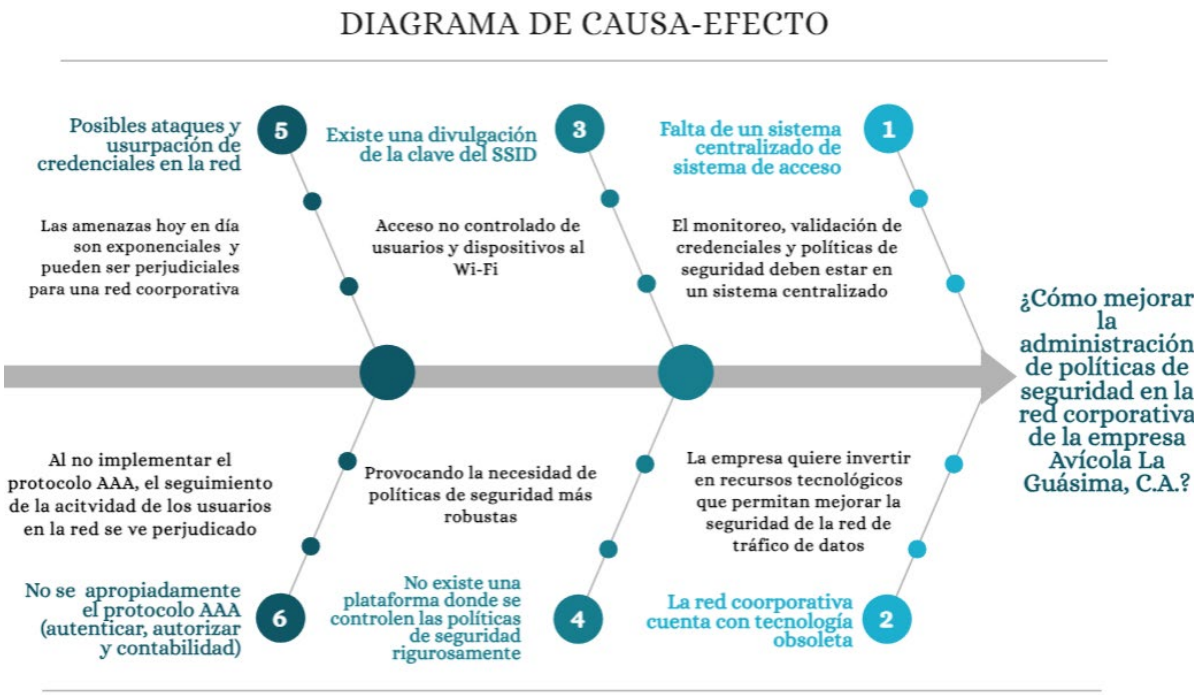


Figura 9. Diagrama Causa-Efecto.
Fuente: Pineda, Y. (2023)

Consiste en seis causas recolectadas, se analizó la situación expuesta por los expertos en las entrevistas y se evaluaron seis puntos principales que son presentados en la **figura** de Diagrama de Causa-Efecto.

Matriz FODA.

La matriz FODA es una técnica de análisis de resultado recomendada para evaluar de manera integral aspectos internos y externos relevantes de una organización. En la presente investigación, se realizaron dos matrices FODA para ver las diferentes fortalezas, oportunidades, debilidades y amenazas que se deben evaluar. La primera matriz FODA evalúa la situación actual de la gestión de acceso y políticas de seguridad de la empresa "Avícola La Guásima" así como información recolectada de las entrevistas realizadas anteriormente.

Las fortalezas son descritas para determinar cómo se puede aprovechar las fortalezas existentes. Las oportunidades podrán identificar aspectos que pueden ser mejorados como la mejora de la seguridad y automatización de tareas. Las debilidades identificarán puntos débiles de la gestión de acceso y seguridad para indicar dónde se puede abordar los problemas y mejorarlos. Por último, se identificarán potenciales amenazas a la seguridad de la empresa, como brechas de seguridad o riesgos cibernéticos, de esta manera, se podrá proteger contra estas amenazas.

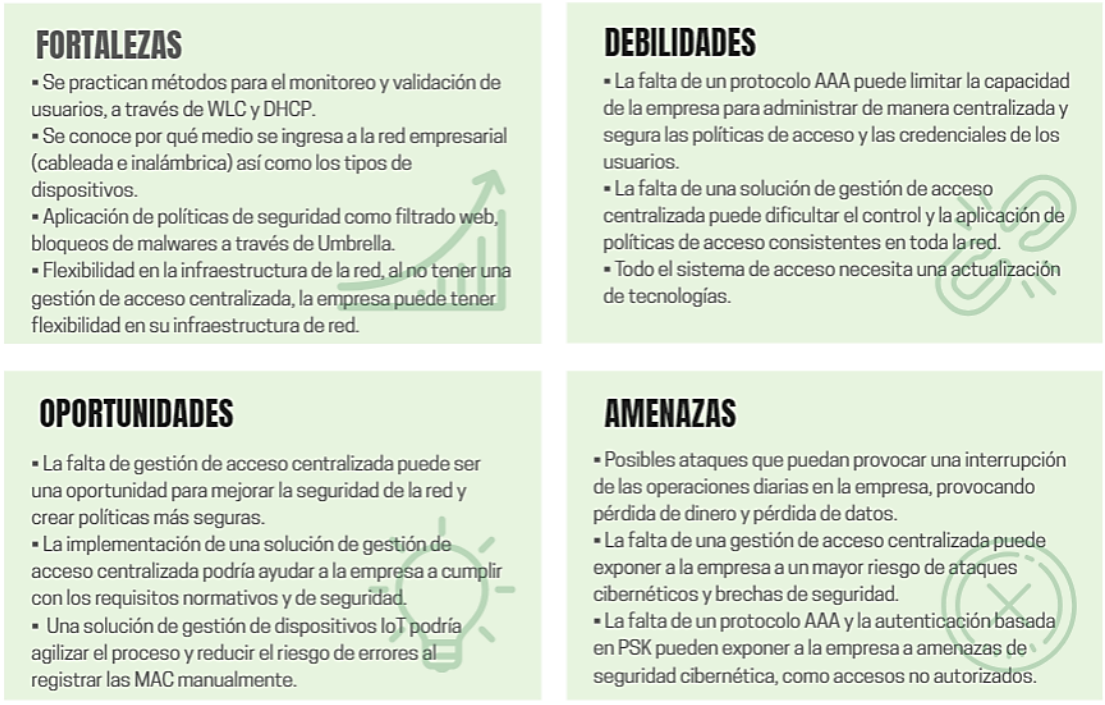


Figura 10. Matriz FODA.
Fuente: Pineda, Y. (2023)

De esta manera, igualmente se aplica la matriz FODA a CISCO ISE para poder realizar una evaluación completa y estratégica a los aspectos internos y externos, al comprender mejor las ventajas, desafíos y oportunidades de CISCO ISE, permitirá tomar decisiones y estrategias para mejorar la gestión de acceso y la seguridad en la red de la organización, apreciado en la **figura 11**.

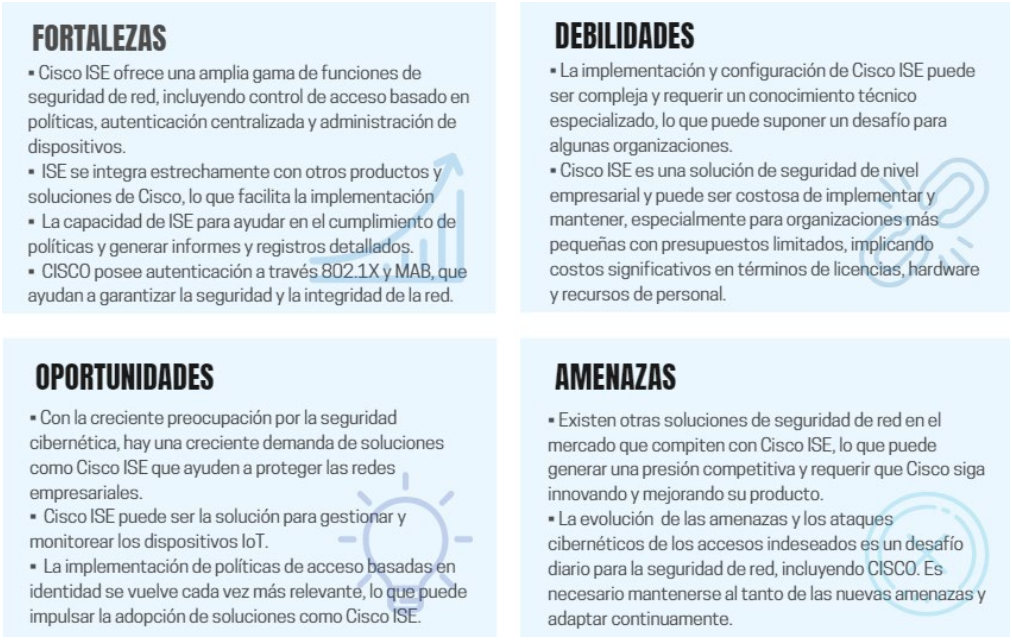


Figura 11. Matriz FODA sobre CISCO ISE.
Fuente: Pineda, Y. (2023)

5.2 Fase II: Análisis de la estructura actual de la topología de la interconexión de la red empresarial y las configuraciones disponibles a través del medio/plataforma para el proceso de seguridad de datos y usuarios.

La siguiente fase consiste en el análisis de la estructura de la topología de la red corporativa de la empresa "Avícola La Guásima C.A", por lo que se impartirán dos (2) tareas esenciales para su cometido.

Tabla 2.
Actividades: Fase 2.

Actividad	Descripción	Tareas	Responsables
1.Levantamiento de la topología actual.	En esta actividad se procede a descubrir la topología actual y levantar un mapa	Investigar y descubrir la topología a través del	Autor de trabajo de grado Equipo de Setrys

	topológico de la red empresarial.	gateaway de la red empresarial	
2.Levantamiento de inventario/recursos.	En esta actividad se procede a realizar el levantamiento de inventario y recursos disponibles en la red.	Investigar y descubrir los recursos e inventario a través de gateaway de la red empresarial	Autor de trabajo de grado Equipo de Setrys

Fuente: Pineda, Y. (2023)

- **Actividad Nro. 1.** Levantamiento de la topología actual.

Inicialmente, el Departamento de Telecomunicaciones proporciona una máquina virtual donde se trabajará remotamente a través de una sesión abierta con *SSH* (Secure Shell) o un *Telnet* (Telecommunication Network), ambos casos permitiendo a los usuarios trabajar remotamente conectándose a un host. Ejecutando de esta manera el comando en consola (cmd): **C:\Users\setrys>ipconfig.**

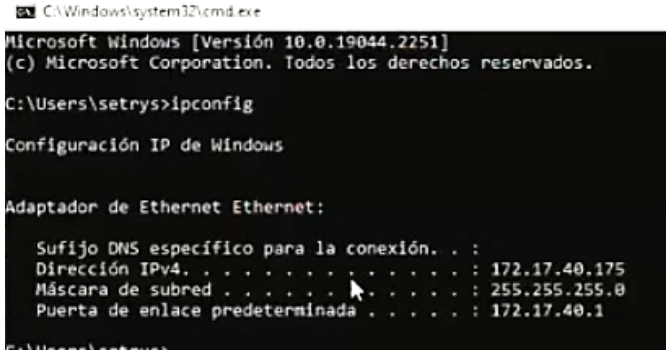


Figura 12. Puerta de enlace preterminada.
Fuente: Pineda, Y. (2023)

De esta manera, permitiendo apreciar el gateaway (puerta de enlace preterminada), en este caso siendo 172.17.40.1. En este caso, se puede apreciar en la **figura 13**, que se abrió una sesión con Telnet, llenando los espacios de 'remote host' con la misma puerta de enlace.

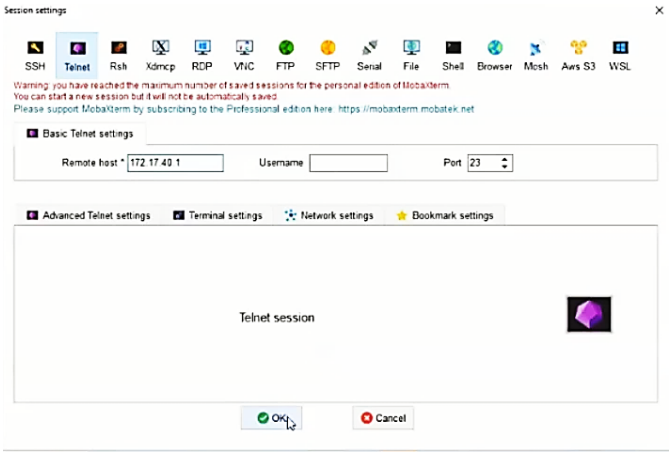


Figura 13. Nueva sesión de Telnet.
Fuente: Pineda, Y. (2023)

Para empezar con el descubrimiento de la red corporativa, inicialmente se abre una sesión en el gateaway del Telnet en la máquina de destino, a través de credenciales de tipo "admin", cuyo equipo es llamado "**VALALGCORE**".

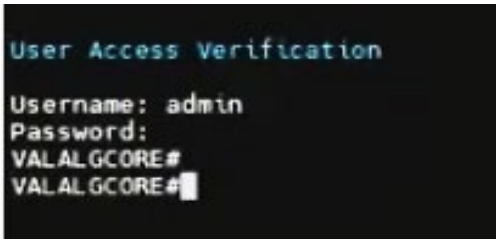


Figura 14. User Access Verification.
Fuente: Pineda, Y. (2023)

Primeramente, para levantar la topología actual de la red corporativa de la empresa "Avícola La Guásima", se tiene como objetivo descubrir qué está conectado localmente entre sí, por lo que el protocolo CDP (Cisco Discovery Protocol) es utilizado para obtener información de router y switches que están conectados, destinado para descubrir vecinos y es una herramienta de gran utilizad de capa 2 (enlace de datos), donde incluye información como identificador del dispositivo, interfaz local, tiempo de espera, capacidad, plataforma e identificador del puerto. Por lo que, el comando mostrado es **VALALGCORE#show cdp neighbors** según la **figura 15**:

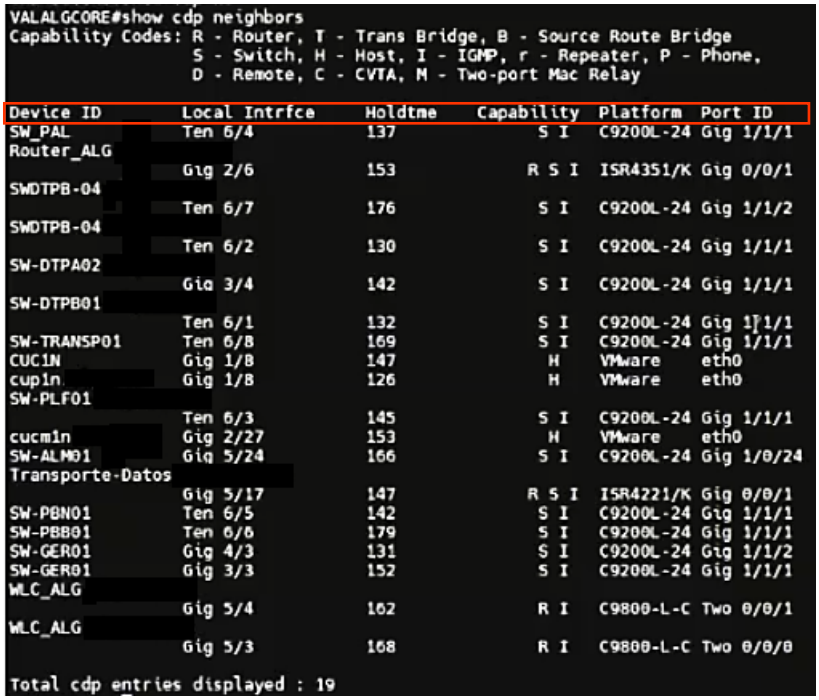


Figura 15. Descubrimiento de equipos vecinos con show cdp.
Fuente: Pineda, Y. (2023)

De esta manera, se descubren equipos CISCO que están conectados en la red y aportando información a la topología de la red. En este mismo orden de ideas, existe el protocolo LLDP (Link Layer Discovery Protocol) siendo un protocolo de detección de vecinos de la capa 2, sin embargo, ha sido creado para estandarizar el descubrimiento de la capa 2 en un entorno donde existen diferentes proveedores. Permite apreciar el identificador del dispositivo, la interfaz local, el tiempo de espera, capacidad e identificación de puerto, a través del comando **VALALGCORE#show lldp neighbors,** ilustrado en la **figura 16**.

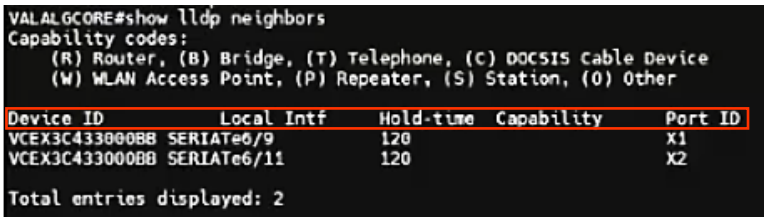


Figura 16. Descubrimiento de equipos vecinos con show lldp.
Fuente: Pineda, Y. (2023)

Siguiendo con el descubrimiento, se hace uso del comando **VALALGCORE#show cdp neighbors detail**. Permite ver los mismos elementos mostrados en el comando **#show cdp neighbors**, de una manera más detallada e información de interés, como es la ip, la plataforma o el modelo de nuestro equipo, la capacidad, la interfaz local y la identificación de puerto, así mismo como la versión del producto, siendo bastante beneficioso para la creación de la topología de la red empresarial.

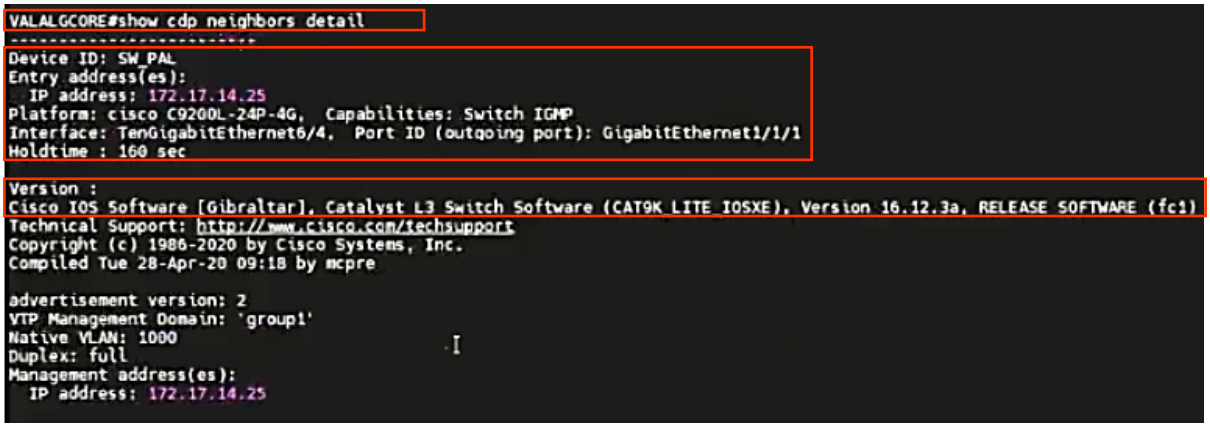


Figura 17. Descubrimiento de los detalles de los vecinos con show cdp.
Fuente: Pineda, Y. (2023)

Es importante resaltar que la misma forma, se tiene que ingresar a cada elemento encontrado para descubrir y establecer la jerarquía con los mismos comandos expuestos anteriormente, de esta manera descubriendo elementos que están conectados a los switches/routers encontrados recientemente. Finalmente, se muestra una lista de elementos principales de la red en la topología local:

Tabla 3.
Tabla de elementos principales en la topología local.

Nro	Elemento	IP
1	SW_PAL	172.17.14.25
2	SW-ALM01	172.17.14.16
3	SWDTPB-04	172.17.14.4
4	SW-DTPB01	172.17.14.2
5	SW-DTPA02	172.17.14.6
6	SW-PLF01	172.17.14.28
7	SW-GER01	172.17.14.9
8	SW-PBB01	172.17.14.24
9	SW-TRANSP01	172.17.14.18
10	SW-PBN01	172.17.14.21
11	Router_ALG	172.17.14.253
12	Transporte-Datos	172.17.253.13
13	cucm1n	10.10.4.12
14	CUC1N	10.10.4.11
15	cucp1n	10.10.4.12
16	WLC_ALG	172.17.41.254

Fuente: Pineda, Y. (2023)

A partir de la **tabla 3**, se crea la topología del sitio principal de la red local de "Avícola La Guásima", se aprecia que cada elemento posee sub-divisiones que fueron descubiertos con protocolos y comandos presentados anteriormente. **(Ver Anexo 1).**

En lo que respecta del site remoto, se utilizaron métodos como comandos e información proporcionada por el cliente para poder descubrir la topología del tráfico de datos. Inicialmente, se tiene entendido que el equipo tiene varias maneras de establecer rutas de redes que están conectadas, rutas que son configuradas por el usuario y son estáticas y por último establecer un protocolo de comunicaciones estándar para aprender redes conectadas a él (vecinos). Por lo que, para apreciar las rutas se utiliza el comando **VALALGCORE#show ip route** en la **figura 18.**

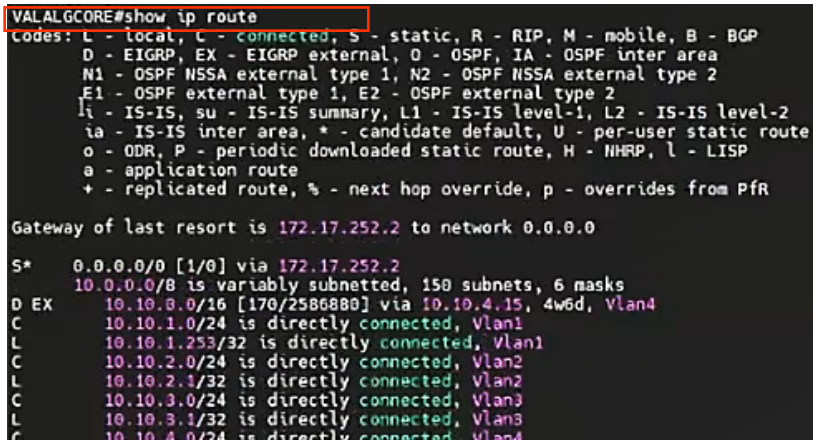


Figura 18. Descubrimiento de rutas del tráfico de datos de la red empresarial.
Fuente: Pineda, Y. (2023)

Se presenta una tabla de enrutamiento, siendo similar a una base de datos local capaz de distinguir cuándo una red se encuentra conectada, es decir, si está configurada estáticamente, significando que está asignada o aprendida por el mismo protocolo de comunicaciones que se habilita con el comando. A partir de la **figura**, se encuentran diferentes códigos cuales determina el origen de la información de enrutamiento a partir de la cual se aprendió una ruta. Una de las variantes de este comando es **VALALGCORE#show ip route connected** mostrado en la **figura 19**.

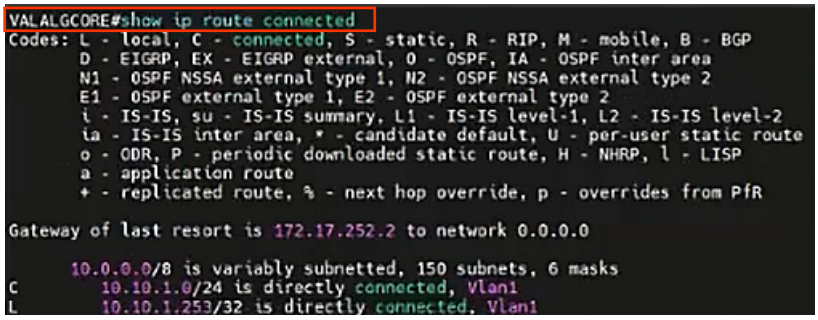


Figura 19. Descubrimiento de rutas conectadas en el tráfico de red.
Fuente: Pineda, Y. (2023)

De esta manera, muestra solo las rutas a redes directamente conectadas presentes en la tabla de enrutamiento, las mismas igualmente se deben estar conectadas a una vlan para que aparezca satisfactoriamente en la tabla de enrutamiento. Agregando a lo anterior, también se utiliza el comando variante **VALALGCORE#show ip route static,** indicando que fue configurada manualmente por un usuario.

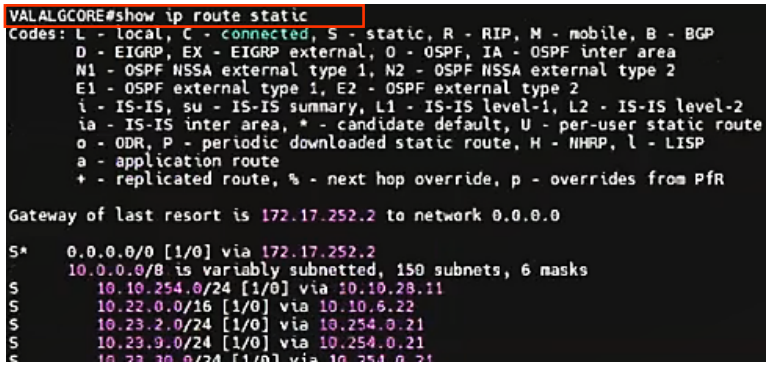


Figura 20. Descubrimiento de rutas estáticas en el tráfico de red.
Fuente: Pineda, Y. (2023)

Uno de los comandos utilizados de igual manera es **VALALGCORE#show running-config | include ip route**, esta variante del comando running-config muestra la configuración actual del router, switch o firewall. La configuración en ejecución es la configuración que está en la memoria del enrutador, actuando como una memoria. Por lo que, permite observar el tráfico de datos, la máscara de red y hacia dónde van dirigidos los datos.

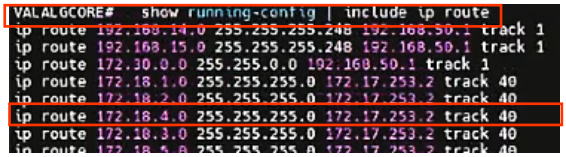


Figura 21. Configuración actual de rutas estáticas con show running-config.
Fuente: Pineda, Y. (2023)

De esta manera, es importante destacar el uso del Protocolo EIGRP (Enhanced Interior Gateway Routing Protocol), caracterizándose por ser un producto de CISCO para la detección

de vecinos relacionándose con routers conectados directamente y contribuyendo al transporte a través del protocolo RTP. Por lo que, para este tipo de casos en el descubrimiento de la topología de la red empresarial, resulta un protocolo importante y eficiente. Se puede apreciar con el comando **VALALGCORE#show ip route eigrp** en la **figura 22**.

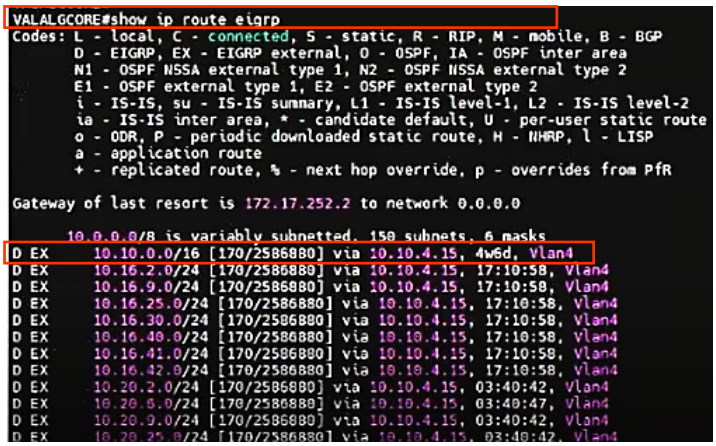


Figura 22. Descubrimiento de rutas inalámbricas aprendidas con protocolo EIGRP.
Fuente: Pineda, Y. (2023)

A través del comando, podemos apreciar una red que es aprendida a través de un salto, que es reconocida por una vlan o una interfaz, así mismo se aprecia la máscara de red en formato CIDR (Classless Inter-Domain Routing). De esta manera, a partir de los comandos mostrados anteriormente y datos proporcionados por el mismo equipo del Departamento de Telecomunicaciones se permite crear la tabla de los sitios principales remotos:

Tabla 4.
Tabla de elementos principales en la topología remota.

Nro	Elemento	IP WAN
1	GUASI_GRANJA_DON_MICHELLE_4003	10.254.0.5
2	ASDAC_ARAURE_4001	10.254.0.97
3	Router_Probalca	10.254.0.9
4	GUASI_ESMERALDA_4080	10.254.0.85
5	PROAV_MARACAIBO_4013	10.254.0.13
6	La_Tuchera	10.254.0.81
7	Router_Gterra	10.254.0.89
8	GUASI_SAN_FELIPE_4002	10.254.0.73
9	GUASI_TINAQUILLO_4010	10.254.0.53
10	Ro_MC	10.254.0.105
11	GUASI_BEJUMA_4099	10.254.0.61

12	GUASI_GRANJA_MONTAQA_ALTA_4102	10.254.0.57
13	GUASI_LOS_ROBLES_4009	10.254.0.65
14	Router_LANTA	172.17.253.14
15	Router_Forum	172.17.253.18

Fuente: Pineda, Y. (2023)

De esta manera, se crea el mapa topológico de la los sites remotos de la "Avícola La Guásima", se puede observar que consisten en diferentes granjas que se conectan a través de gateaways de routers así como cada uno tiene sub-divisiones que fueron descubiertos a través de los comandos de descubrimiento anteriormente. **(Ver Anexo 2)**

– **Actividad Nro. 2.** Levantamiento de inventario/recursos.

En la segunda actividad que se realiza paralelamente con la actividad anterior, se llenará un Excel de inventario/recursos que será distribuido en hostname, la ip del equipo, el serial (SN), modelo y versión de software o IOS.

Inicialmente, utilizando el comando apreciado en la **figura** 23: **VALALGCORE#show inventory**.

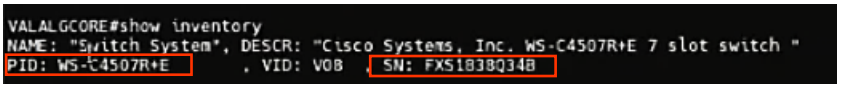


Figura 23. Descubrimiento de especificaciones de los equipos.
Fuente: Pineda, Y. (2023)

Permite ver una lista de equipos en una red con información detallada sobre las especificaciones del hardware, por lo que al aplicarse se muestra información como el PID siendo el nombre o modelo del equipo, históricamente llamado "Product Name", el VID es la versión del producto, y, por último, el SN es la serialización exclusiva del proovedor del producto, donde ayuda a identificar una instancia individual y específica. Por lo que, en este caso se resalta en la **figura 24** el PID y el SN. En el mismo orden de ideas, se utilizó un comando de la misma naturaleza que muestra, la información de una manera más resumida y directa; **VALALGCORE#show inventory | include SN:**

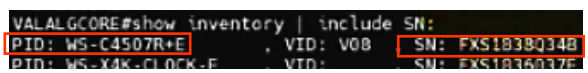


Figura 24. Descubrimiento de especificaciones de los equipos resumido.
Fuente: Pineda, Y. (2023)

Para el cometido de esta segunda actividad, igualmente se busca el software IOS del dispositivo, permitiendo observar su versión, su ROM y el tiempo que permanece encendido en la **figura 25** con el comando: **VALALGCORE#show version**

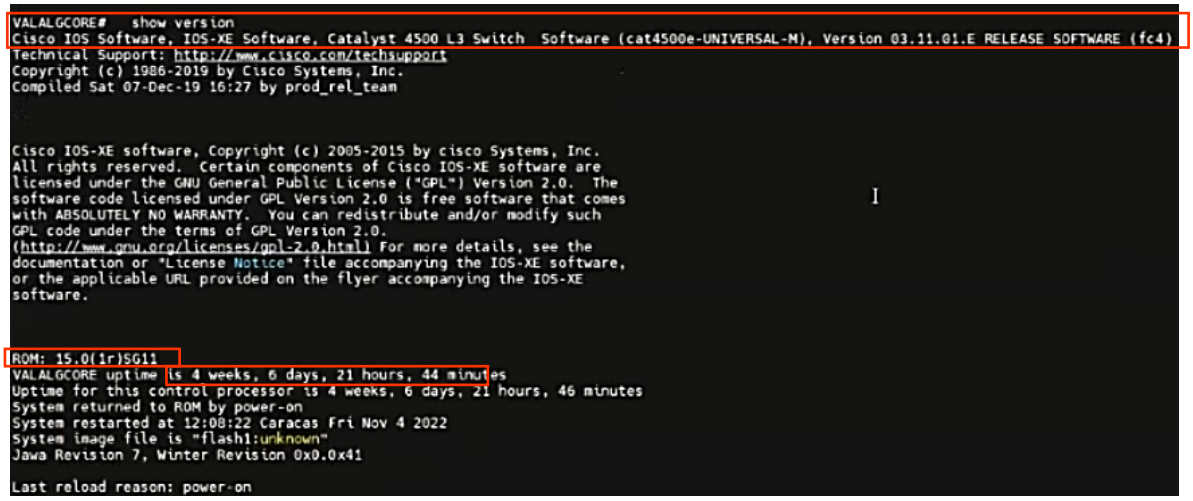


Figura 25. Descubrimiento del software IOS de los equipos.
Fuente: Pineda, Y. (2023)

Igualmente, como en el caso anterior, se utiliza el comando que muestra la información de una manera sencilla y resumida apreciado en la **figura 26: VALALGCORE#show inventory | include SN:**

Figura 26. Descubrimiento del software IOS de los equipos resumido.
Fuente: Pineda, Y. (2023)

Para el cometido de esta actividad, de igual forma se hizo uso de los protocolos **CDP, LLDP y EIGRP** mencionados en la anterior actividad, cuales permiten descubrir los dispositivos vecinos y poder añadir la información a la tabla de inventario mostrada a continuación en la **figura 27.**

Hostname	IP	Serial	Modelo	Version IOS
cucm1n	10.10.4.10		VMware	Linux 2.6.32-504.12.2.el6.x86_64
CUC1N	10.10.4.11		VMware	Linux 2.6.32-504.12.2.el6.x86_64
cup1n	10.10.4.12		VMware	Linux 2.6.32-504.12.2.el6.x86_64
Router_ALG	10.10.6.2	FLM250210WY	ISR4351/K9	X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.4a
VALALGCORE	172.17.14.1	FXS1838Q34B	WS-C4507R+E	(cat4500e-UNIVERSAL-M), Version 03.11.01.E
SW-DTPB01	172.17.14.2	JAE2427327F	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTPB03	172.17.14.3	JAE24260G4A	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SWDTPB-04	172.17.14.4	JAD242000NS	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.9.4
SW-DTPA01	172.17.14.5	JAE242731V3	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTPA02	172.17.14.6	JAE24201A5N	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTPA03	172.17.14.7	JAE242732FY	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a,
SW-DTPA04	172.17.14.8	JAE241508E4	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-GER01	172.17.14.9	JAE2427328S	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PAV01	172.17.14.10	FCQ1621X04H	WS-C2960-24PC-S	(C2960-LANLITEK9-M), Version 12.2(50)SE5
SW-DTSEG01	172.17.14.11	JAE242732HL	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTSEG02	172.17.14.12	JAE242732DY	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTSEGDVR	172.17.14.13	JAE24260H4K	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-DTSEG04	172.17.14.14	JAE242731QT	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PUERTA2	172.17.14.15	JAE24260FK6	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-ALM01	172.17.14.16	JAE242731RS	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-TAL01	172.17.14.17	JAE242732EZ	C9200L-24P-4G	Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.12.3a
SW-TRANSP01	172.17.14.18	JAE2427328Y	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-LAB01	172.17.14.19	JAE242732BT	C9200L-24P-4G	Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PSP01	172.17.14.20	JAE242732EN	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PBN01	172.17.14.21	JAE2427324A	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-OPE01	172.17.14.22	JAE2427324S	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a,
SW-DTPB05	172.17.14.23	JAE242731U4	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 17.3.3
SW-PBB01	172.17.14.24	JAE2427310C	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW_PAL	172.17.14.25	JAE242731WE	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-TallerIT	172.17.14.26	FOC1240Y48U	WS-C3560G-24TS	(C3560-IPBASEK9-M), Version 15.0(2)SE1
SW-Comedor	172.17.14.27	JAE24260VY2	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PLF01	172.17.14.28	JAE2425212U	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-TelfGER	172.17.14.29	FOC2035S2Y9	WS-C2960X-24PD-L	C2960X Software (C2960X-UNIVERSALK9-M), Version 15.2(7)E0a
SW-CCTV-PBN02	172.17.14.30	JAE242732GZ	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-PUERTA01	172.17.14.31	JAE242732K6	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a,
SW-CCTVPT001	172.17.4.3	FOC1136Z23J	WS-C2960G-24TC-L	(C2960-LANBASEK9-M), Version 15.0(2)SE1
Sistemas	172.17.0.25	KWC24190FN3	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Entrada_Gerencia	172.17.1.168	KWC24190FEG	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Nutritec	172.17.20.143	KWC24190FK8	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Edificio	172.17.41.5		PowerBeam M5 400	XW.v6.1.7-licensed.32555.180523.1625
Dormitorio SEG	172.17.41.6		PowerBeam M5 400	XW.v6.1.7-licensed.32555.180523.1625
Produccion_Avicola	172.17.41.12	KWC24190FG5	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Transporte	172.17.41.15	KWC24190FKG	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Data_Center	172.17.41.17	KWC24250FJU	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Contabilidad	172.17.41.18	KWC24250FLD	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Outdoor_Almacen	172.17.41.20	FGL2428L0U6	AIR-AP1562I-A-K9	ap3g3-k9w8 Version: 17.3.4.40
GT_Fabrica	172.17.17.21	KWC24250FLH	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Ventas	172.17.41.33	KWC24190FC5	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Pasillo_FZA	172.17.41.34	KWC24250FGW	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Sub_Producto	172.17.41.38	KWC24210YWP	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Servicio_Medico	172.17.41.39	KWC24250FLG	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Planta_BN	172.17.41.40	FGL2428L0U5	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Laboratorio	172.17.41.41	KWC24190FEN	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Outdoor_Detal	172.17.41.42	FGL2428L0UD	AIR-AP1562I-A-K9	Cisco AP Software, ap3g3-k9w8 Version: 17.3.4.40
AQ	172.17.41.46	KWC24190FCX	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Pasillo_FZA_2	172.17.41.47	KWC24190FLK	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Taller	172.17.41.48	KWC24190FG2	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Proyectos	172.17.41.49	KWC24190FFY	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Vigilancia2	172.17.41.50	KWC24190FJM	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Planta_Frio	172.17.41.51	KWC24190FKZ	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Gerencia_Hilhec	172.17.41.52	KWC24190FKS	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Legal	172.17.41.54	KWC24190FLW	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Planta_Beneficio	172.17.41.76	KWC24190FF3	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
PAL	172.17.41.201	KWC24250FLC	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Comedor	172.17.41.227	KWC24250FLE	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Almacen	172.17.41.232	KWC24190FJJ	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Gestion_Laboral	172.17.41.236	KWC24190FG7	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Operaciones	172.17.41.246	KWC24190FL9	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
Casa_Familia	172.17.41.250	KWC24190FDJ	C9117AXI-A	Cisco AP Software, ap1g6-k9w8 Version: 17.3.4.40
WLC_ALG	172.17.41.254	FCL2427001K	C9800-L-C-K9	(C9800_IOSXE-K9), Version 17.3.4c
Transporte-Datos	172.17.253.13	FJC24321LCG	ISR4221/K9	(X86_64_LINUX_IOSD-UNIVERSALK9_IAS-M), Version 16.4.2
SW-NT01	172.17.21.2	JAE24273101	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
Router-Nutritec	172.16.0.2	FJC24321K8K	ISR4221/K9	(X86_64_LINUX_IOSD-UNIVERSALK9_IAS-M), Version 16.4.2
SW_Nut_Datos	172.17.21.4	JAE24251GUU	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-NT02	172.17.21.3	JAE242731RB	C9200L-24P-4G	(CAT9K_LITE_IOSXE), Version 16.12.3a
SW-Ser01	172.17.16.99	CAT0831N2GF	WS-C3750-48TS	(C3750-IPSERVICESK9-M), Version 12.2(50)SE3
SW-GTDTA01	**172.17.16.98**		**WS-C3560G-24TS**	**(C3560-IPBASEK9-M), Version 15.0(2)SE1**

Figura 27. Tabla de las especificaciones y atributos de los dispositivos.

Fuente: Pineda, Y. (2023)

5.3 Fase III: Análisis de los requerimientos proporcionados por el cliente para su implementación en la red empresarial.

La tercera fase del presente trabajo de grado consiste en el análisis de los requerimientos mínimos para la implementación de la plataforma CISCO ISE, a través de nuestras actividades se desenvuelve esta fase.

Tabla 5.
Actividades: Fase 3.

Actividad	Descripción	Tareas	Responsables
1.Analizar los requerimientos que necesita CISCO ISE	En esta actividad se procede a analizar requerimientos para la implementación de CISCO ISE	Investigar y definir los requisitos que necesita la plataforma CISCO ISE	Autor de trabajo de grado Equipo de Setrys

Fuente: Pineda, Y. (2023)

- **Actividad Nro. 1.** Analizar los requerimientos que necesita CISCO ISE

Por lo que, para su implementación la guía de CISCO ISE presenta los diferentes requerimientos relevantes para el presente trabajo que se dividen en CPU, memoria, Hard Disks, y VMware Virtual Hardware.

Requirement Type	Specifications
CPU	• **Evaluation** • Clock speed: 2.0 GHz or faster • Number of CPU cores: 4 CPU cores • **Production** • Clock speed: 2.0 GHz or faster • Number of cores: • **SNS 3500 Series Appliance:** • Medium: 16 • Large: 16 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3500 series, due to hyperthreading. • **SNS 3600 Series Appliance:** • Small: 16 • Medium: 24 • Large: 24 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads.
Memory	• **Evaluation**: 16 GB • **Production** • Small: 32 GB for SNS 3615 • Medium: 64 GB for SNS 3595 and 96 GB for SNS 3655 • Large: 256 GB for SNS 3695
Hard Disks	• **Evaluation**: 300 GB • **Production** 300 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following link: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use more than one **virtual** disk to meet the disk space requirement, the installer may not recognize all the disk space.
VMware Virtual Hardware Version/Hypervisor	• VMware version 9 for ESXi 6.5 • VMware version 14 for ESXi 6.7 and later

Figura 28. Especificaciones de recursos para la implementación de CISCO ISE.
Fuente: Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021)

De esta manera, los requisitos mínimos para la instalación de Cisco ISE (en su versión "**SMALL**" y aplicable a "entornos productivos") en su versión 3.1 (se instala esta versión por temas de compatibilidad con el WLC) son los siguientes:

- **CPUs:** 16 virtual CPU a 2 GHz o superior.
- **Memoria RAM**: 32GB
- **Disco**: 300 GB

Recomendaciones de tamaño de dispositivo de máquina virtual para Cisco ISE

Para la instalación de CISCO ISE es muy importante que se dediquen únicamente los recursos de la máquina virtual y no compartirlos o usar los recursos a través de múltiples invitados de la máquina virtual. Es importante destacar que la mínima cantidad de espacio en el disco para cualquier producción del nodo de CISCO ISE es 300 GB, según la **figura 29**.

Cisco ISE Persona	Minimum Disk Space for Evaluation	Minimum Disk Space for Production	Recommended Disk Space for Production	Maximum Disk Space
Standalone Cisco ISE	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration only	300 GB	600 GB	600 GB	2.4 TB
Distributed Cisco ISE,Monitoring only	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE,Policy Service only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, pxGrid only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, Administration and Monitoring (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration, Monitoring, and Policy Service (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB

Figura 29. Recursos de espacio de almacenamiento para los nodos de CISCO ISE.
Fuente: Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021)

Permitiendo de esta manera, la aplicación de los nodos de Administración, Monitoreo y Políticas de servicio (sin pxGrid). De esta forma, se debe tomar en cuenta que la asignación de disco varía según requisitos de retención de registros, por lo que, si se posee el nodo de monitoreo, el 60% del espacio en el disco de la máquina virtual se asigna al almacenamiento, dependerá del número de endpoints aproximados que posea la red corporativa Avícola La Guásima. Por lo que se presentan una tabla del número de día que los registros (logs) de Radius y TACACSS+ pueden ser retenidos en base al espacio dedicado:

No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

Figura 30. Periodo de retención en días para RADIUS.
Fuente: Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021)

Así mismo, los logs de TACACS+ pueden ser registrados en el nodo de Monitoreo basado en el almacenamiento dedicado y número de endpoints en la red, suponiendo que se posee un script de 4 sesiones por día y 5 comandos por sesión.

No. of Endpoints	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516

Figura 31. Periodo de retención en días para TACACS.
Fuente: Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021)

Debido a que la implementación de la plataforma CISCO ISE se hará por medio de una máquina virtual VMware ESXi, se tendrán en cuenta igualmente sus requisitos mínimos y requisitos previos para su configuración. Principalmente, la versión de vSphere Client y VMware ESXi es 6.0 (apreciado en la **figura 32**).

Figura 32. Versión de vSphere Client y VMware ESXi.
Fuente: Pineda, Y. (2023)

Así mismo, esta máquina virtual será creado en un servidor **UCS C240 M3** (Unified Computing System) proveniente del fabricante "CISCO", es conocido como una arquitectura de centro de información de datos que integra computo, redes, acceso y almacenamiento. La interconexión de estructura es un conmutador de red (networking switch) o unidad principal (head unit) donde se conecta el chasis UCS, esencialmente un bastidor (su acrónimo en inglés más famoso conocido como rack) donde se conectan los componentes del servidor. Se puede

utilizar de forma independiente (standalone) o como parte del sistema informático unificado de Cisco. Tienen la habilidad de soportar sistemas operativos (OS) y posee aplicaciones en ambientes virtuales.

Figura 33. Servidor CISCO UCS C240 M3
Fuente: Pineda, Y. (2023)

Requisitos previos para configurar un servidor VMware ESXi

Según CISCO (2021), se debe revisar los siguientes requisitos previos de configuración enumerados en esta sección antes de intentar configurar un Servidor VMware ESXi:

- Recuerde iniciar sesión en el servidor ESXi como usuario con privilegios administrativos (usuario raíz).
- Cisco ISE es un sistema de 64 bits. Antes de instalar un sistema de 64 bits, asegúrese de que la tecnología de virtualización (VT) está habilitado en el servidor ESXi.
- Asegúrese de asignar la cantidad recomendada de espacio en disco en la máquina virtual de VMware.

5.4 Fase IV: Despliegue de los componentes, estructura lógicas y funcionales de la capa de seguridad.

La cuarta fase del presente trabajo de grado consiste en el procedimiento para la implementación de CISCO ISE en la red empresarial de “Avícola La Guásima”, la presente

fase tendrá diez (10) actividades que se dividirán en la creación y configuración de la máquina virtual, instalación y configuración de CISCO ISE, así como la creación de plantillas para la creación y configuración de los servidores de RADIUS y TACACS+.

Tabla 6.
Actividades. Fase 4.

Actividad	Descripción	Tareas	Responsables
1. Descargar archivo .ISO para la creación de la máquina virtual	En esta actividad se procede a obtener el archivo .ISO por donde se instalará CISCO ISE.	Buscar, descargar y guardar archivo .ISO para su instalación	Autor de trabajo de grado Equipo de Setrys
2. Creación de la Máquina Virtual (VM) a través de un ESXi Server	En esta actividad se procede a crear la máquina virtual (VM).	Subir archivo .ISO, crear la VM y configurar la VM	Autor de trabajo de grado Equipo de Setrys
3. Instalación de la plataforma CISCO ISE por consola	En esta actividad se instalará a través de la consola CISCO ISE.	Instalar CISCO ISE en la VM, configurar el setup, verificación del application server	Autor de trabajo de grado Equipo de Setrys
4. Ingresar al portal web de la plataforma CISCO ISE	Se ingresará al portal web de la plataforma CISCO ISE.	Ingresar con la IP asignada con las credenciales admin	Autor de trabajo de grado Equipo de Setrys
5.Configuraciones iniciales de los nodos, administración de dispositivos, certificados, de seguridad y RADIUS de la plataforma CISCO ISE.	Configuración de la sección "administration" del dashboard de CISCO ISE.	Configurar los deployments nodes, los certificados, opciones de seguridad y RADIUS.	Autor de trabajo de grado Equipo de Setrys

6. Configuración del acceso de usuario "onlyview" y grupos de identidad para lectura.	Crear y configurar un perfil para únicamente lectura llamado onlyview.	Crear usuario en network Access users, crear un grupo "onlyview" y políticas RBAC.	Autor de trabajo de grado Equipo de Setrys
7. Integración usuarios y grupos del Active Directory a la plataforma CISCO ISE.	Integrar los usuarios y grupos del Active Directory a la plataforma.	Añadir usuarios y grupos del Active Directory a la plataforma CISCO ISE.	Autor de trabajo de grado Equipo de Setrys
8. Creación de políticas para administración de la autenticación y autorización de la plataforma CISCO ISE.	Se crearán políticas para la autenticación y autorización de usuarios y dispositivos de la plataforma.	Crear y configurar políticas de administración de la autenticación y autorización.	Autor de trabajo de grado Equipo de Setrys
9. Añadir dispositivos de la red corporativa a la plataforma CISCO ISE	Se añadirán los dispositivos a la pestaña "Network Devices" en la plataforma CISCO ISE.	Realizar archivo .CVS, importar archivo a la plataforma, añadir y configurar los dispositivos.	Autor de trabajo de grado Equipo de Setrys
10. Configuración de todos los dispositivos a través de plantillas de RADIUS y TACAS.	Se configurarán los dispositivos a través de las plantillas creadas de RADIUS y TACACS.	Crear y configurar las plantillas RADIUS y TACACS Instructiva de configuración para autenticación RADIUS	Autor de trabajo de grado Equipo de Setrys

Fuente: Pineda, Y. (2023)

– **Actividad Nro. 1.** Descargar archivo .ISO para la creación de la máquina virtual.

Para la intención de esta actividad, en la guía de **Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021)** permite observar diferentes métodos de instalación, pudiendo ser por plantillas .OVA o .ISO. Eligiéndose de esta manera, el método de instalación por .ISO.

De esta manera, se procede a descargar el archivo .ISO desde la página oficial de CISCO con las credenciales del cliente, apreciado en la **figura 34**:

Figura 34. Selección del producto CISCO Identity Services Egine Software (ISE)
Fuente: Pineda, Y. (2023)

Por lo que, se dirige a la versión escogida para CISCO ISE "SMALL" versión 3.1, apreciado en la **figura 35**:

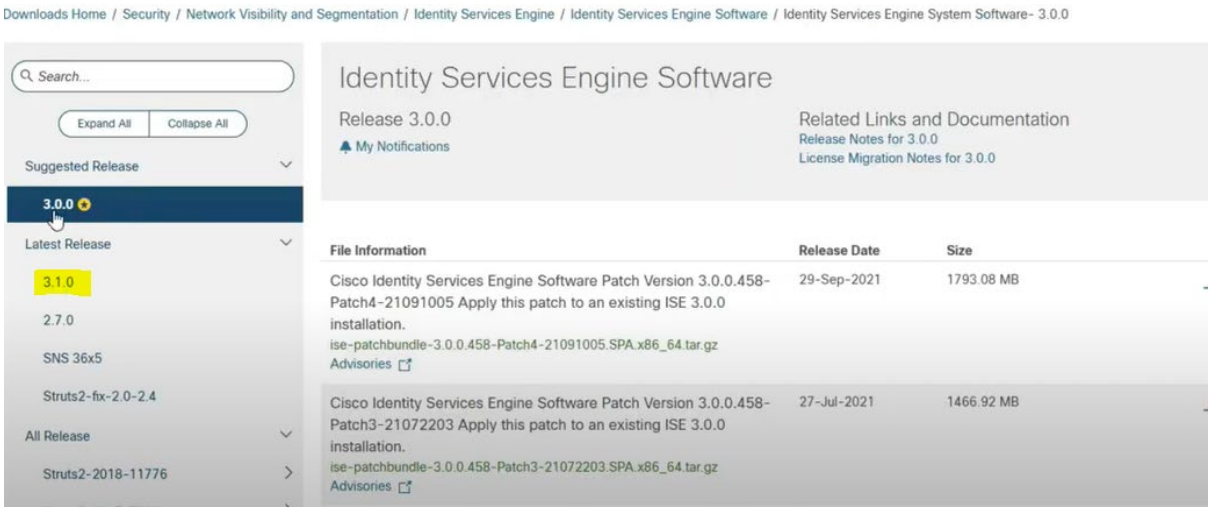


Figura 35. Descarga del producto CISCO Identity Services Egine Software (ISE)
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 2.** Creación de la Máquina Virtual (VM) a través de un ESXi Server

Una vez, ya obtenido nuestro archivo necesario para la instalación, es necesario configurar el servidor de VMware, permitiendo de esta manera crear la máquina virtual

destinada para la instalación de CISCO ISE. Inicialmente, se procede a acceder al ESXi server y en el panel izquierdo. Es importante, de esta manera añadir el archivo .ISO al almacenamiento del host antes de proceder a la creación de la máquina virtual a través de la opción **Configuration>Storage>Browse Datastore>Upload File.**

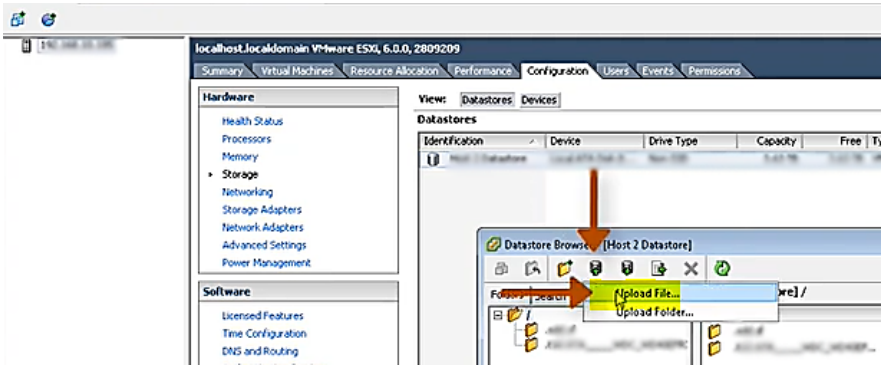


Figura 36. Subida del archivo .ISO al almacenamiento del host.
Fuente: Pineda, Y. (2023)

De esta manera, se procede a realizar click derecho al host y se selecciona la opción **New Virtual Machine**. En la configuración del diálogo, se escoge la opción **Custom** según la guía de instalación, para la configuración del VMware, apreciado en las **figura**s:

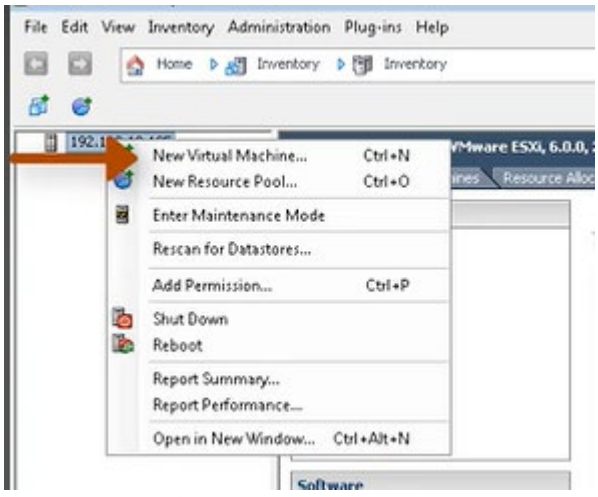


Figura 37. Creación de la Máquina Virtual (VM) a través de un ESXI Server
Fuente: Pineda, Y. (2023)

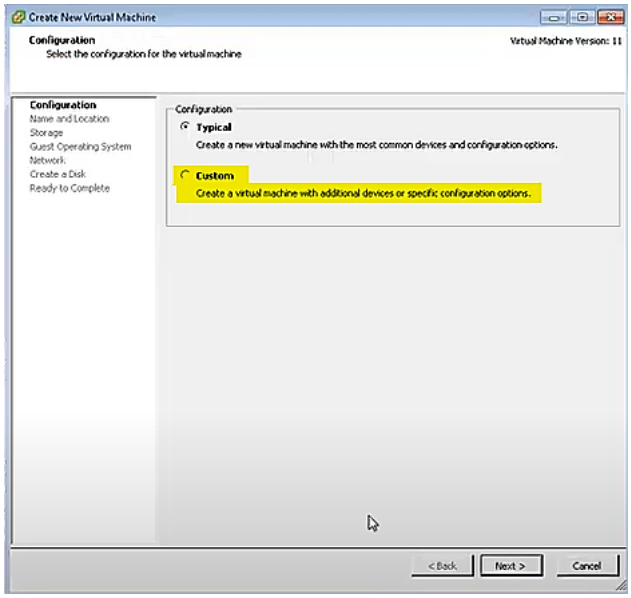


Figura 38. Selección de la opción "custom" en la creación de la VM.
Fuente: Pineda, Y. (2023)

Al hacer click en **Next**, se le asignará un nombre al sitema de VMware y su locación con tiempo universal UTC. Luego, se escoge el datastore con la cantidad disponible de almacenamiento, e igualmente se procede a escoger Linux e igualmente la opción "Red Hat Enterprise Linux" en la lista de versiones. Al hacer click en **Next**, se escoge un número virtual de sockets y número de núcleos por virtual sockets (en su aplicación "SMALL" son 16).

Siguiendo con el procedimiento, se escoge la cantidad de memoria de almacenamiento, se escoge el NIC driver con el adaptador, de esta manera, se procede a ver las propiedades de la máquina virtual, resaltando la opción **New CD/DVD (adding)**, donde se utilizará el archivo .ISO anteriormente añadido al almacenamiento.

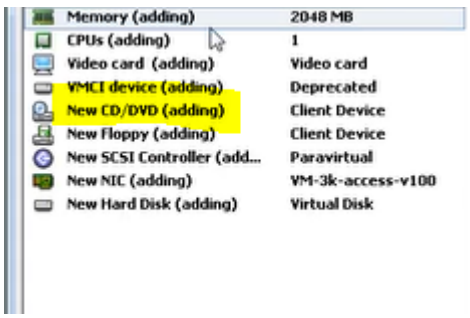


Figura 39. Selección de la opción "custom" en la creación de la VM.
Fuente: Pineda, Y. (2023)

Al hacer click en la opción, se procede importar el archivo .ISO en la máquina virtual, apreciado en la **figura 40.**

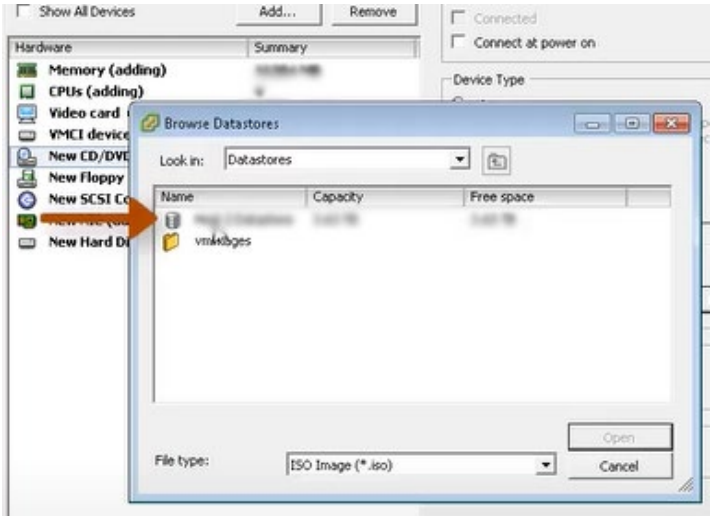


Figura 40. Añadir .ISO image para la instalación de CISCO ISE.
Fuente: Pineda, Y. (2023)

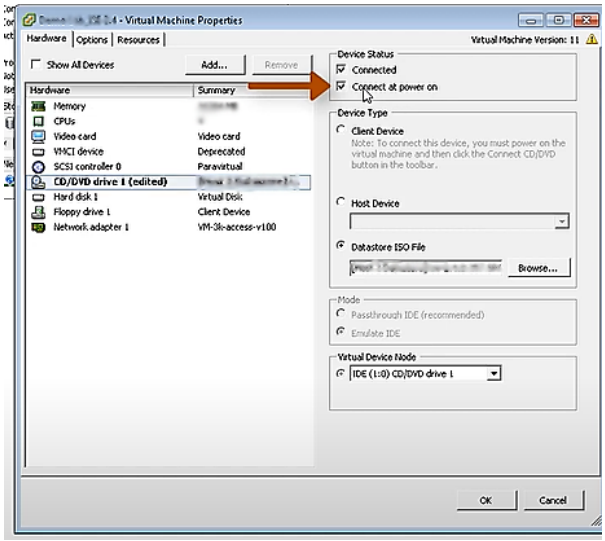


Figura 41. Selección de casilla "connect at power on".
Fuente: Pineda, Y. (2023)

Al añadirlo, es importante, de esta manera seleccionar la casilla **Connect at power on**, Una vez todos los datos colocados, se procede a seleccionar en **Resources**, donde se configura datos como el **CPU, Memory, y Disk.** Luego se selecciona la opción **Finish.** Al crearse la máquina virtual, se realiza click derecho y se procede a seleccionar **Open console.** Al seleccionar esta opción, se aprecia la ventana para iniciar la máquina virtual y la consola muestra en pantalla las opciones para la instalación de CISCO ISE.

- **Actividad Nro. 3.** Instalación de la plataforma CISCO ISE por consola

La instalación de CISCO ISE se realiza a través de un menú donde se despliegan diferentes opciones (4 opciones en total), donde se indicará un número del menú disponible.

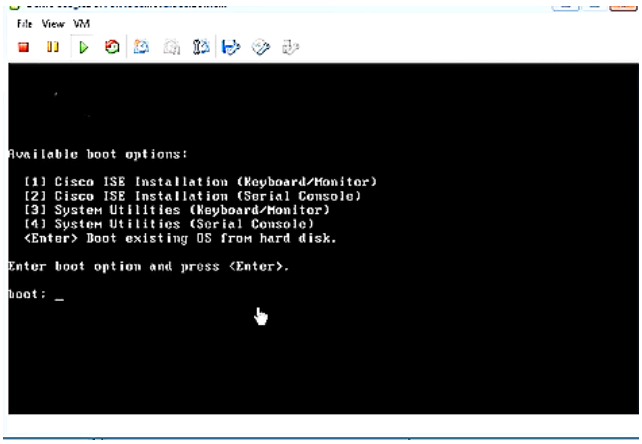


Figura 42. Menú de instalación de CISCO ISE.
Fuente: Pineda, Y. (2023)

Escogiendo de esta manera, la opción **(1) CISCO ISE Installation (Keyboard/Monitor),** escribiendo el número por teclado y presionando **Enter**, permitiendo así su instalación en la máquina virtual. Al finalizar su instalación, la máquina virtual procede a reiniciarse automáticamente y mostrar por consola la configuración de la instancia, escribiendo **"setup"** y presionando **Enter.**

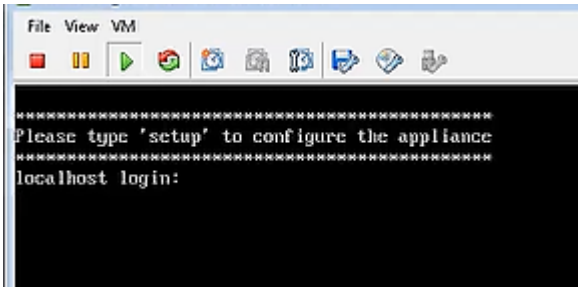


Figura 43. Setup para configurar CISCO ISE.
Fuente: Pineda, Y. (2023)

Apareciendo por consola, el setup, guiando el proceso incial de la configuración del CISCO ISE, añadiendo información como **hostname, IP address, IP netmask, IP deafult dateaway, DNS domain, primary nameserver, timezone, username y password.** A continuación, según la guía de instalación de CISCO ISE (2021), muestra una lista completa de los parámetros pedidos y sus condiciones:

Table 10: Cisco ISE Setup Program Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical (A–Z, a–z, 0–9), and the hyphen (-). The first character must be a letter. **Note** We recommend that you use lowercase letters to ensure that certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verifications. You cannot use "localhost" as hostname for a node.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 or Global IPv6 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14/ 2001:420:54ff:4::458:121:119
Netmask	Must be a valid IPv4or IPv6 netmask.	255.255.255.0/ 2001:420:54ff:4::458:121:119/122
Default gateway	Must be a valid IPv4or Global IPv6 address for the default gateway.	10.12.13.1/ 2001:420:54ff:4::458:1
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	example.com
Primary name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	10.15.20.25 / 2001:420:54ff:4::458:118
Add/Edit another name server	Must be a valid IPv4 or Global IPv6 address for the primary name server.	(Optional) Allows you to configure multiple name servers. To do so, enter y to continue.
Primary NTP server	Must be a valid IPv4 or Global IPv6 address or hostname of a Network Time Protocol (NTP) server. **Note** Ensure that the primary NTP server is reachable.	**clock.nist.gov** / 10.15.20.25 / 2001:420:54ff:4::458:117
Add/Edit another NTP server	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.
System Time Zone	Must be a valid time zone. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT (or Coordinated Universal Time (UTC) minus 8 hours). **Note** Ensure that the system time and time zone match with the CIMC or Hypervisor Host OS time and time zone. System performance might be	UTC (default)
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The username must be three to eight characters in length and comprise of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password in order to continue because there is no default password. The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Figura 44. Atributos para la configuración de "setup".
Fuente: Pineda, Y. (2023)

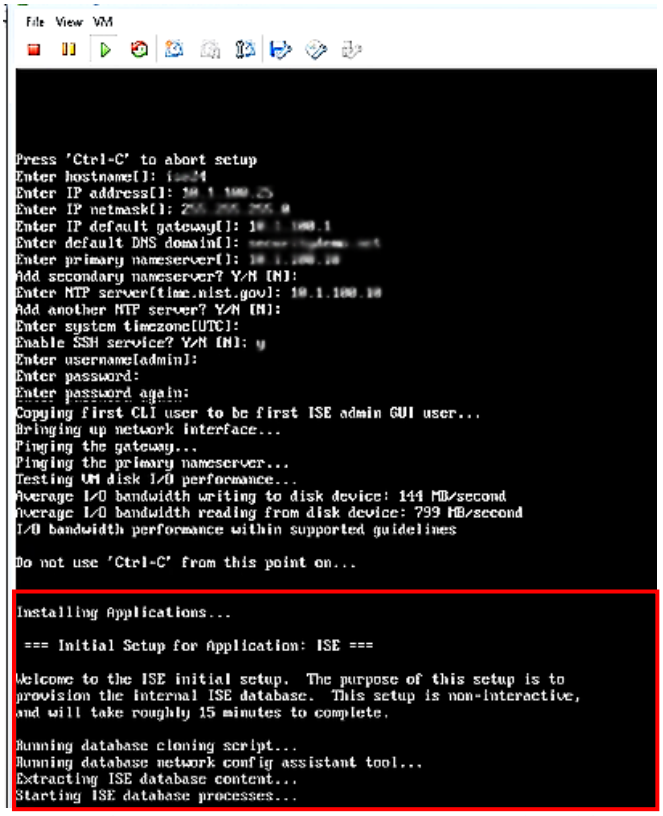


Figura 45. Iniciación de la aplicación CISCO ISE por consola.
Fuente: Pineda, Y. (2023)

De esta forma, luego que el proceso de instalación y la configuración de la plataforma CISCO ISE sea completado, se reinicia la VM y se procede a introducir el usuario y la contraseña, para introducir el comando **admin# show application status ise,** permitiendo observar todos los procesos y los estados que conforman la plataforma conjunto a su ID, apreciado en la **figura 46**.

```
valalgise01/admin#show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          8475
Database Server                        running          124 PROCESSES
Application Server                     running          31189
Profiler Database                      running          16392
ISE Indexing Engine                    running          32237
AD Connector                           running          33399
M&T Session Database                   running          27620
M&T Log Processor                      running          31454
Certificate Authority Service          running          33256
EST Service                            running          65470
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  disabled
PassiveID Syslog Service               disabled
PassiveID API Service                  disabled
PassiveID Agent Service                disabled
PassiveID Endpoint Service             disabled
PassiveID SPAN Service                 disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          11481
ISE API Gateway Database Service       running          15225
ISE API Gateway Service                running          26278
ISE pxGrid Direct Service              running          50468
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
```

Figura 46. Comando show application status ise.
Fuente: Pineda, Y. (2023)

Es importante de esta manera, resaltar la importancia el estado del proceso llamado "**Application Server**", existiendo tres posibles estados**, not running, initializing** y **running**, por lo que, si no se encuentra activo no se podrá ver la consola web de la plataforma CISCO ISE.

- **Actividad Nro. 4.** Ingresar al portal web de la plataforma CISCO ISE

La cuarta actividad de esta fase, se basa en el ingreso del portal de la plataforma a través de un navegador, como lo indica la **figura 47**, se dispone de un usuario y unas credenciales para acceder a la plataforma.

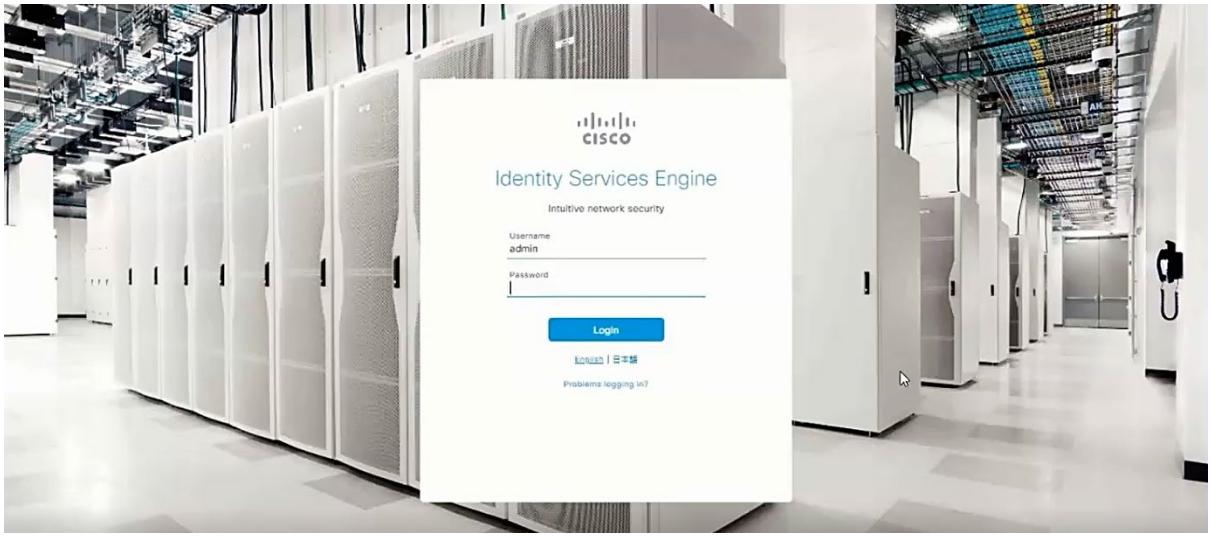


Figura 47. Ingreso al portal de la Plataforma CISCO ISE.
Fuente: Pineda, Y. (2023)

Por lo que, con la IP de ingreso asignada como **10.10.2.83** se puede acceder a través de navegador, como muestra la **figura 48**.

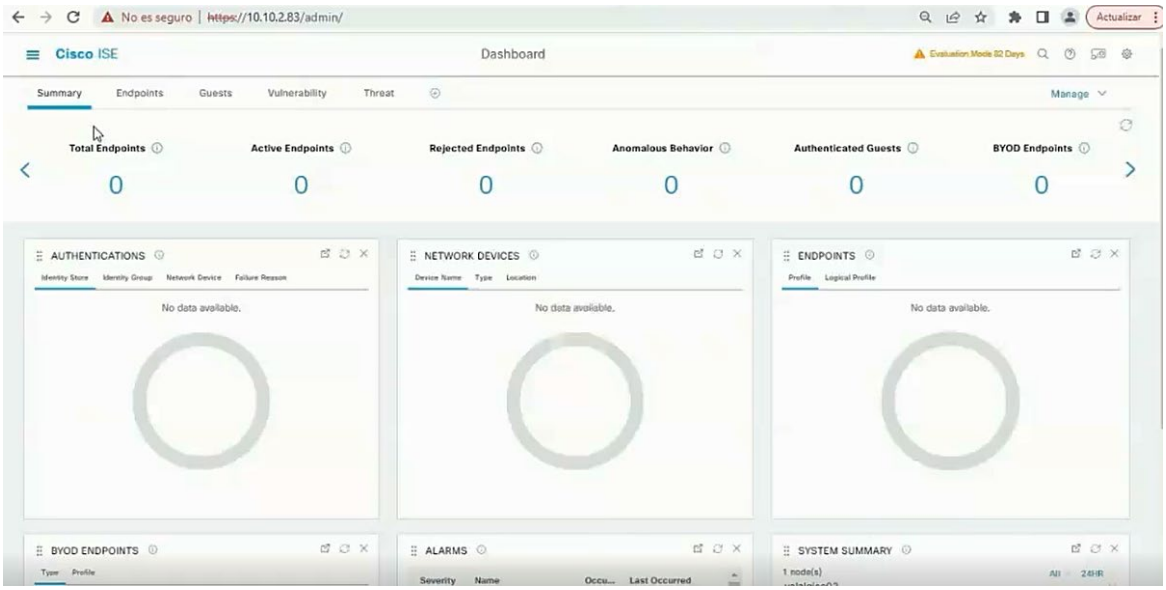


Figura 48. Plataforma CISCO ISE.
Fuente: Pineda, Y. (2023)

A continuación, se puede ver la plataforma de CISCO ISE con sus diferentes pestañas como **Summary, Endpoints, Guests, Vulnerability, y Threat,** presentando de esta manera las estadísticas que recopilará a lo largo de su uso. A través de las **Authentications**, se podrán ver los usuarios que estarán autenticados en dispositivos y sesiones, en el apartado del **Network Devices** nos permite ver los diferentes dispositivos conectados a la red empresarial, así mismo los **Endpoints** permiten ver la cantidad de dispositivos finales, conocidos como dispositivos informáticos remotos.

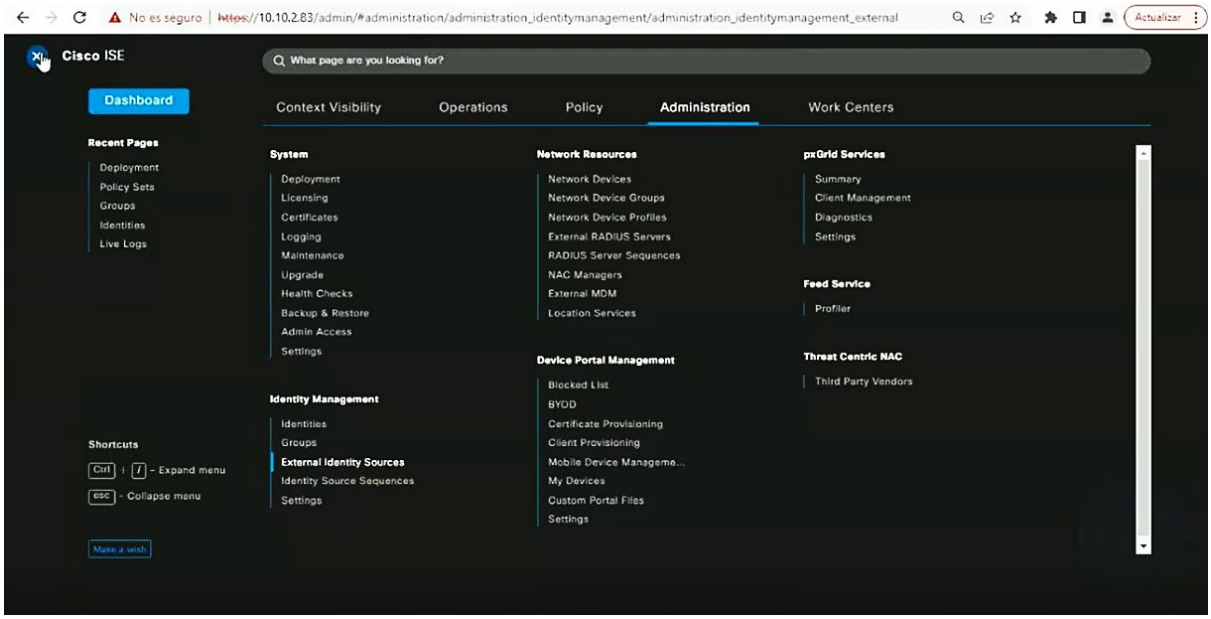


Figura 49. Dashboard de la Plataforma CISCO ISE.
Fuente: Pineda, Y. (2023)

Así mismo, en el panel izquierdo, al seleccionar las tres líneas, nos permite apreciar el **Dashboard** de la plataforma CISCO ISE, donde se divide en diferentes secciones como **Context Visibility, Operations, Policy, Administration y Work Centers**. La pestaña de administración es una sección importante debido que la mayoría de las configuraciones se harán por este medio, esta sección tiene sub-categorías que se presentan como **System** que contiene toda la información del sistema como son la integración, licencias, certificados, mantenimiento y su configuración. Luego, **Identity Management** donde se ubican todas las identificaciones y credenciales de los usuarios, así como los grupos, e igualmente el AD (Active Directory), **Network Resources** es donde se ubica la identificación de los dispositivos y los grupos de dispositivos, así como servidores externos de RADIUS**, Device Portal Management** donde se ubica el BYOD y certificados**.**

Así mismo, se puede apreciar los detalles de la plataforma CISCO ISE y su servidor, el host o nodo, cual es llamado **valalgise02**, con las personas de administración, monitoreo y servicios de políticas en el mismo nodo, al mismo tiempo, se aprecia la versión elegida del CISCO ISE 3.1.0.518 así como la información del parche es 1,3,4,5.

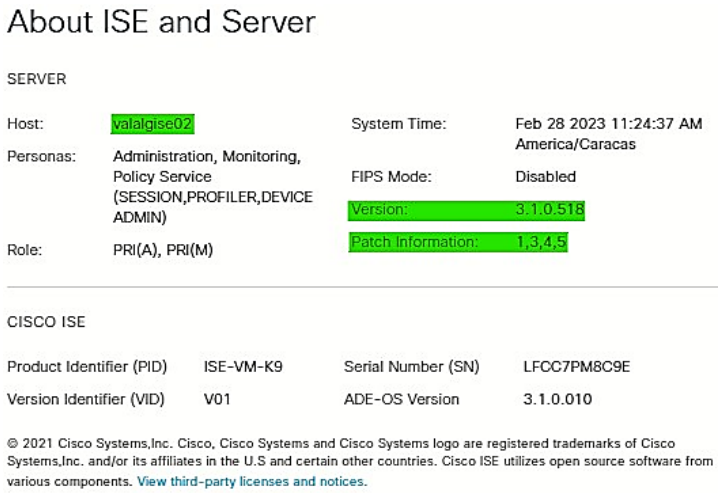


Figura 50. Acerca de CISCO ISE y el servidor.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 5.** Configuraciones iniciales de los nodos, administración de dispositivos, certificados, de seguridad y RADIUS de la plataforma CISCO ISE

Inicialmente, al dirigirnos en el **Dashboard**>**Administration**>**Systems**, seleccionamos **Deployment**.

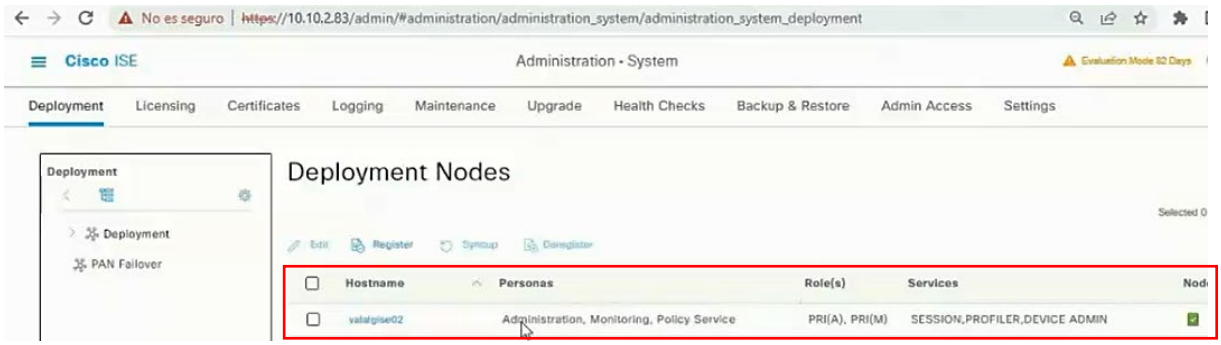


Figura 51. Deployment Nodes.
Fuente: Pineda, Y. (2023)

Se aprecia el único nodo activo, llamado **valalgise02**, cuenta con tres personas activas, **Administration, Monitoring y Policy Service**, se despliegan las diferentes configuraciones para cada persona, por lo que se activa la pestaña "**Enable Device Admin Service**" en la sección de **Policy Service** para poder trabajar con los servicios de administración de dispositivos.

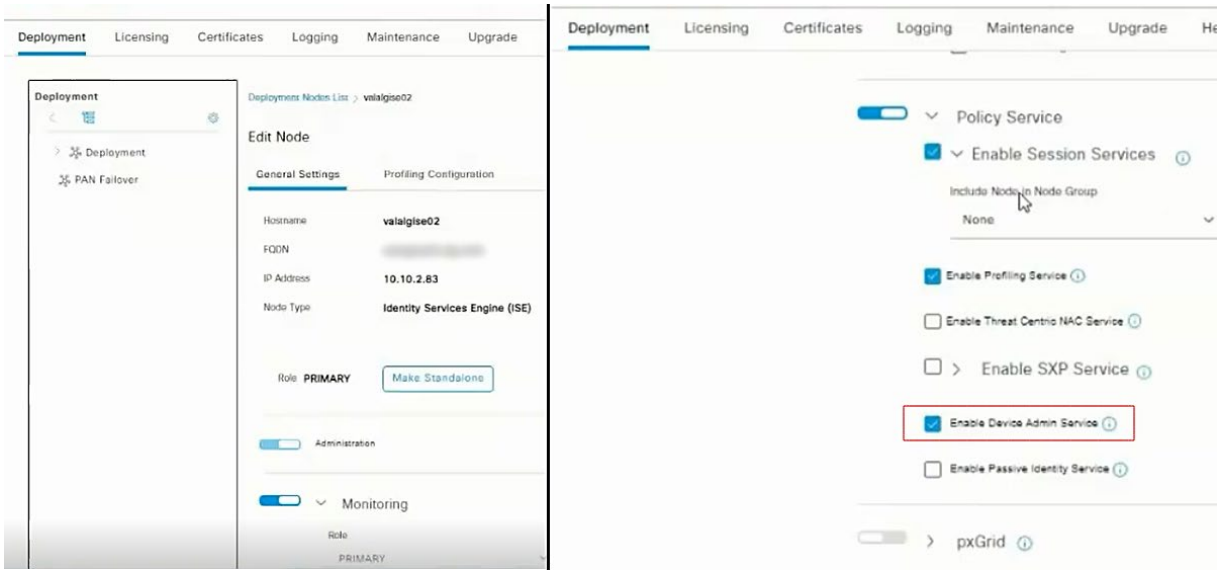


Figura 52. Configuración del nodo valalgise02.
Fuente: Pineda, Y. (2023)

Luego, se procede a ir a la pestaña de **Certificates**, y extender la fecha de vencimiento del certificado del sistema, siendo válido desde el 9 de enero de 2023 hasta el 6 de enero de 2038.

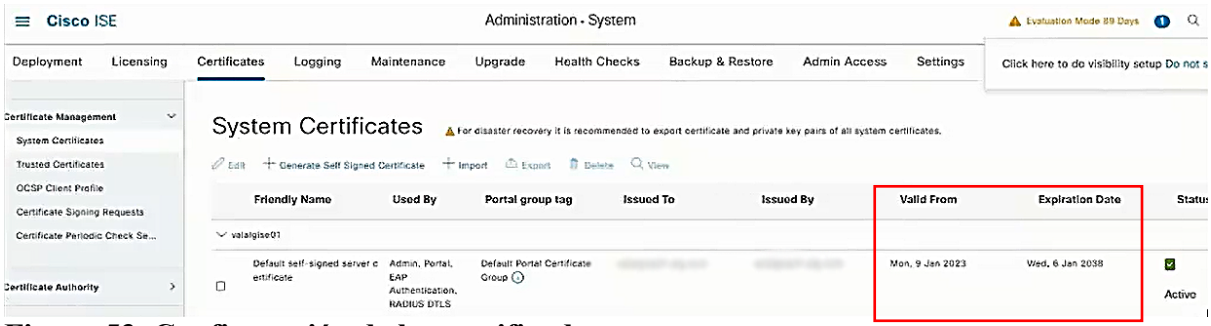


Figura 53. Configuración de los certificados.
Fuente: Pineda, Y. (2023)

A continuación, se selecciona **Admin Access>Security Settings** y se seleccionan las siguientes casillas como Allow TLS 1.0, TLS 1.2, SHA1 ciphers, ECDHE-RSA, 3DES ciphers, certificados sin validación, DSS cipers para ISE como cliente, y se guardan los cambios.

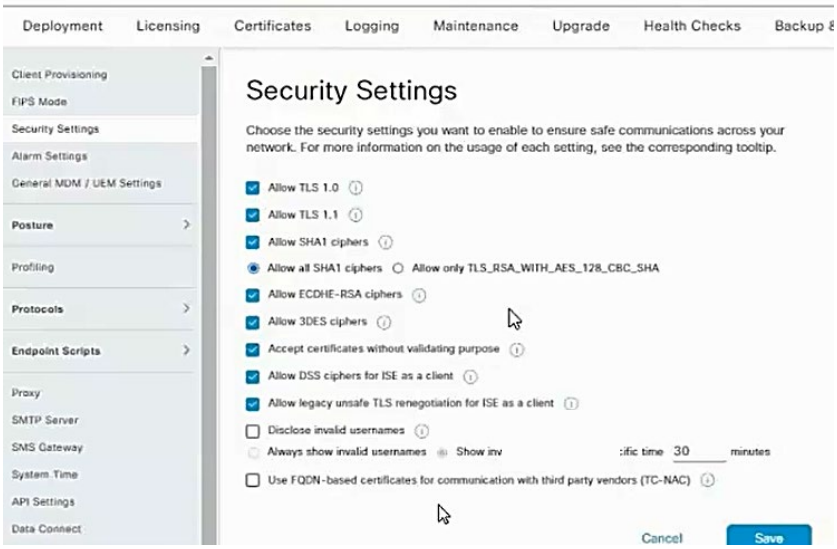


Figura 54. Configuración de las opciones de seguridad.
Fuente: Pineda, Y. (2023)

Así mismo, nos dirigimos a **Admin Access>Protocols>RADIUS,** configuramos las siguientes opciones, se desactiva "**Suppress repeated failed clients",** así mismo como "**Suppress repreated successfull clients"** debido a que estas opciones no permiten que los eventos repetidos con los clientes aparezcan en los logs para no sobrecargarlos, sin embargo, a preferencia del cliente se desactivaron para que estén presente en los registros.

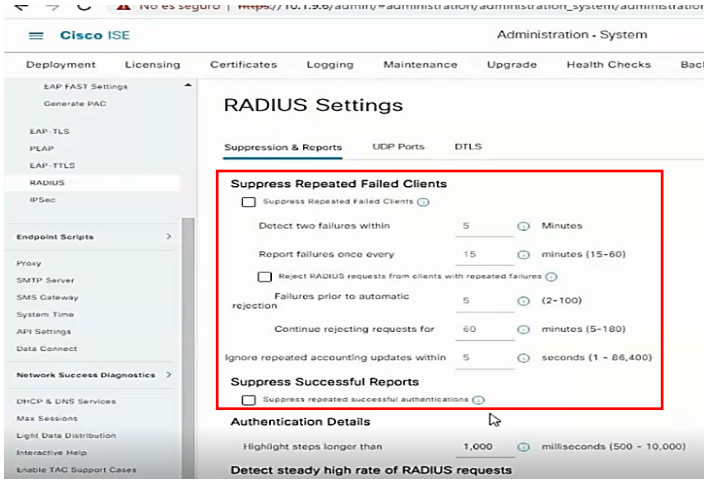


Figura 55. Configuración de RADIUS.
Fuente: Pineda, Y. (2023)

- **Actividad Nro. 6.** Configuración del acceso de usuario "onlyview" y grupos de identidad para lectura.

Para continuar la configuración principal del CISCO ISE, nos dirigimos a **Administration>Identity Management>Identities>Users**, a petición del cliente, se creó un usuario específicamente para lectura, llamado **onlyviewdevint,** apreciado en la **figura 56**.

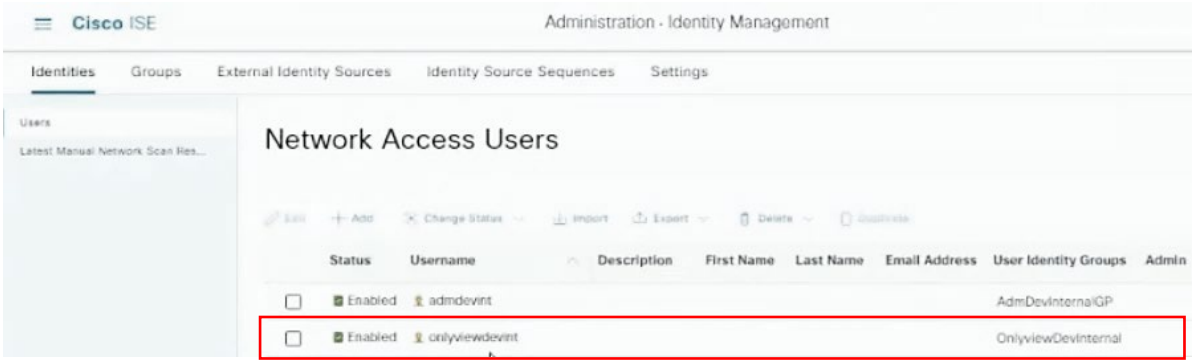


Figura 56. Network Access Users.
Fuente: Pineda, Y. (2023)

Así mismo, se creó un grupo para incluir el usuario **onlyviewdevint**, seleccionando **Administration>Identity Management>Groups**, creándolo en la pestalla "+ Add", así mismo llamándolo "OnlyviewDeInternal", la intención de su creación recae en trabajadores de la Avícola La Guásima de nivel 1 que únicamente tenga opciones de lectura en la plataforma.

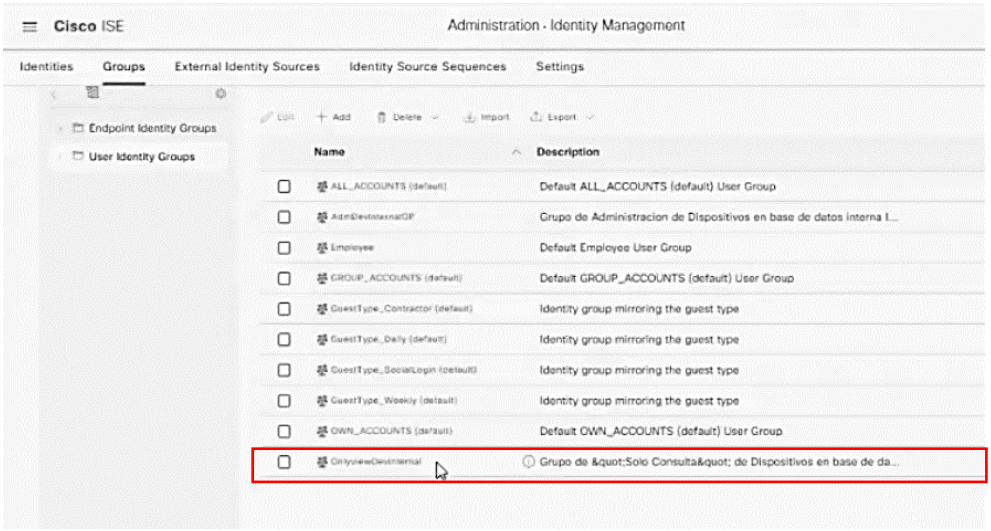


Figura 57. Configuración "user identity groups".
Fuente: Pineda, Y. (2023)

De esta manera, se puede apreciar en la **figura 58**, que se crea un **RBAC** (Role-based Access control) para lectura llamado **"OnlyView_1rst_Level"**, esta política se utiliza para controlar el acceso basado en roles, asignándole derechos a usuarios de la organización para la función que desempeñan en la empresa, en este caso, únicamente lectura.

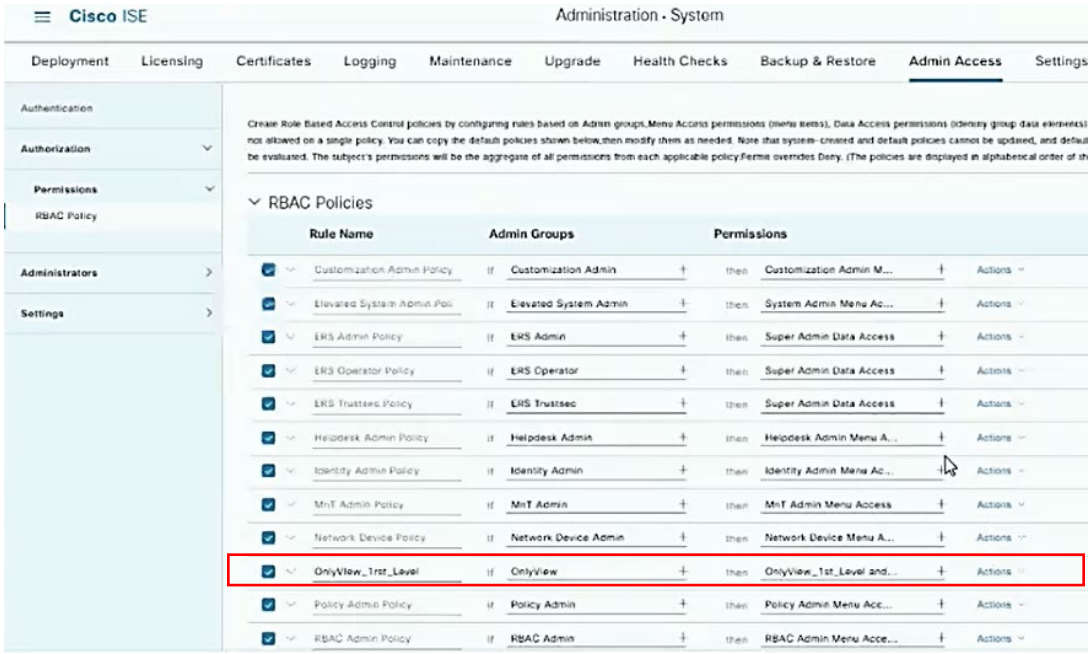


Figura 58. Configuración RBAC Policies.
Fuente: Pineda, Y. (2023)

Así mismo, a través de la configuración del RBAC se selecciona "**Actions**", se pueden mostrar y ocultar secciones del **Dashboard**, en este caso únicamente para lectura, a continuación, se muestra en la **figura 59**, cómo se muestran u ocultan las categorías o subcategorías a usuarios y grupos.

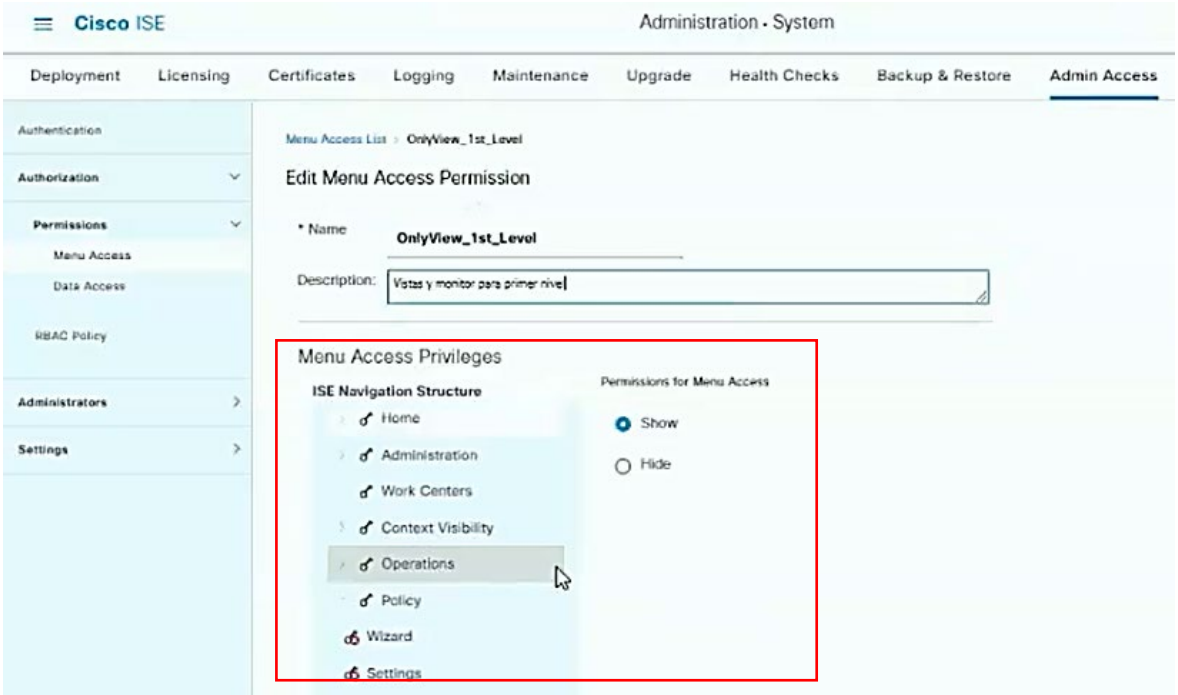


Figura 59. Editar los permisos de acceso del menú o dashboard.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 7.** Integración usuarios y grupos del Active Directory a la plataforma CISCO ISE.

En otro orden de ideas, se procede a dirigirse a **Administration>Identity Management>External Identity Sources** donde se integra el Active Directory llamado AD_ALG con la plataforma de CISCO ISE a través de la opción **"+ Join",** al integrarse muestra el resumen del estado cual fue exitoso y completado, así mismo ya en el nodo principal muestra que el estado del AD es operacional**,** apreciado en la **figura 60**.

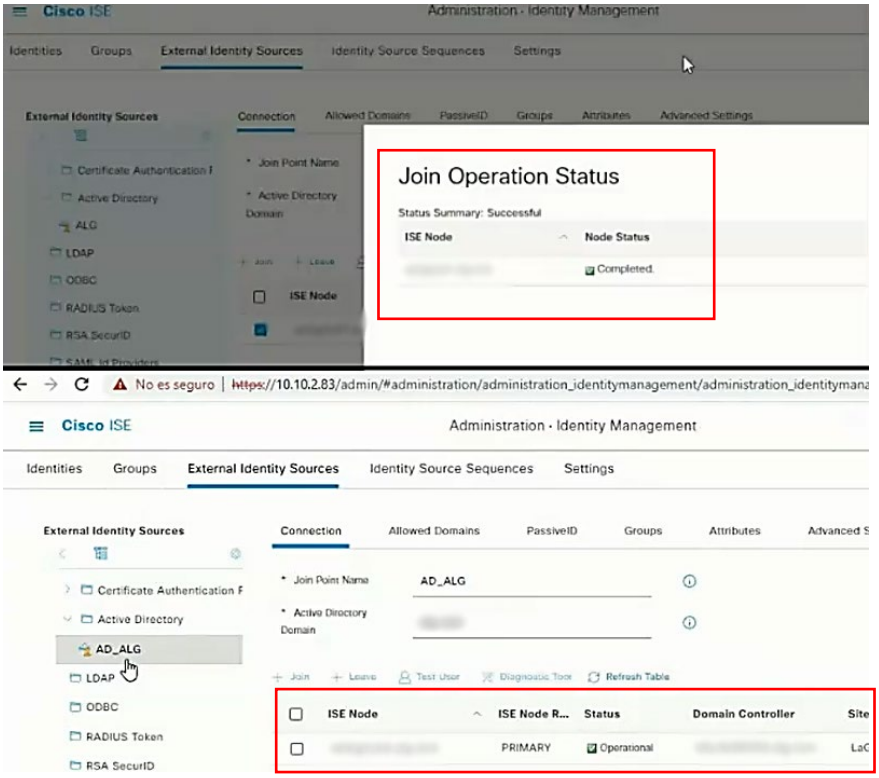


Figura 60. Integración del AD con External Identity Sources.
Fuente: Pineda, Y. (2023)

Igualmente, en la pestaña de "**Groups**" la misma sección, se pueden observar todos los grupos del **Active Directory** de Avícola La Guásima, cuales se seleccionaron tres grupos únicamente con la intención de utilizarlos para las pruebas piloto que se desarrollarán, cuales son administradores, usuarios y usuarios del dominio.

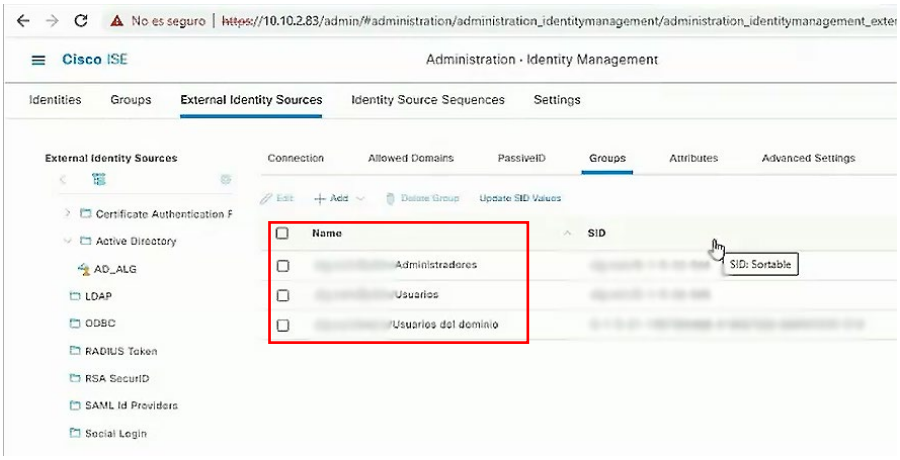


Figura 61. Grupos importados en External Identity Sources.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 8.** Creación de políticas para administración de la autenticación y autorización de la plataforma CISCO ISE.

Para el cometido de esta actividad, se procede a crear las políticas de acceso a la red corporativa, por lo que se dirige hacia el **Dashboard** y se escoge **Policy>Policy Sets,** se aprecia de esta forma los sitios que se pueden administrar, en este caso únicamente se administrará el sitio de "**ALG_Venezuela**", apreciado en la **figura 62**.

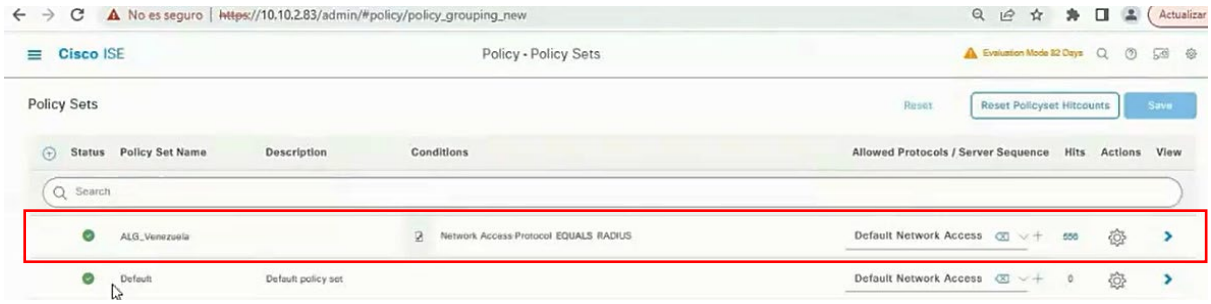


Figura 62. Creación de políticas para el sitio ALG_Venezuela.
Fuente: Pineda, Y. (2023)

De esta forma, al seleccionar el sitio, saldrán diferentes configuraciones como "**Autenthication Policy**" que configura las autenticaciones para los dispositivos, así mismo como "**Autorization Policy**" que permitirá la autorización de privilegios para los distintos roles.

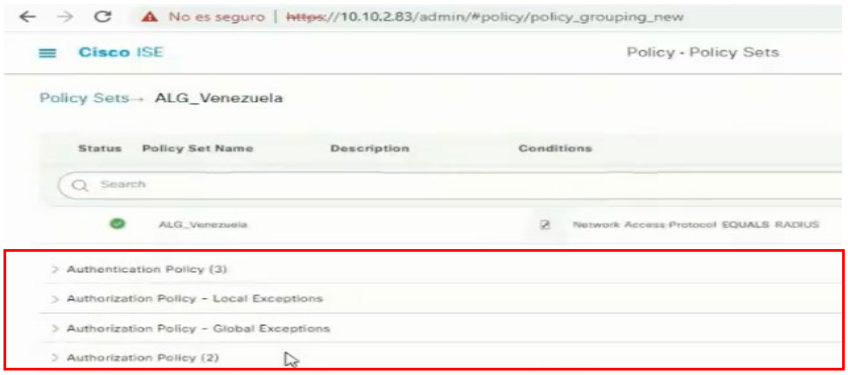


Figura 63. Políticas de autenticación y autorización en Policy Sets.
Fuente: Pineda, Y. (2023)

Para el apartado de autenticación, se deciden utilizar dos medios de autenticación, que serán cableado llamado "**Wired_802.1X"** y por red inalámbrica llamado "**Wireless_802.1X",** así mismo como una tercera opción llamada "**Default"** que no tendrá privilegios en caso de que no cumpla ninguna de las dos opciones anteriores. Las autenticaciones de los usuarios se realizan a partir de la base de datos de credenciales integrado en CISCO ISE, por lo que cualquier usuario que, incluido en el mismo, que desee ingresar a la red empresarial tendrá que ser autenticado a través de estos dos medios.

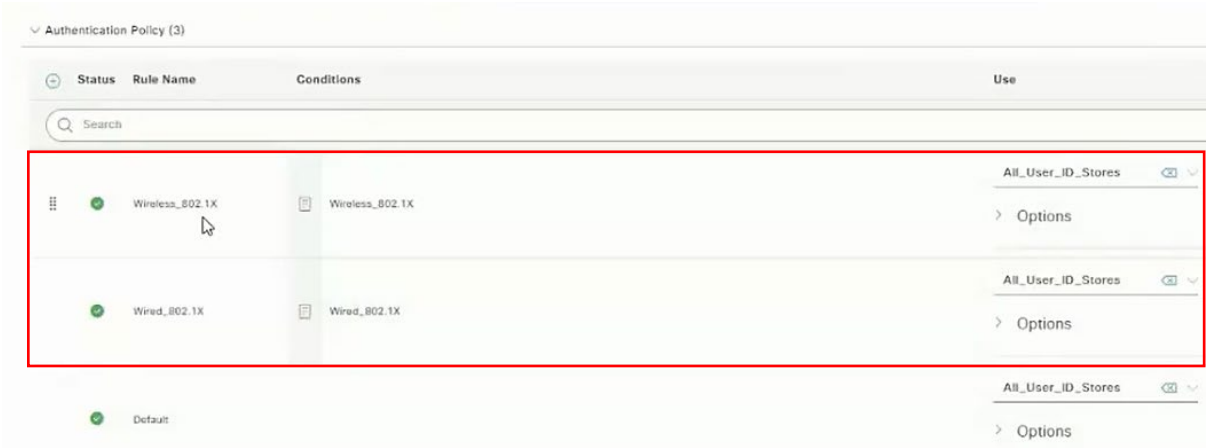


Figura 64. Políticas de autenticación.
Fuente: Pineda, Y. (2023)

De esta manera, en el apartado de autorización, se decide incluir la autorización para dos grupos llamados "**Usuarios del dominio**" y "**Usuarios**" con intención de usarlos en las primeras pruebas piloto. Se encuentran ubicados externamente en el Active Directory llamado "**AD_ALG ExternalGroups**", permitiendo de esta manera con la opción "**PermitAccess**", al crear la condición de "or" permite que cualquiera de los dos grupos del AD sean autorizados a los privilegios, así mismo se crea una política para el grupo llamado "**Default**" que tendrá el perfil "**DenyAccess**" y no autorizará privilegios.

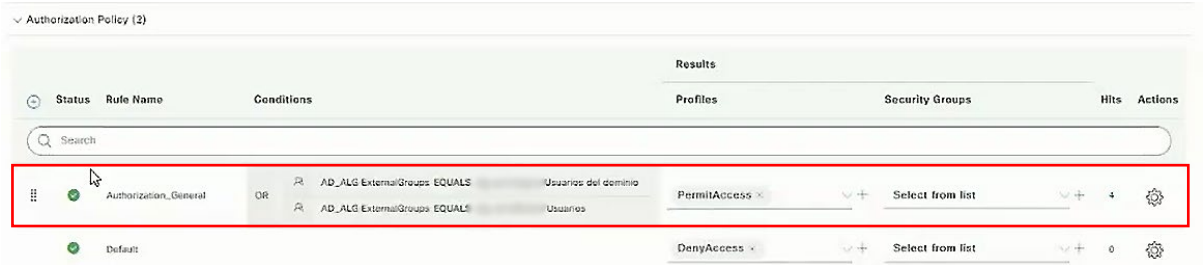


Figura 65. Políticas de autorización.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 9.** Añadir dispositivos de la red corporativa a la plataforma CISCO ISE

La penúltima actividad de esta fase, consiste en añadir los dispositivos de la red a la plataforma CISCO ISE. Se procede a dirigirse a **Dashboard>Administration>Network Resources>Network Devices,** donde se encuentra el panel de dispositivos, para la importación de dispositivos se puede realizar a través de dos métodos:

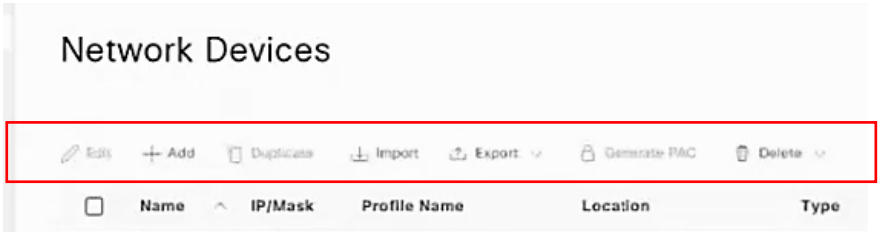


Figura 66. Opciones para Network Devices.
Fuente: Pineda, Y. (2023)

Método 1:

Agregar los dispositivos individualmente a partir de la pestaña de **"+ Add"**, cual desplegará diferentes atributos para otorgarle al dispositivo. Se le asigna un nombre, descripción, su IP o distintas IP que maneja, el perfil de dispositivo (fabricante), el modelo de dispositivo, la versión de software, así mismo, su ubicación y el tipo de dispositivo que se añade, apreciado en la **figura 67.**

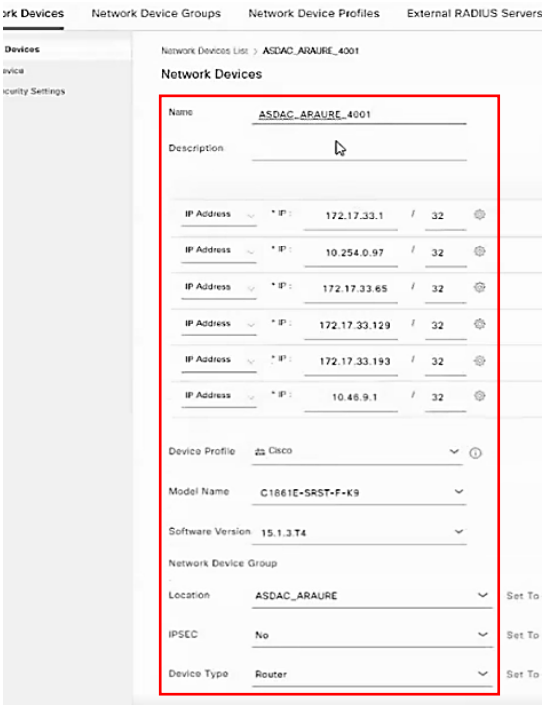


Figura 67. Asignación de los atributos para dispositivos.
Fuente: Pineda, Y. (2023)

De esta forma, se habilitan las configuraciones de RADIUS y TACACS, ambas contarán con una contraseña compartida (Shared secret), las transacciones entre el cliente y el servidor RADIUS y TACACS se autentican mediante el uso de esta contraseña, así mismo permite la configuración de estos servidores a través de consola.

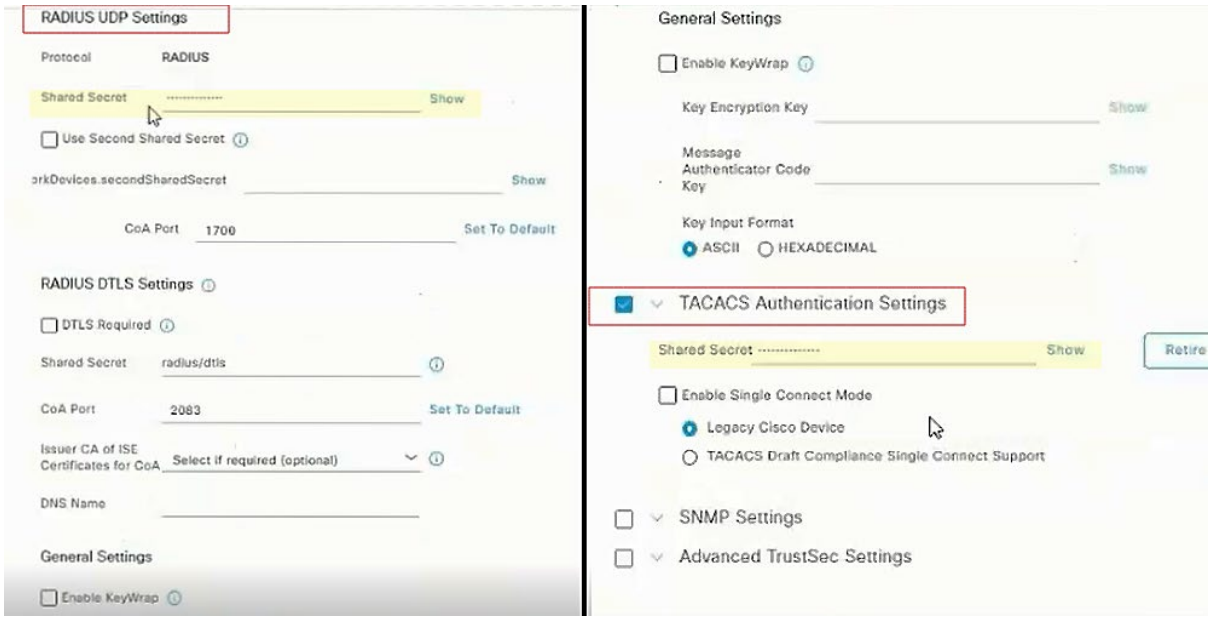
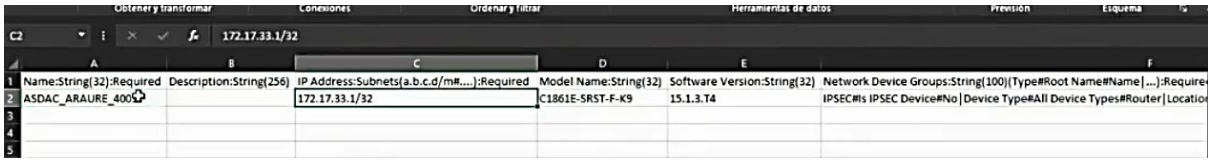


Figura 68. Configuración de RADIUS y TACACS en dispositivos.
Fuente: Pineda, Y. (2023)

Método 2:

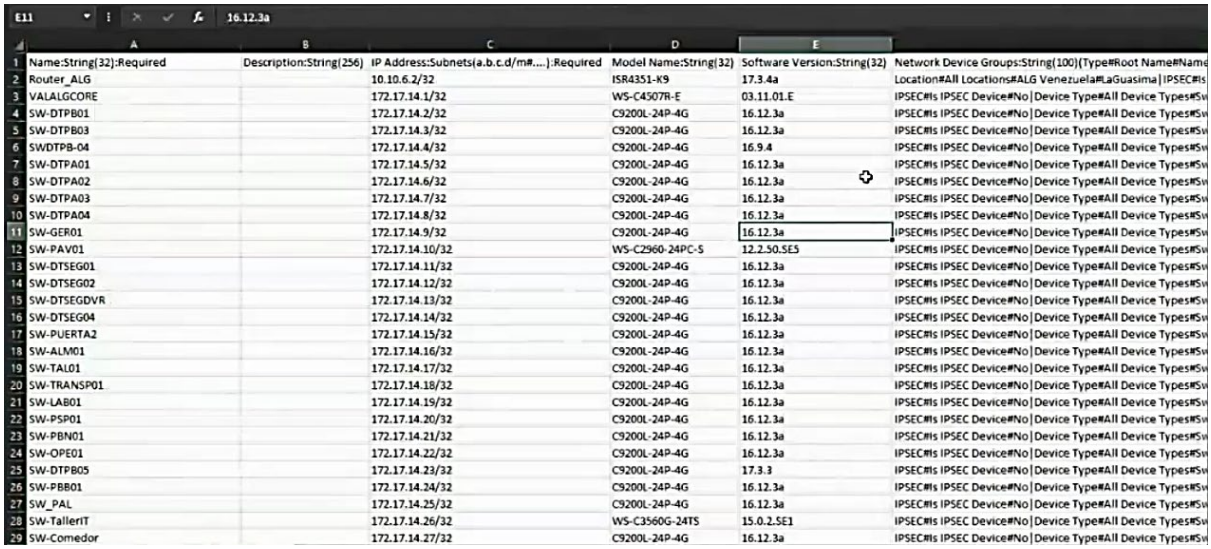
El segundo método consiste en importar masivamente los dispositivos a través de la pestaña "**Import**". La importación es realizada a través de un archivo CVS (comma-separated values), se conoce como un archivo de texto y los datos están separados a través de comas en tablas, este proceso se realiza a través del programa "Excel". Los datos de los equipos descubiertos en la fase dos de la presente investigación (apreciado en la **figura 27**) serán importados desde un archivo CVS hacia la plataforma CISCO ISE. A través de la **figura 69**, se aprecia un ejemplo con los mismos datos del método anterior, donde se muestra el formato con los diferentes atributos, es importante destacar que las IP deben poseer la correspondiente máscara de subred para que sean válidas. Los campos a llenar serán: name, IP address, model name, software version, network device groups and location, authentication protocol, authentication shared secret, tacacs shared secret, profile (nombre del fabricante).



	A	B	C	D	E	F
1	Name:String(32):Required	Description:String(256)	IP Address:Subnets(a.b.c.d/m#....):Required	Model Name:String(32)	Software Version:String(32)	Network Device Groups:String(100)(Type#Root Name#Name|...):Require
2	ASDAC_ARAURE_400		172.17.33.1/32	C1861E-SRST-F-K9	15.1.3.T4	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Router|Locatio
3						
4						
5						

Figura 69. Atributos a consideración para el archivo .CVS.
Fuente: Pineda, Y. (2023)

Así mismo, se aprecia el archivo completo de los dispositivos descubiertos en la segunda fase de la presente investigación. Este método resulta más eficiente debido que permite importaciones masivas de dispositivos a la plataforma.



	A	B	C	D	E	
1	Name:String(32):Required	Description:String(256)	IP Address:Subnets(a.b.c.d/m#....):Required	Model Name:String(32)	Software Version:String(32)	Network Device Groups:String(100)(Type#Root Name#Name
2	Router_ALG		10.10.6.2/32	ISR4351-K9	17.3.4a	Location#All Locations#ALG Venezuela#LaGuasima|IPSEC#Is
3	VALALGCORE		172.17.14.1/32	WS-C4507R-E	03.11.01.E	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
4	SW-DTPB01		172.17.14.2/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
5	SW-DTPB03		172.17.14.3/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
6	SWDTPB-04		172.17.14.4/32	C9200L-24P-4G	16.9.4	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
7	SW-DTPA01		172.17.14.5/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
8	SW-DTPA02		172.17.14.6/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
9	SW-DTPA03		172.17.14.7/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
10	SW-DTPA04		172.17.14.8/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
11	SW-GER01		172.17.14.9/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
12	SW-PAV01		172.17.14.10/32	WS-C2960-24PC-S	12.2.50.SE5	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
13	SW-DTSEG01		172.17.14.11/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
14	SW-DTSEG02		172.17.14.12/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
15	SW-DTSEGDVR		172.17.14.13/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
16	SW-DTSEG04		172.17.14.14/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
17	SW-PUERTA2		172.17.14.15/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
18	SW-ALM01		172.17.14.16/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
19	SW-TAL01		172.17.14.17/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
20	SW-TRANSP01		172.17.14.18/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
21	SW-LAB01		172.17.14.19/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
22	SW-PSP01		172.17.14.20/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
23	SW-PBN01		172.17.14.21/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
24	SW-OPE01		172.17.14.22/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
25	SW-DTPB05		172.17.14.23/32	C9200L-24P-4G	17.3.3	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
26	SW-PBB01		172.17.14.24/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
27	SW_PAL		172.17.14.25/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
28	SW-TallerIT		172.17.14.26/32	WS-C3560G-24TS	15.0.2.SE1	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw
29	SW-Comedor		172.17.14.27/32	C9200L-24P-4G	16.12.3a	IPSEC#Is IPSEC Device#No|Device Type#All Device Types#Sw

Figura 70. Archivo .CVS para su importación en Network Devices.
Fuente: Pineda, Y. (2023)

De esta manera, se aprecia la importación de dispositivos de la red empresarial, adjuntando el archivo .CSV en la pestaña seleccionada, apreciado en la **figura 71**.

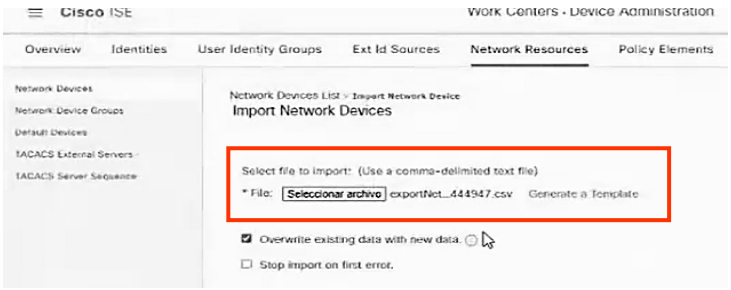


Figura 71. Selección del archivo para la importación masiva de dispositivos.
Fuente: Pineda, Y. (2023)

Para finalizar esta actividad, se muestra finalmente la importación exitosa de todos los dispositivos en la base de datos ubicado en la sección de "Network Devices", apreciado en la **figura 72**.

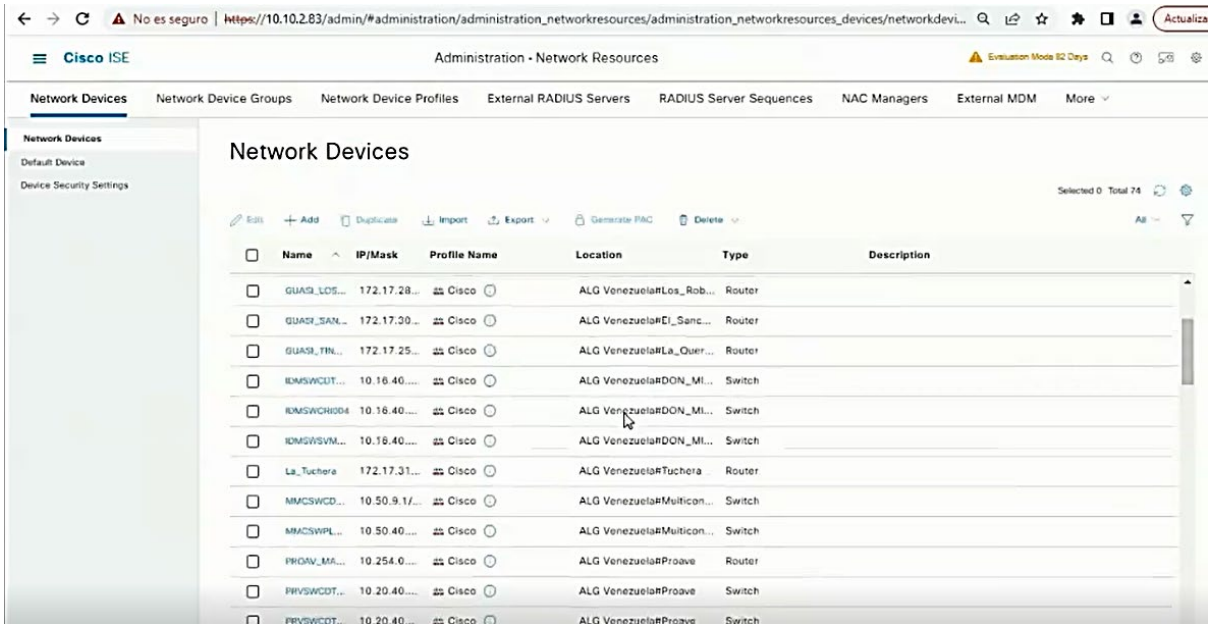


Figura 72. Network Devices.
Fuente: Pineda, Y. (2023)

De esta manera, a través de la pestaña "**Network Device Groups**" se pueden categorizar los tipos de dispositivos que existen, se dividen en AP's, firewall, router, switch y WLC, así mismo se muestran la cantidad de dispositivos que existen por cada tipo. Así mismo, realiza la categorización de los equipos a partir de su locación, se puede apreciar que se crea un apartado específico a nivel nacional llamado "**ALG Venezuela**" y se divide en las diferentes locaciones y granjas de la empresa "Avícola La Guásima", apreciado en la **figura 73**.

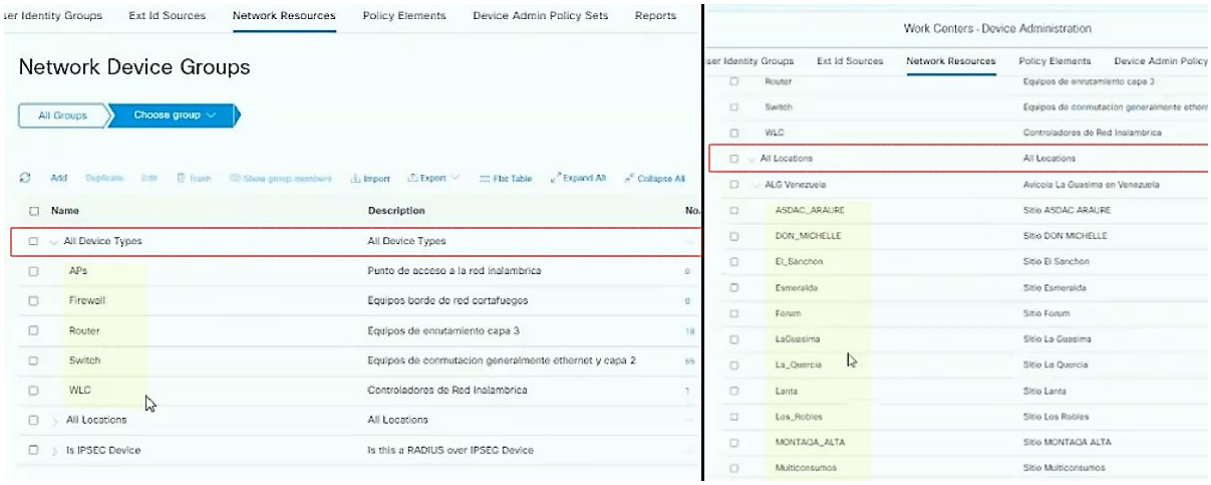


Figura 73. Network Device Groups: tipos de dispositivos y sus locaciones.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 10.** Configuración de todos los dispositivos a través de plantillas de RADIUS y TACAS.

La última actividad de la cuarta fase consiste en la configuración de todos los dispositivos que se necesiten conectar a la red empresarial, conocidos como los endpoints, para la autenticación de RADIUS y TACACS. Este tipo de configuración es necesaria ya que es el paso final para la autenticación en cada dispositivo, a través de plantillas. A continuación, la plantilla de autenticación de RADIUS:

```
!
dot1x system-auth-control
!
identity profile default
!
radius server ALG-ISE-Dot1X
 address ipv4 10.10.2.83
 key *****  (Shared Secret)
!
aaa group server radius ALG-ISE-Dot1X-G
 server name ALG-ISE-Dot1X
!
aaa authentication dot1x default group ALG-ISE-Dot1X-G
aaa accounting dot1x default start-stop group ALG-ISE-Dot1X-G
!
ip access-list extended PreAuth
 remark # Pre-authorization ACL customized for deployed environment
#
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit udp any any eq tftp
 permit icmp any any echo
```

```
 permit icmp any any echo-reply
 permit ip any host 10.10.2.83
 deny   ip any any
!
interface "type and number"
 ip access-group PreAuth in
 switchport mode access
 switchport access vlan "XXY"
 switchport voice vlan "XYZ"
 switchport voice vlan dot1p
 authentication event server dead action authorize vlan 1
 authentication event server dead action authorize voice
 authentication port-control auto
 authentication host-mode multi-domain
 authentication order mab dot1x
 mab
 dot1x pae authenticator
 mls qos trust cos
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

Por lo que, RADIUS funciona como un cliente/servidor que protege la red ante el acceso no autorizado a través de la plantilla, esta autorización se ejecuta en enrutadores y conmutadores CISCO compatibles, de esta manera, los clientes envían solicitudes de autenticación a servidor RADIUS que contiene la autenticación de usuario e información de acceso. El comando "**radius server**" permite crear un servidor llamado "**ALG-ISE-Dot1X**", con la dirección IP 10.10.2.83, y así mismo se añade la contraseña shared secret en este caso, llamado **key**, la contraseña se puede encontrar en el apartado de "**Network Devices**", situado en la **figura 68.** A continuación, se crea un grupo llamado "**ALG-ISE-Dot1X-G**" utilizado para la autenticación y la contabilidad de los usuarios. Así mismo, a continuación, se observa el comando "**ip access-list extended**" conocido como la lista de control de acceso extendida (ACL) que determina qué tráfico tiene acceso permitido o denegado. Por último, existen una serie de comandos utilizados para la autenticación. De esta manera, el proceso de autenticación por TACACS+ igualmente se aplica a través de la plantilla a continuación:

```
aaa new-model
!
ip tacacs source-interface vlan 180
!
tacacs server ALG-ISE
 address ipv4 10.10.2.83
```

```
 key *****
!
aaa group server tacacs+ ALG-ISE-G
 server name ALG-ISE
!
aaa authentication login default group ALG-ISE-G local
!
aaa accounting exec default start-stop group ALG-ISE-G
aaa accounting commands 15 default start-stop group ALG-ISE-G
aaa accounting commands 14 default start-stop group ALG-ISE-G
aaa accounting commands 13 default start-stop group ALG-ISE-G
aaa accounting commands 12 default start-stop group ALG-ISE-G
aaa accounting commands 11 default start-stop group ALG-ISE-G
aaa accounting commands 10 default start-stop group ALG-ISE-G
aaa accounting commands 9 default start-stop group ALG-ISE-G
aaa accounting commands 8 default start-stop group ALG-ISE-G
aaa accounting commands 7 default start-stop group ALG-ISE-G
aaa accounting commands 6 default start-stop group ALG-ISE-G
aaa accounting commands 5 default start-stop group ALG-ISE-G
aaa accounting commands 4 default start-stop group ALG-ISE-G
aaa accounting commands 3 default start-stop group ALG-ISE-G
aaa accounting commands 2 default start-stop group ALG-ISE-G
aaa accounting commands 1 default start-stop group ALG-ISE-G
aaa accounting commands 0 default start-stop group ALG-ISE-G
aaa session-id common
!
!
aaa authorization config-commands
aaa authorization console
aaa authorization exec default group ALG-ISE-G local
aaa authorization commands 15 default group ALG-ISE-G local
!
!
```

TACACS+ se conoce por proveer una validación centralizada de usuarios que intentan obtener acceso a un dispositivo, como un enrutador o un servidor de acceso a la red. Así mismo, permite utilizar en procesos individuales la autenticación, autorización y contaduría, de esta manera manejando diferentes puntos de acceso desde un solo servicio de gestión. Para usar el comando de configuración global, se utiliza el comando "**aaa new-model**", permite generar una nueva plantilla. Así mismo, se utiliza "**tacacs-server**" para crear el servidor TACACS+ con su respectivo nombre y su dirección IP, e igualmente "**tacacs-server key**" para establecer una clave de encriptación (**shared secret** apreciado en la **figura 68**) que ayuda a encriptar el servidor de acceso a la red y el servidor de TACACS+. Se utiliza el comando "**aaa authentication**" para definir medios de autenticación por TACACS+, en este caso se indicó

que los usuarios se autentican a través del grupo "ALG-ISE-G". Se utiliza el comando "**aaa authorization**" para establecer parámetros que otorgan permisos al usuario basado en rol, en este caso a través del grupo llamado "ALG-ISE-G". Por último, se utiliza el comando "**aaa accounting**" que permite seguir los servicios de acceso del usuario, así como la cantidad de recursos que consumen, por lo que en este caso igualmente se realiza con el grupo anteriormente mencionado.

Instructiva configuración "PC Windows" para Autenticación RADIUS

En otro orden de ideas, para que esta autenticación sea completamente satisfactoria se deben configurar todos los equipos (o endpoints) que posean Windows para que sea autenticado por RADIUS cuando se desee conectar a la red empresarial por el medio cableado.

Paso 1. Por lo que, para este proceso inicialmente se abre "**administrador de servicios**" PC (mediante comando: **services.msc**).

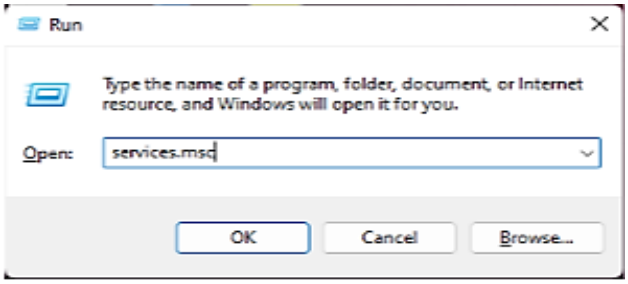


Figura 74. Administración de servicios: services.msc.
Fuente: Pineda, Y. (2023)

Paso 2. Ubicar el servicio "**Configuración automática de redes cableadas**". Hacer clic con botón derecho de mouse, y en menú desplegable clic sobre "**Propiedades**". En la nueva ventana asegurar que el campo "**Tipo de inicio**" este seleccionado "**Automático**" y en el campo "**Estado del servicio**" este iniciado o en todo caso hacer clic en "**Iniciar**". Para finalizar haga clic en "**Aceptar**".

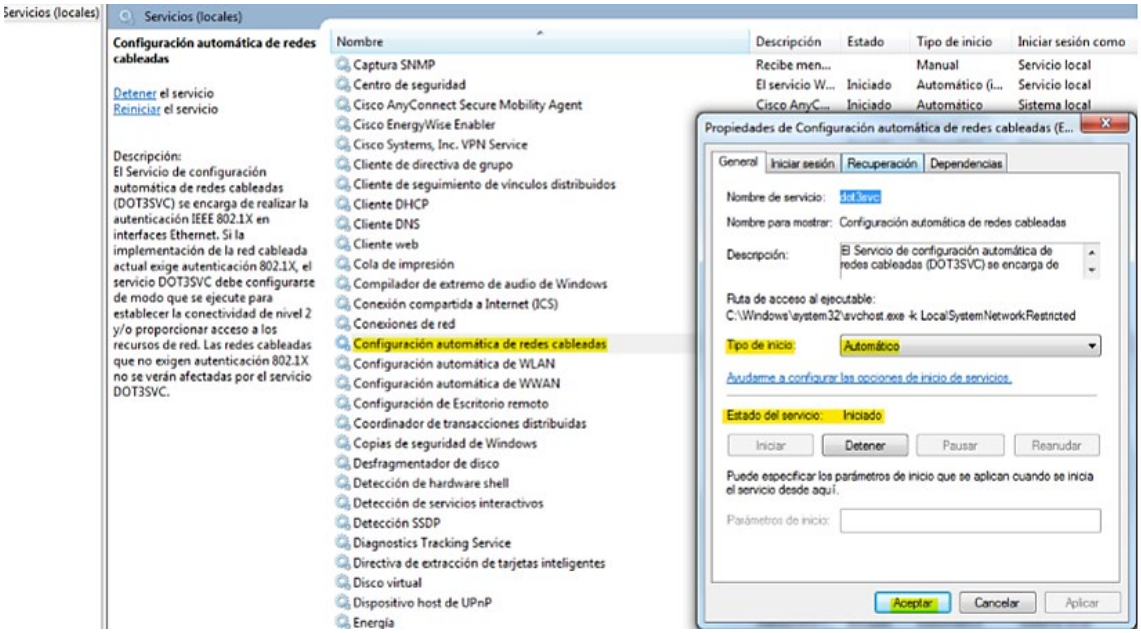


Figura 75. Configuración automática de redes cableadas.
Fuente: Pineda, Y. (2023)

Paso 3. Conectar el cable de red al PC, esperar hasta que se active la conexión (significando esto que se vea actividad del lado de los LED indicadores o inclusive en las estadísticas de la conexión de red en PC.

Paso 4. Abrir las "**Conexiones de Red**" o "**Centro de Recursos Compartidos**" (puede ser a través del comando: **ncpa.cpl**)

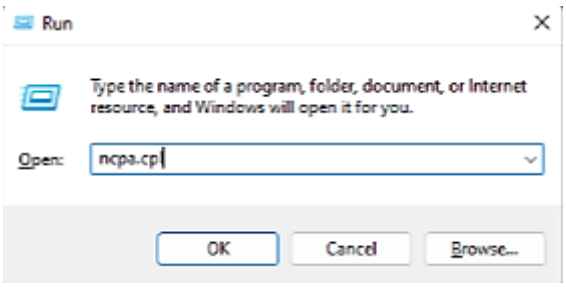


Figura 76. Conexiones de red.
Fuente: Pineda, Y. (2023)

Paso 5. Ubicar a "**Conexión de Área Local**" activa gracias a la conexión del cable de red. Hacer luego clic con botón derecho sobre el icono y seleccionar "**Estado**". Una vez aparezca la nueva ventana, es decir, "**Estado de conexión del área local**" hacer clic en el botón "**Propiedades**". Luego aparecerá una tercera ventana llamada "**Propiedades de conexión del área local**", y allí seleccionar la pestaña "**Autenticación**", por último, hacer los siguientes ajustes:

✓ Marcar la opción "**Habilitar autenticación de IEEE 802.1X**"

- ✓ Marcar la opción "**Recordar mis credenciales para cada conexión cada vez que inicie sesión**"
- ✓ Marcar la opción "**Retroceso a acceso de red no autorizado**"
- ✓ Y en el campo "**Elija un método de autenticación de red**" elegir "**Microsoft: EAP protegido (PEAP)"**

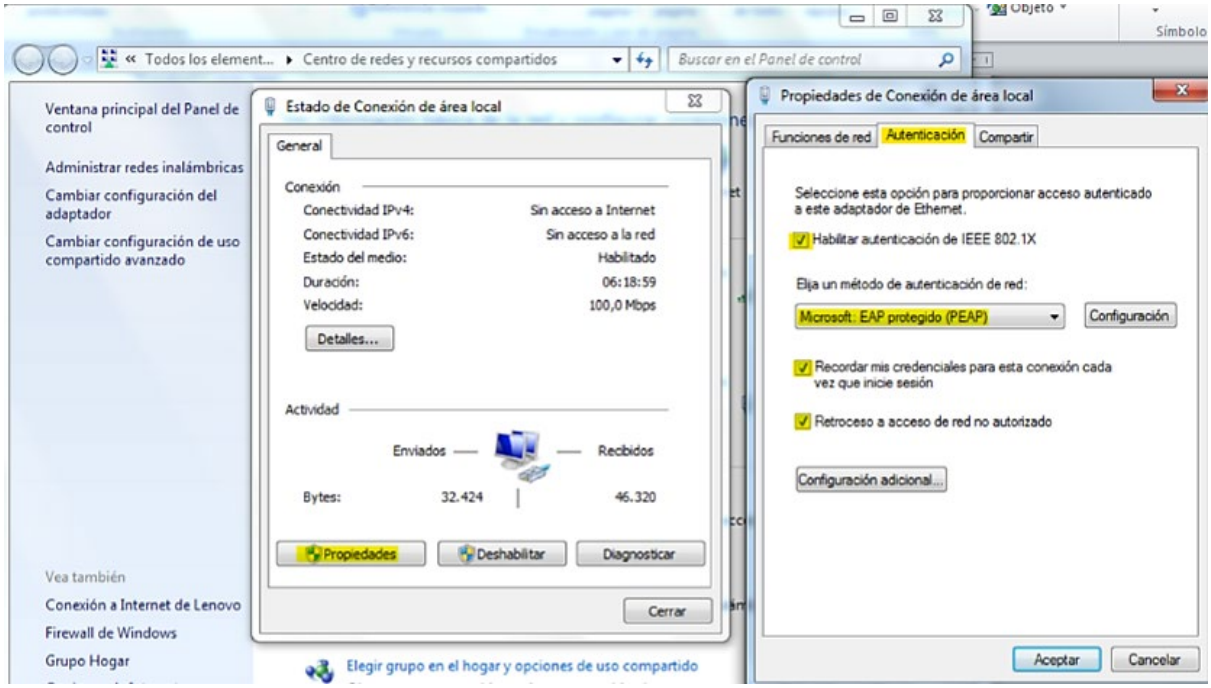


Figura 77. Propiedades de Conexión de área local.
Fuente: Pineda, Y. (2023)

Paso 6. Sin cerrar dicha tercera ventana, "**Propiedades de conexión del área local**", haga clic sobre el botón ubicado al lado del "**método de autenticación de red**", es decir: "**Configuración**", luego en cuarta ventana emergente llamada "**Propiedades de EAP protegido**", hacer los siguientes ajustes:

- ✓ Marcar la opción "**Validar un certificado de servidor**"
- ✓ Marcar la opción "**Habilitar reconexión rápida**"
- ✓ Y en el campo "**Seleccione el método de autenticación**" elegir "**Contraseña segura (EAP-MSCHAP-v2)"**
- ✓ Por último, clic en el botón "**Aceptar**" de esta cuarta ventana.

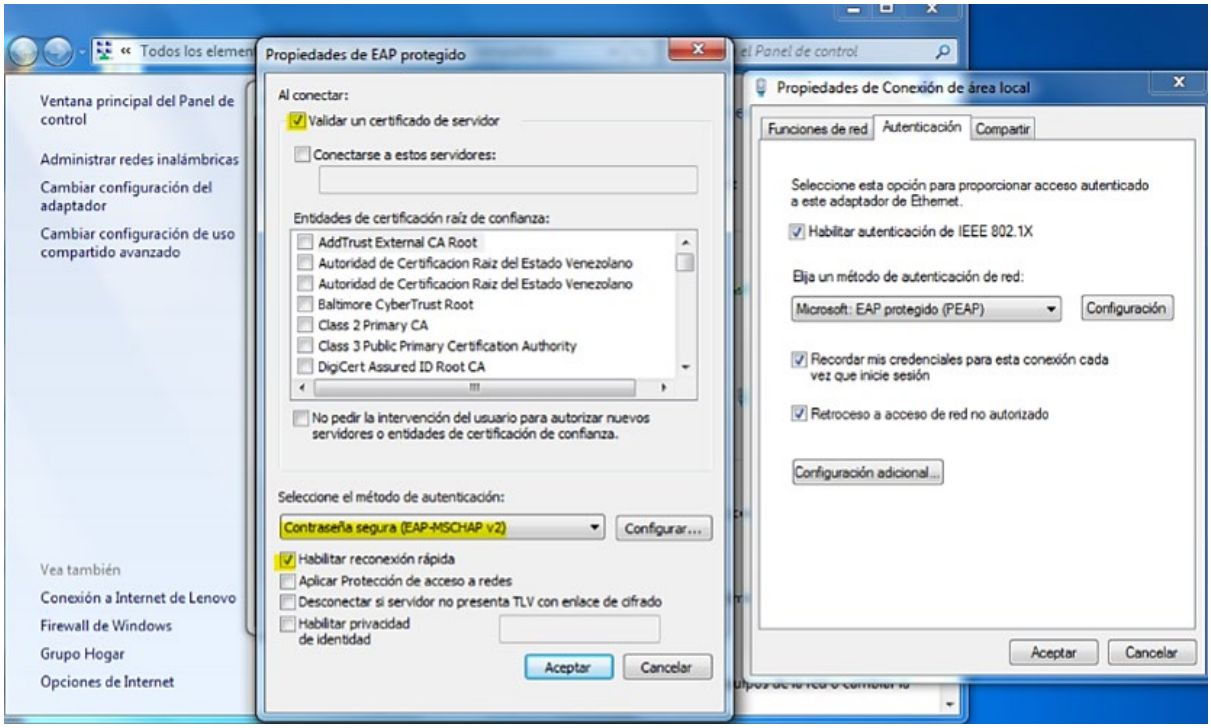


Figura 78. Propiedades de conexión de área local: método de autenticación.
Fuente: Pineda, Y. (2023)

Paso 7. Una vez cerrada la cuarta ventana y sin cerrar dicha la tercera, hacer clic en el botón "**Configuración adicional…",** se abrirá una quinta ventanilla de nombre "**Configuración avanzada**", hacer los siguientes ajustes:

- ✓ Marcar la opción "**Especificar modo de Autenticación**" elegir "**Autenticación del usuario**"
- ✓ Marcar la opción "**Habilitar inicio de sesión único en esta red**"
- ✓ Marcar la opción "**Realizar inmediatamente antes de que el usuario inicie sesión**"
- ✓ Marcar la opción "**Permitir cuadros de dialogo adicionales durante el inicio de sesión único"**
- ✓ Hacer clic botón "**Aceptar"** en esta quinta ventanilla, luego esta se cerrará.

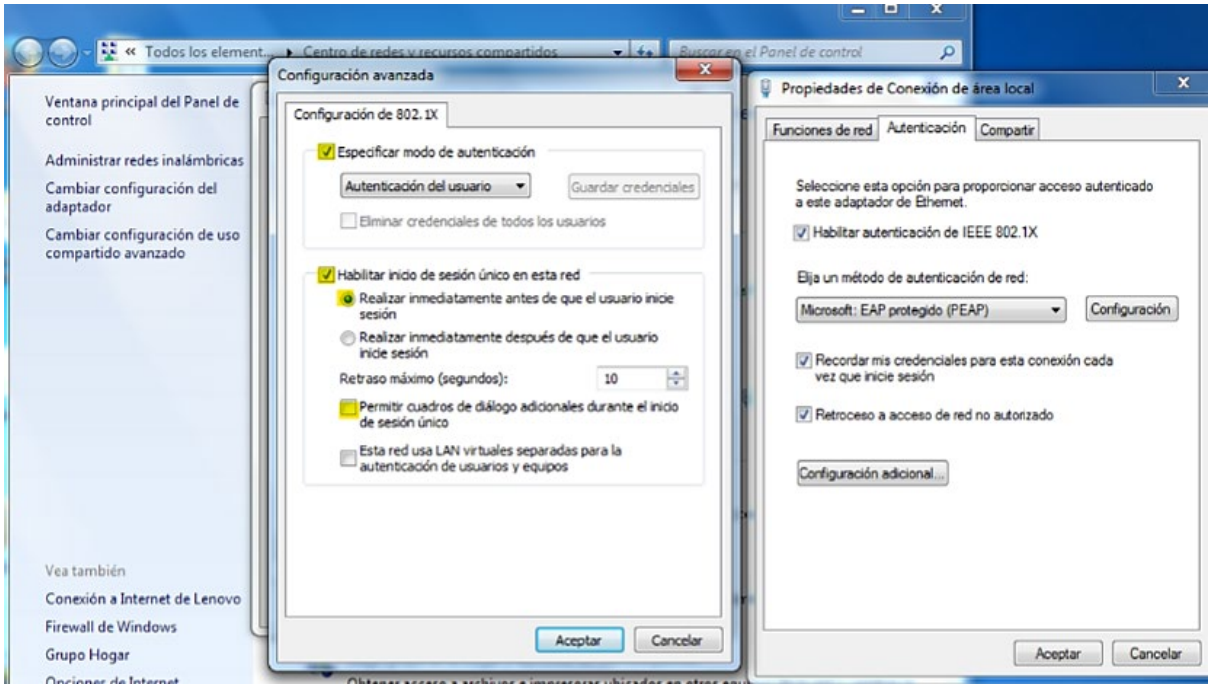


Figura 79. Configuración de 802.1X.
Fuente: Pineda, Y. (2023)

Seguidamente, clic en botón "Aceptar" dentro de la tercera ventana llamada "**Propiedades de conexión del área local"** Por último, clic en botón "**Cerrar**" dentro de la ventana "**Estado de conexión del área local**".

5.5 Fase V: Evaluación de la eficiencia de la plataforma de sistema de acceso a la red a través de plan piloto.

La quinta fase del presente trabajo de grado consiste en tres (3) actividades que se basan en la evaluación de la eficiencia y certificación de la funcionabilidad de la plataforma CISCO ISE a través de las pruebas piloto que se realizarán en diferentes equipos.

Tabla 7.
Actividades. Fase 5.

Actividad	Descripción	Tareas	Responsables
1. Prueba realizada para la autenticación de usuarios en los Live Logs a través de RADIUS.	En esta actividad se procede a realizar la autenticación de usuarios a través de los Live Logs en RADIUS.	Aplicar la plantilla de autenticación de usuarios, verificar autenticación en la plataforma y los detalles de la prueba.	Autor de trabajo de grado Equipo de Setrys

2. Prueba realizada para la autenticación de usuarios y dispositivos a través de la red cableada en puntos de acceso a través de RADIUS.	Se procede a realizar la autenticación de usuarios y dispositivos en la red cableada a través de RADIUS.	Aplicar la instructiva de configuración de RADIUS, aplicar la plantilla de RADIUS, realizar prueba de autenticación a través de Ethernet, verificar los detalles.	Autor de trabajo de grado Equipo de Setrys
3. Prueba realizada para la autenticación y autorización través de TACACS	Se realizará la prueba para la autenticación y autorización a través de TACACS.	Aplicar la plantilla de TACACS, verificar autenticación y autorización en la plataforma y los detalles de la prueba.	Autor de trabajo de grado Equipo de Setrys

Fuente: Pineda, Y. (2023)

- **Actividad Nro. 1.** Prueba realizada para la autenticación de usuarios en los Live Logs a través de RADIUS.

A continuación, se realizarán las pruebas piloto para la autenticación de los usuarios. La prueba se realiza a través de una sesión abierta de SSH con un usuario que se encuentra dentro de Active Directory incluido en la plataforma CISCO ISE, en el switch utilizado para la prueba llamado "**SW-TallerIT**". Este proceso se monitorea a través de la pestaña de **Dashboard>Operations>Radius>Live Logs**, que nos permitirá ver en vivo todas las operaciones que se han realizado, y mostrando información como el tipo de autenticación, autorización y su ubicación, apreciado en la **figura** 80.

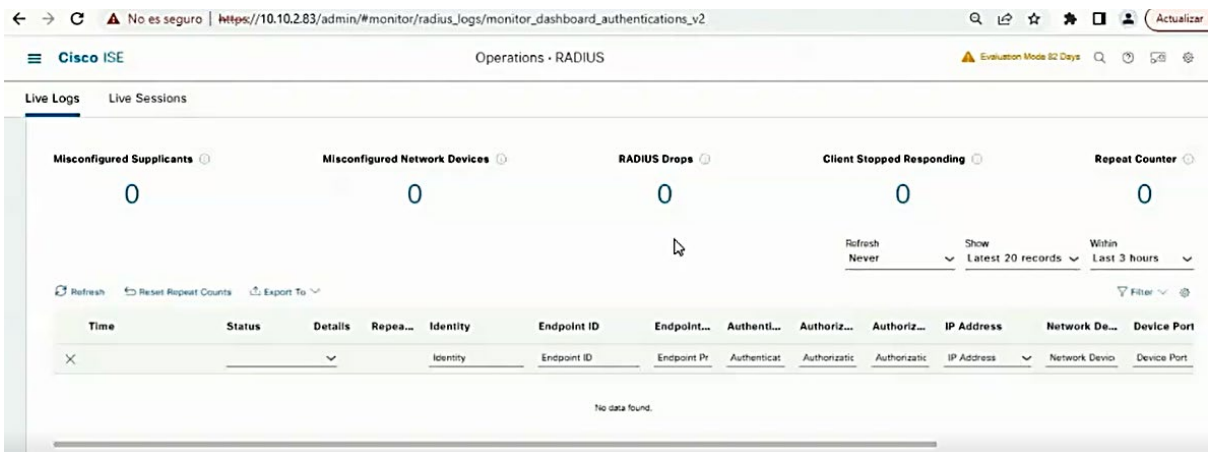


Figura 80. Live Logs de RADIUS.
Fuente: Pineda, Y. (2023)

De esta manera, luego de implementar las plantillas de RADIUS y TACACS+ mostradas en la fase cuatro de la presente investigación, se prosigue a realizar la primera prueba de autenticación de usuarios, a través del siguiente comando:

test aaa group ALG-ISE-Dot1X-G server name ALG-ISE-Dot1X **USUARIO-X** **CONTRASENA-X** new-code

Se aprecia de esta manera que contamos con el grupo "**ALG-ISE-Dot1X-G**" y el nombre del servidor "**ALG-ISE-Dot1X**" y así mismo se introduce el nombre del usuario y la contraseña, en este caso, se realiza con el usuario de prueba llamado "wramirez_s" seguido de su contraseña. El resultado de esta prueba de autenticación fue exitoso, como muestra por consola, apreciado en la **figura 81.**

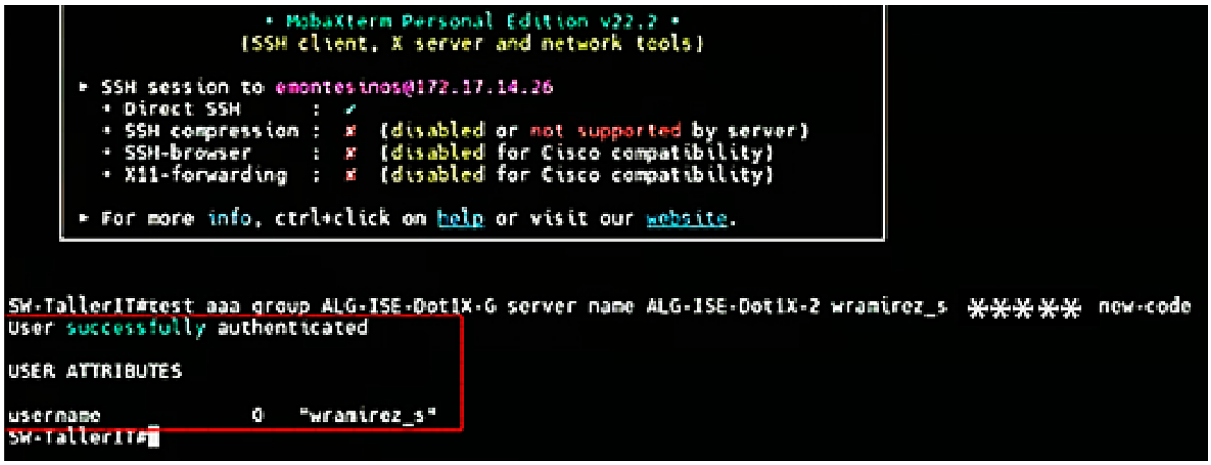


Figura 81. Autenticación satisfactoria de usuario por RADIUS.
Fuente: Pineda, Y. (2023)

Por lo que, cada usuario que se autentique a través de los protocolos RADIUS/TACACS+ serán mostrados en este medio (de manera automática), observamos de esta manera el usuario, las políticas de autenticación en este caso fueron "**Default**", y las políticas de autorización se realizaron por "**Autorization_General**", luego finalmente se observa que fue autenticado por un dispositivo llamado "**SW-TallerIT**" siendo el switch de esta área.

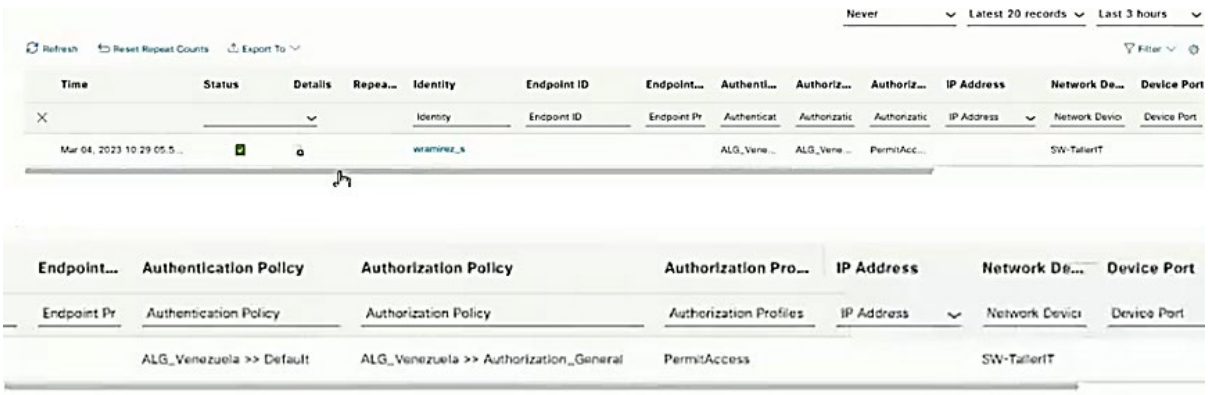


Figura 82. Autenticación del usuario en Live Logs a través de RADIUS.
Fuente: Pineda, Y. (2023)

Una de las herramientas de gran utilidad de esta sección llamada Live Logs es tener la capacidad de ver todos los detalles de cómo se autenticó y por qué medios, a continuación, se selecciona en la pestaña de "**Details**" y nos ofrece una gran cantidad de información, apreciado en la **figura 83**.

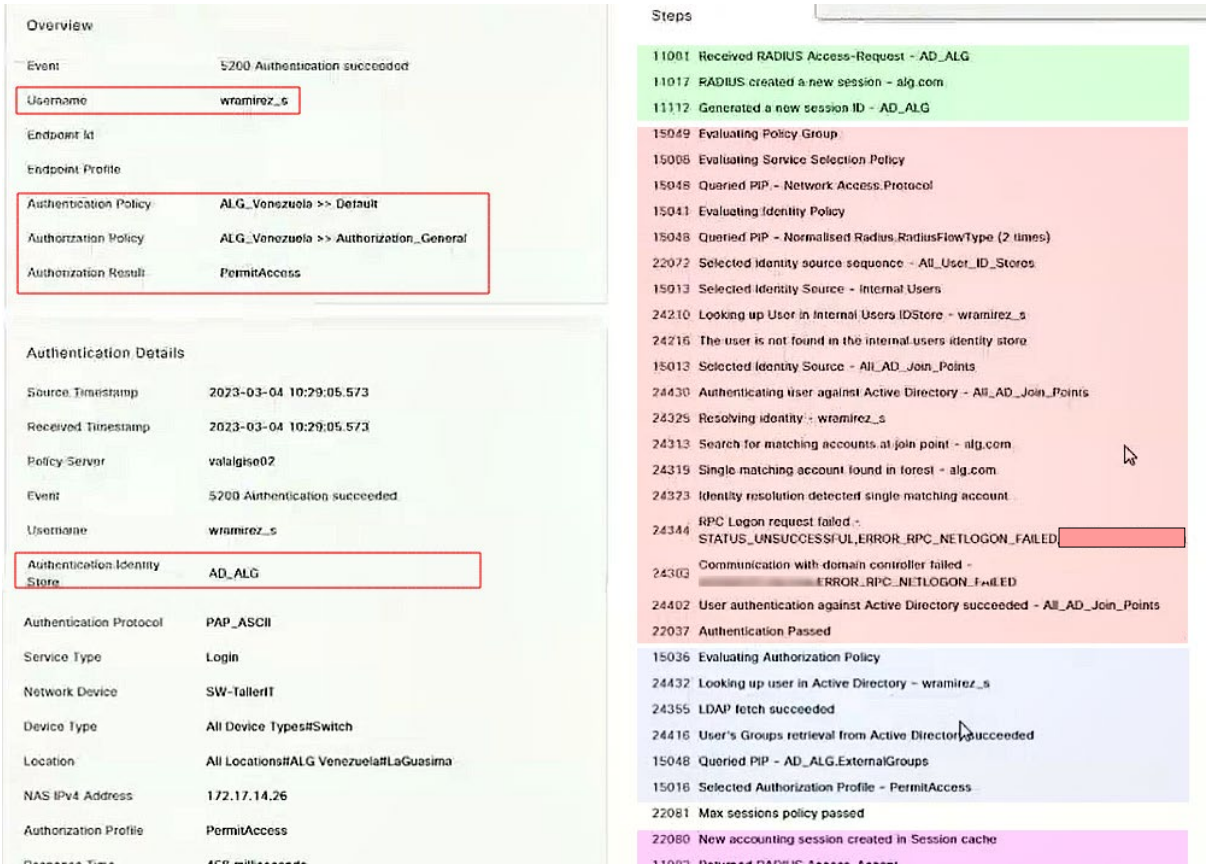


Figura 83. Detalles de la autenticación del usuario y consola.
Fuente: Pineda, Y. (2023)

En el panel izquierdo observamos el usuario, las políticas de autenticación y autorización. Así como los detalles de autenticación que nos permite ver el servidor donde se encuentra, en qué base de datos de identidades se encuentra (en este caso el Active Directory),

el protocolo de autenticación, el dispositivo que se utilizó para autenticar (en este caso un switch), etc. Así mismo, en el panel derecho se observa la consola de todos los registros realizados por el Live Log, inicialmente en el primer cuadro verde se crea la sesión con RADIUS, y se genera la ID de la sesión. Luego, en el cuadro rojo, se procede a evaluar en dónde se encuentran las credenciales del usuario que se busca autenticar y el grupo dónde se encuentra. Continuando en el cuadro azul, se evalúan el tipo de perfil de autorización que tendrá el usuario. Por último, en el cuadro violeta, ya autenticado y autorizado el usuario, se abre una sesión de contabilidad que permite registrar logs y recursos consumidos de la plataforma.

- **Actividad Nro. 2.** Prueba realizada para la autenticación de usuarios y dispositivos a través de la red cableada en puntos de acceso a través de RADIUS.

La autenticación de RADIUS por medio de PC/ Red cableada es realizada a partir de la configuración de las plantillas y el procedimiento de configuración por Windows para la autenticación, utilizando en este caso el método de autenticación el protocolo de autenticación extensible (EAP). Al utilizar las plantillas sin la configuración de Windows descrita en la última actividad de la fase cuatro de la presente investigación, arroja un cuadro de autenticación de Ethernet, cual no podrá verificar la identidad del servidor y está relacionado con los certificados que autentican el servidor, apreciado en la **figura** 84.

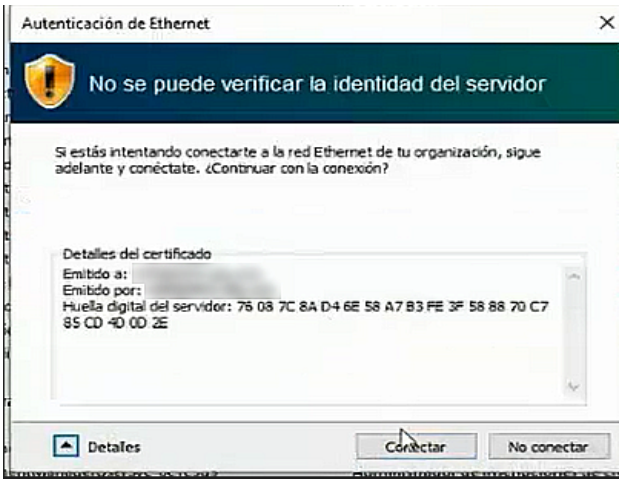


Figura 84. Autenticación de Ethernet fallida.
Fuente: Pineda, Y. (2023)

A continuación, la plantilla de RADIUS anteriormente explicada en la fase cuatro de la presente investigación, es implementada por la consola en el dispositivo switch llamado "**SW-DTPB05**", apreciado en las **figura**s 85, 86, y 87.

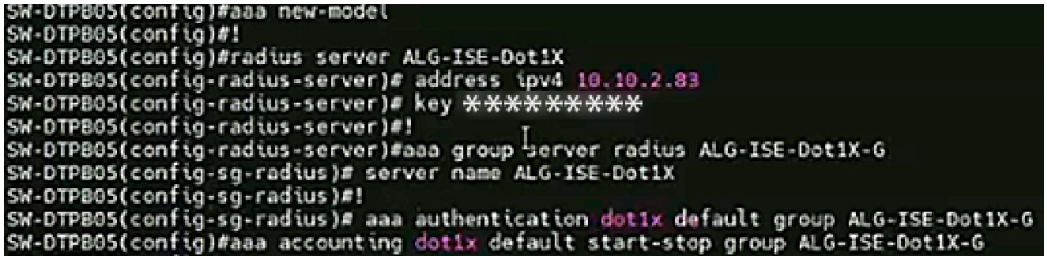


Figura 85. Aplicación de la plantilla RADIUS (1).
Fuente: Pineda, Y. (2023)

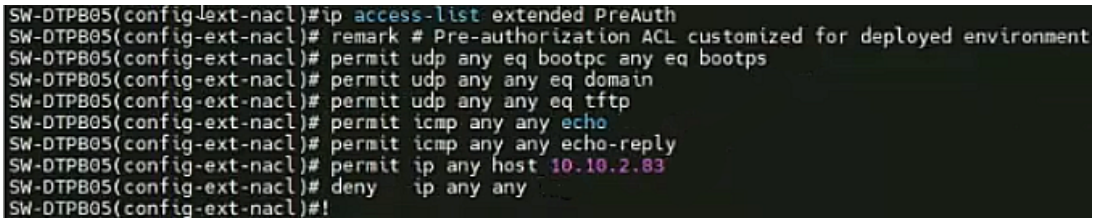


Figura 86. Aplicación de la plantilla RADIUS (2).
Fuente: Pineda, Y. (2023)

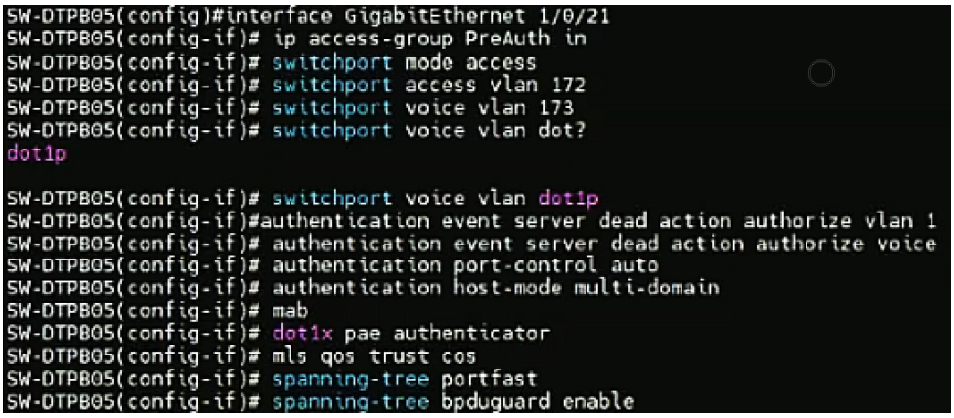


Figura 87. Aplicación de la plantilla RADIUS (3).
Fuente: Pineda, Y. (2023)

De esta forma, la prueba piloto se llevó a cabo con un dispositivo, en este caso una laptop, de la marca “Dell” donde se conectó un cable de red conectado por un punto de acceso físico de la empresa “Avícola La Guásima”, en la **figura 88** se puede apreciar un cuadro de Windows, pidiendo las credenciales usuario y contraseña, en este caso, utilizando el usuario de prueba “**wramirez**” seguido su contraseña.

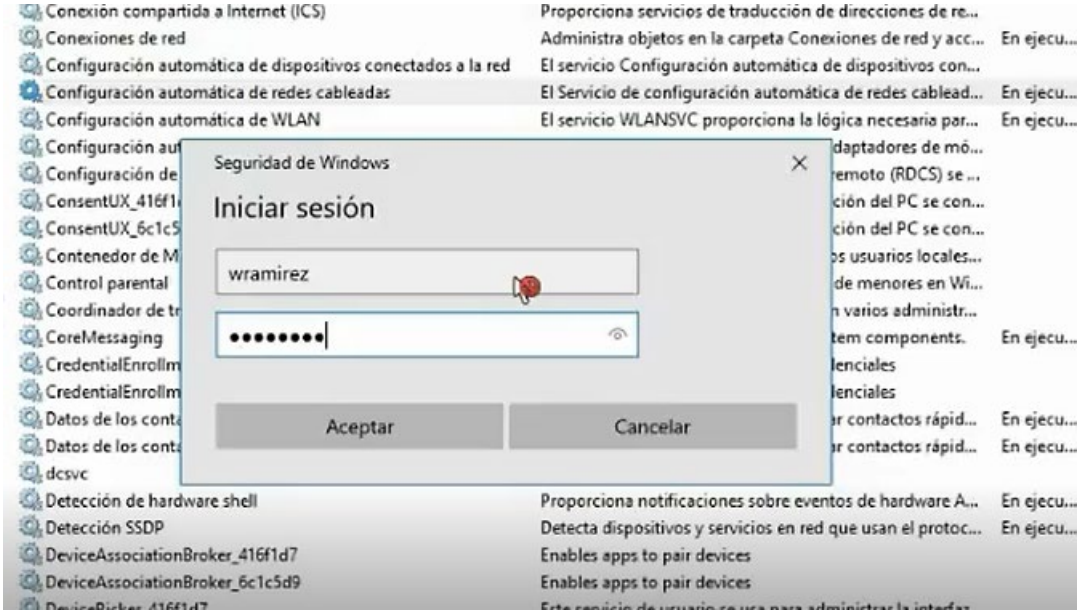


Figura 88. Autenticación por medio cableado satisfactoria.
Fuente: Pineda, Y. (2023)

Así mismo, en las configuraciones de red en el panel de control de Windows, aparece de esta forma, la red conectada a través de Ethernet a la red **"AvicolaLaGuasima",** permitiendo la conexión a través de puntos de acceso por medio de la autenticación de RADIUS, de esta manera, cada dispositivo que sea conectado estará autenticado y autorizado para realizar sus actividades diarias.

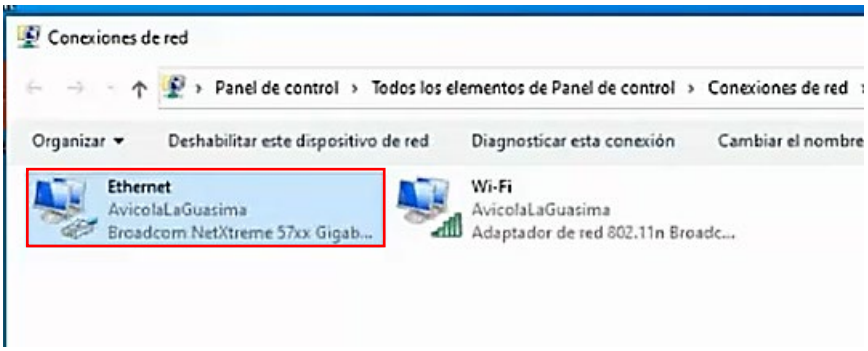


Figura 89. Conexiones de red a través de Ethernet.
Fuente: Pineda, Y. (2023)

Las pruebas realizadas son registradas por los "**Live Logs**" de la plataforma CISCO ISE, a través de RADIUS, por lo que se aprecia en la **figura 90**, distintas pruebas realizas con el dispositivo "**Dell**" utilizado. En la primera prueba marcada de rojo, se aprecia que su estado fue fallido debido a que no se encontraba la configuración de Windows descrita en la actividad de la fase anterior, provocando que no fuera autenticado a través de RADIUS, se puede apreciar en la **figura** que no se le asignó ningún atributo al apartado de autorización. A continuación, se observa la fecha que fue registrado, así mismo el estado que se encuentra la sesión y detalles,

la identidad del usuario "**wramirez**", el identificador de endpoint, el tipo de dispositivo que se está registrando siendo "**Dell**", el tipo de política de autenticación que se aplicó, en este caso se observa que fue a través de la política "**Wired_802.1X**", igualmente se autoriza con la política de "**Autorization_General**" debido que el usuario pertenece a los grupos de usuarios importados en la plataforma y por ende, recibe los permisos de autorización y se le asigna "**PermitAccess**".

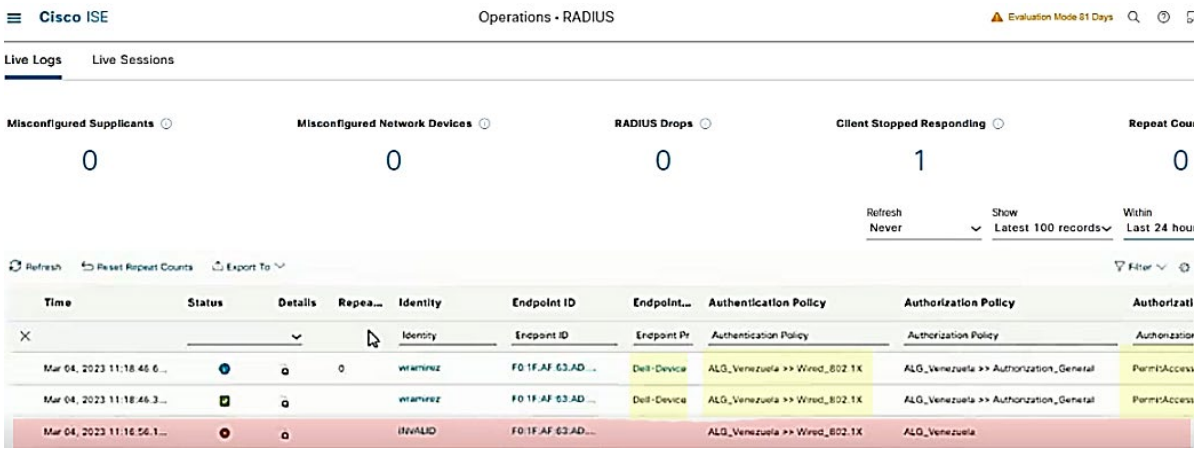


Figura 90. Registros de la prueba piloto en los Live Logs de RADIUS.
Fuente: Pineda, Y. (2023)

De esta manera, igualmente se observan los detalles de esta prueba y se lee por consola el proceso donde se crea una petición para generar una sesión de RADIUS, se evalúa las políticas de grupo del Active Directory, así mismo el proceso de autenticación el protocolo de autenticación extensible (EAP) se emplea. Por lo tanto, en la **figura 91** se aprecia que fue completamente satisfactoria.

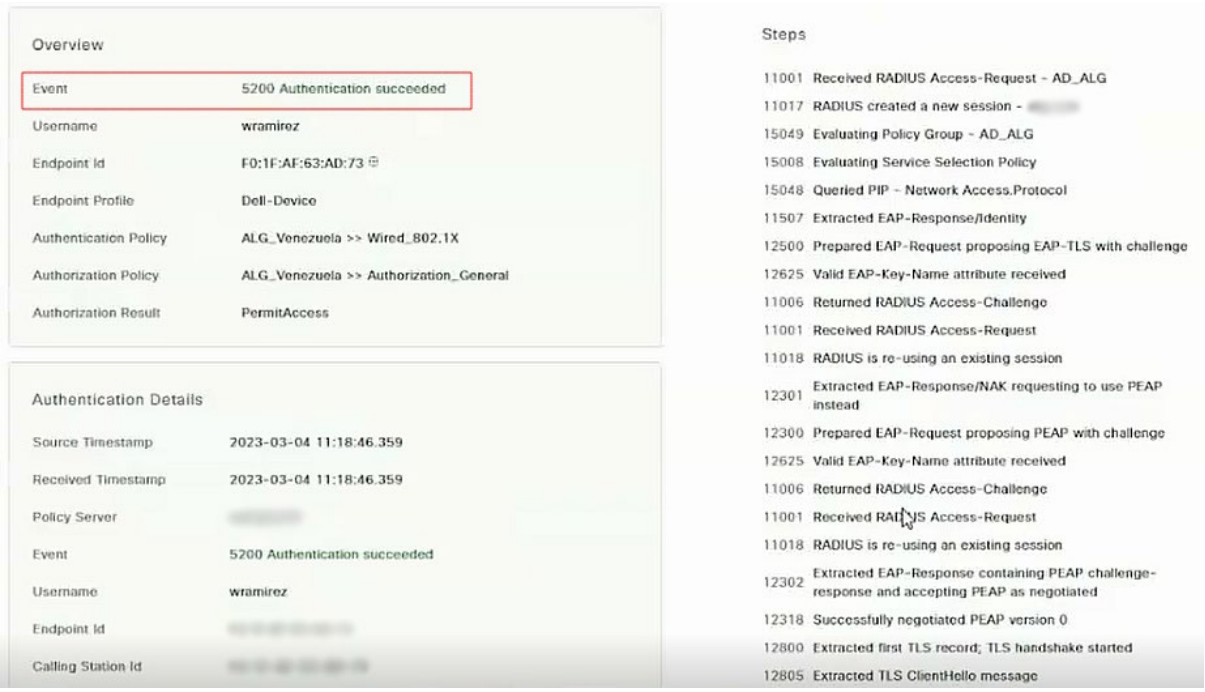


Figura 91. Detalles de la prueba piloto en los Live Logs de RADIUS.
Fuente: Pineda, Y. (2023)

– **Actividad Nro. 3** Prueba realizada para la autenticación y autorización través de TACACS.

La actividad se realizó con la intención de realizar las pruebas de autenticación, autorización y auditoría (logs) han donde a través de la **figura 92**, muestran que han sido exitosas. Las mismas se realizaron a través del conmutador (switch) llamado "**SW-DTPB05**".

```
SW-DTPB05(config)#tacacs server ALG-ISE
SW-DTPB05(config-server-tacacs)# address ipv4 10.10.2.83
SW-DTPB05(config-server-tacacs)# key **********
SW-DTPB05(config-server-tacacs)#exit
SW-DTPB05(config)#aaa group server tacacs+ ALG-ISE-G
SW-DTPB05(config-sg-tacacs+)# server name ALG-ISE
SW-DTPB05(config-sg-tacacs+)#
SW-DTPB05(config-sg-tacacs+)#exit
SW-DTPB05(config)#aaa authentication login default group ALG-ISE-G local
SW-DTPB05(config)#
SW-DTPB05(config)#aaa accounting exec default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 15 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 14 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 13 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 12 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 11 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 10 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 9 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 8 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 7 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 6 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 5 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 4 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 3 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 2 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 1 default start-stop group ALG-ISE-G
SW-DTPB05(config)#$ing commands 0 default start-stop group ALG-ISE-G
SW-DTPB05(config)#aaa session-id common
```

Figura 92. Aplicación de la plantilla TACACS+.
Fuente: Pineda, Y. (2023)

Se procede a implementar la plantilla de TACACS+, apreciado en la **figura 92**, para la creación del servidor de TACACS+, cual nos ayudará a crear un medio de autenticación y autorización para usuarios y dispositivos. Por lo que, para verificar los usuarios se lleva a cabo dos comandos de verificación:

```
Comandos de verificacion:
-------------------------
test aaa group tacacs+ USUARIO-X CONTRASENA-X legacy
test aaa group tacacs+ USUARIO-X CONTRASENA-X new-code
```

El comando de verificación consiste en probar la configuración de autenticación de un USUARIO-X y una CONTASENA-X, con diferentes modos (legacy y new-code) utilizado para el usuario y credenciales correspondientes, cual ha sido autenticado satisfactoriamente a través de los comandos mencionados anteriormente, apreciado en la **figura 93**.

Figura 93. Autenticación satisfactoria de usuario por TACACS+
Fuente: Pineda, Y. (2023)

A través de los "**Live Logs**" se muestra la identidad de usuario llamado "**wramirez_s**", así como el tipo de acción que está realizando, en este caso autenticación del usuario así mismo la autorización del dispositivo, que es autenticado por las políticas de "**AdmDEV_ALG**" y así mismo, autorizado por la política de "**Author_AdmDEV_ALG**". De esta manera, también se muestra el dispositivo mencionado anteriormente, donde se realizaron las pruebas y, por último, muestra la IP del dispositivo donde se realiza la acción.

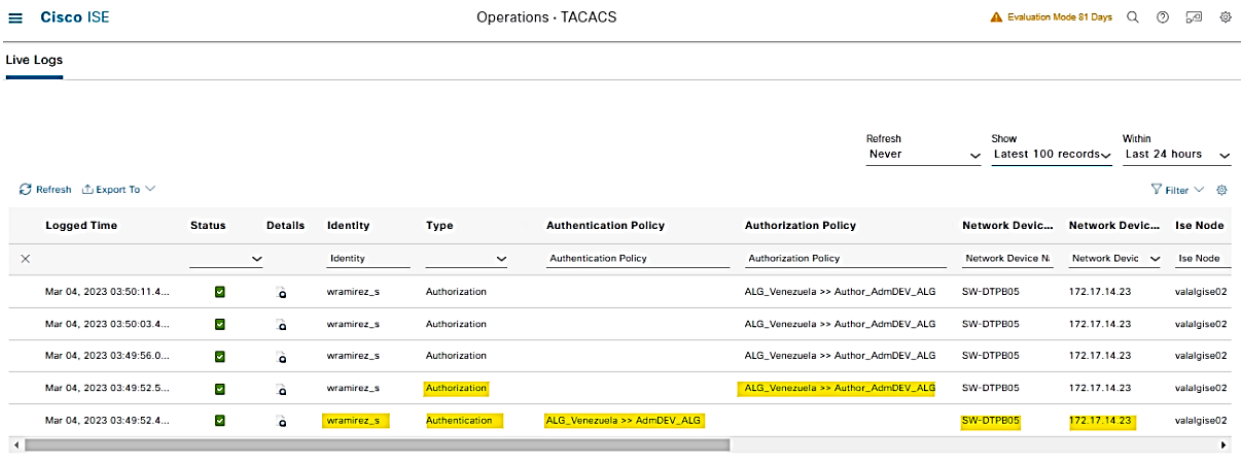


Figura 94. Detalles de la prueba piloto en los Live Logs de TACACS.
Fuente: Pineda, Y. (2023)

CONCLUSIONES

En el presente trabajo de investigación, se ha llevado a cabo cinco (5) fases metodológicas con diferentes actividades sobre Cisco ISE, un sistema de gestión de identidad y acceso para la red empresarial "Avícola La Guásima", donde los resultados obtenidos durante el proceso de pruebas han demostrado que la implementación de Cisco ISE es efectiva y confiable en el entorno evaluado. A través de la investigación, se generaron las siguientes conclusiones:

1. La investigación permitió diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A. Se obtuvo un análisis completo de los aspectos clave relacionados con el acceso a la red, identificando fortalezas y debilidades en el sistema existente. A través de la entrevista formal, guía de observación, así como el diagrama de Causa-Efecto y matriz FODA
2. Se realizó un análisis exhaustivo de la estructura actual de la topología de la interconexión de la red empresarial y se evaluaron las configuraciones disponibles a través del medio/plataforma para el proceso de seguridad de datos y usuarios. Esto proporcionó una visión detallada de la infraestructura de red existente y las medidas de seguridad implementadas por medio del estudio de la topología cableada e inalámbrica
3. Se identificaron los requisitos mínimos necesarios para la implementación de CISCO ISE en la empresa Avícola La Guásima, C.A. Esto permitió establecer los criterios necesarios para garantizar una implementación exitosa y efectiva de la solución de seguridad
4. Se logró desplegar los componentes y estructuras lógicas y funcionales de la capa de seguridad en la red empresarial. Se configuraron adecuadamente los dispositivos y sistemas necesarios para garantizar una protección óptima de la red y los datos sensibles de la empresa
5. Se evaluó el desempeño de la nueva capa de seguridad implementada utilizando la plataforma CISCO ISE. Se realizaron pruebas para medir la eficacia de las políticas de seguridad implementadas y se analizó el impacto en la empresa Avícola La Guásima, C.A. Esto permitió determinar la eficiencia y efectividad de las medidas de seguridad implementadas.

Durante las pruebas, se comprobó la funcionalidad y robustez del sistema en cuanto a la autenticación, autorización y auditoría de los usuarios y dispositivos en la red. Las pruebas realizadas abarcaron diferentes tres escenarios y casos de uso, y en todos ellos, Cisco ISE demostró un rendimiento y capacidad para garantizar la seguridad y el control de acceso a la red ante los accesos indebidos y reconocimiento de los equipos utilizados así mismo los detalles que fueron almacenados en los Live Logs.

La operatividad de Cisco ISE con otros componentes de la red y sistemas de autenticación existentes también fue evaluada, y se encontró que el sistema es compatible y se integra sin problemas con las infraestructuras de red ya establecidas.

En resumen, a través del presente trabajo de investigación ha confirmado que Cisco ISE es una solución eficiente para la gestión de identidad y acceso en entornos empresariales, así como una opción valiosa para aquellas organizaciones que buscan fortalecer la seguridad de su red y proteger sus activos digitales.

RECOMENDACIONES

A continuación, se explicarán las recomendaciones que contribuirán a mantener un entorno seguro y protegido en la organización y garantizar la continuidad operativa a mitigar posibles riesgos de seguridad:

1. Realizar un análisis periódico de la situación del sistema de acceso a la red empresarial Avícola La Guásima, C.A., con el fin de mantener actualizada la evaluación de seguridad y detectar posibles brechas o vulnerabilidades. Esto permitirá tomar medidas preventivas de forma proactiva
2. Continuar el monitoreo y análisis de la estructura de la topología de la interconexión de la red empresarial, así como las configuraciones disponibles para el proceso de seguridad de datos y usuarios. Es importante mantenerse al tanto de los avances tecnológicos y las mejores prácticas en seguridad de redes para adaptar y mejorar constantemente la infraestructura de red
3. Revisar y actualizar regularmente los requisitos mínimos para la implementación de CISCO ISE. A medida que la tecnología y las necesidades empresariales evolucionan, es esencial mantenerse actualizado sobre los requisitos y las capacidades de las soluciones de seguridad para asegurarse de que la implementación cumpla con los estándares más recientes
4. Realizar auditorías periódicas de la capa de seguridad implementada con CISCO ISE y las políticas de seguridad asociadas. Esto garantizará que las medidas de seguridad sean efectivas y estén alineadas con las necesidades y los objetivos de seguridad de la empresa Avícola La Guásima, C.A. Además, permitirá identificar áreas de mejora y corregir posibles desviaciones
5. Mantenerse al día con las actualizaciones y parches de seguridad proporcionados por CISCO y otros proveedores relevantes. Es fundamental aplicar las actualizaciones de software y firmware para proteger la infraestructura de red contra las últimas amenazas y vulnerabilidades conocidas
6. Capacitar al personal de la empresa Avícola La Guásima, C.A. en cuanto a las mejores prácticas de seguridad informática y el uso adecuado de la red. La concienciación y la educación en seguridad cibernética son fundamentales para garantizar que los usuarios comprendan y cumplan con las políticas de seguridad establecidas
7. Actualizar constantemente los datos de los dispositivos, e ir actualizando constantemente el mapa topológico de la red empresarial de forma cableada e

inalámbrica en caso de algún cambio. Igualmente, se recomienda a la organización sacarle el mayor provecho a la plataforma Cisco ISE y explotar sus funciones.

Se propone que aún tengan en funcionamiento todos los elementos y sistemas de autenticación, para poder tener una alta disponibilidad y continuidad del control de acceso en caso de alguna incidencia pueda presentarse, con la finalidad que el acceso a la red no se vea afectado.

Por último, se recomienda que en próximos trabajos de investigación se aborde y se dirijan al tema tratado o similares en el presente estudio para la implementación de sistemas de acceso a la red, para promover la importancia de poder controlar, poseer mayor seguridad de los datos y mejorar el acceso de los dispositivos en las organizaciones.

REFERENCIAS BIBLIOGRÁFICAS

¿Qué es Cloud Computing? (s. f.). Salesforce.com. Recuperado de: https://www.salesforce.com/mx/cloud-computing/

Altuve, S., & Rivas, A. (1998). **Metodología de la Investigación.** Módulo Instruccional III. Caracas: Universidad Experimental Simón Rodríguez.

Arias, I; Carrillo, C. (2017) **Rediseño del Sistema de Autenticación de Usuarios de una red Cooperativa a través de la aplicación de la Plataforma Técnológica de Autenticación CISCO ISE (Identity Services Engine) para la empresa NET IO Servicios S.A** [tesis de grado, Escuela Politécnica Nacional]

Arias, F. (1999). **El proyecto de investigación: Guía para su elaboración**. (3ra ed.) Editorial Episteme.

Arias, F. (2006) **El proyecto de investigación: Introducción a la Metodología Científica.** (5ta ed.) Editorial Episteme.

Augustowsky, G. (s. f.). **El registro fotográfico para el estudio de las prácticas de enseñanza en la universidad. De la ilustración al descubrimiento**. Consultado el 10 de enero de 2023. https://area.fadu.uba.ar/area-23/augustowsky23/

Bejarano, E. (2017). **Seguridad en Redes**. Fondo editorial Areandino. Fundación Universitaria del Área Andina. Repositorio Institucional Areandina: https://digitk.areandina.edu.co/bitstream/handle/areandina/1419/Seguridad%20en%20redes.pdf?sequence=1&isAllowed=y

Bonilla, E., Rodríguez, P. (1997) **Más allá del dilema de los métodos**. Grupo Editorial Norma. Colombia.

Bustamante, R. (s. f.). **Seguridad en Redes**. [tesis de grado, Universidad Autónoma del Estado de Hidalgo]. Recuperado de: https://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad+en+redes.pdf

Cisco Identity Services Engine Administrator Guide, Release 2.0. (2020, 18 agosto). Cisco. https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html

Cisco ISE Identity Services Engine Installation Guide, Release 3.1 (2021). Cisco. https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/install_guide/b_ise_InstallationGuide31.html

Cisco Systems**.** (s.f) **Propiedades del Cisco Discovery Protocol (CDP) en el Switches manejado 200/300 Series. Cisco.** Recuperado de: https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-200-series-smart-switches/smb982-cisco-discovery-protocol-cdp-properties-on-200-300-series-ma.pdf

Cisco Systems. (s.f) **Configure el protocolo del descubrimiento de la capa de link (LLDP) en un WAP571 o un WAP571E**. Cisco. Recuperado de: https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-500-series-wireless-access-points/smb5230-configure-link-layer-discovery-protocol-lldp-on-a-wap571-or.html

Cisco Systems**.** (s.f) **Propiedades del Cisco Discovery Protocol (CDP) en el Switches manejado 200/300 Series. Cisco.** Recuperado de: https://www.cisco.com/c/es_mx/support/docs/smb/switches/cisco-small-business-200-series-smart-switches/smb982-cisco-discovery-protocol-cdp-properties-on-200-300-series-ma.pdf

Cisco Systems. (2017) **Cisco AnyConnect Secure Mobility Client**. Cisco Press. Recuperado de: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cisco-anyconnect-secure-esp.pdf

Cisco Systems. (2021) **Official Guide CCPN Security Identity Management.** Editorial Cisco Press.

Constitución de la República Bolivariana de Venezuela. 1999 (Venezuela).

Corletti, A. (2006, 1 noviembre). **ISO-27001**. Los Controles. Recuperado de: http://www.iso27000.es/download/ISO-27001_Los-controles_Parte_I.pdf

Corredera, J. (2020). **Estudio y aplicación de contabilidad y autorización con RADIUS y DIAMETER.** [tesis de grado, Escuela Técnica Superior de Ingeniería Universidad de Sevilla]. Recuperado de:

https://biblus.us.es/bibing/proyectos/abreproy/93344/fichero/TFG-3344+CORREDERA+HIGUERAS%2C+JUAN+D..pdf

Etecé. (2021, 5 agosto). **Red.** Equipo Editorial Etecé. Recuperado de: https://concepto.de/red-2/

Feria, H., Matilla, M. y Mantecón, S. (2020) **LA ENTREVISTA Y LA ENCUESTA: ¿MÉTODOS O TÉCNICAS DE INDAGACIÓN EMPÍRICA?** Dialnet. Recuperado de: https://dialnet.unirioja.es/descarga/articulo/7692391.pdf

Figueredo, O., González, Y., Martínez, E., Moreno, J., Jiménez, E. y Weffer, E. (2020). **Manual para la Elaboración y Presentación de los Anteproyectos, Proyectos de Trabajos de Grado, Trabajos de Grado, Tesis Doctoral e Informe de Pasantías y Extramuros de la Universidad José Antonio Páez.** Universidad José Antonio Páez. San Diego, Carabobo, Venezuela.

Greyrat, R. (2022, 5 julio). **¿Qué es AAA (autenticación, autorización y contabilidad)?** – Barcelona Geeks. Recuperado de: https://barcelonageeks.com/que-es-aaa-autenticacion-autorizacion-y-contabilidad/

Gutiérrez, H. (2010). **Calidad Total y Productividad.** Editorial McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Hassel, J (2003). **RADIUS.** Editorial Octal Publishing, Inc.

Helfrich, D., Ronnau, L., Frazier, J. y Forbes, P. (2006). **Control de admisión a la red de Cisco, Arquitectura y diseño del marco NAC**, 1, 21-22. Recuperado de: https://www.ciscopress.com/articles/article.asp?p=662903

Hernández, R., Fernández-Collado, C. y Baptista, L. (2006). **Metodología de la Investigación** (4ta Edic). DF, México. McGraw Hill.

Hernández, R., Fernández-Collado, C. y Baptista, L. (2010). **Metodología de la Investigación**. (5ta Edic.) DF, México. McGraw Hill.

Huerta, A. (2002). **Seguridad en Unix y Redes.** Acceso físico a las redes.

Hurtado, J. (2012). **El Proyecto de Investigación.** Editor Quirón, Sypal. (Séptima Edición)

ISED. **¿Qué es la seguridad lógica?** (2018, 23 noviembre). Instituto Superior de Estudios. Recuperado de: https://www.ised.es/articulo/seguridad/que-es-la-seguridad-logica/

Ley Especial contra Delitos Informáticos (2001). CONATEL. Venezuela.

Machuca, F. (2022). **8 técnicas de recolección de datos: descubre un mundo más allá de la encuesta**. Recuperado de: https://www.crehana.com/blog/desarrollo-web/tecnicas-recoleccion-de-datos/

Manual de Trabajos de Grado de Especialización, Maestrías y Tesis Doctorales. (2016, 5ta edición). Universidad Pedagógica Experimental Libertador Vicerrectorado de Investigación y Postgrado**.** Fondo Editorial de la Universidad Pedagógica Experimental Libertador (FEDUPEL)**.** Caracas,Venezuela.

Mañas, J. (2016). **Guía de Seguridad (CCN-STIC-401)**. Glosario y Abreviaturas. Editor y Centro Criptológico Nacional.

Martin, J. (2020, 7 mayo). **Grupo nominal: una herramienta para la generación de ideas en grupo.** Recuperado de: https://www.cerem.es/blog/buscar-nuevas-ideas-con-el-grupo-nominal-de-delbecq

Merino, J. (2021) **Desarrollo de Plan de Actividades y políticas de acceso AAA para plataforma de red inalámbrica en entorno productivo para Farmatodo en Venezuela**. [trabajo de grado]. Universidad Católica Andrés Bello. Repositorio UCAB. Venezuela.

Microsoft. (2022, 21 diciembre). **Introducción a Active Directory Domain Services. Microsoft Learn.** Recuperado 15 de enero de 2023, de https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Mier, E y Mier, G. (2008) **PROTOCOLOS DE ENRUTAMIENTO RIP, OSPF Y EIGRP.** Universidad Tecnológica De Bolívar Facultad De Ingeniería. Colombia.

Noguera, A. (2019) **Implementación de un sistema de detección de intrusos para Venezolana del Vidrio C.A**. [trabajo para especialización]. Universidad Central de Venezuela.

Palella, Santa; Martins, Feliberto. (2012). **Metodología de la investigación cuantitativa**. (3ra edición) Fondo Editorial de la Universidad Pedagógica Experimental Libertador.

Palella, Santa; Martins, Feliberto. (2006). **Metodología de la investigación cuantitativa**. (1ra reimpresión) Fondo Editorial de la Universidad Pedagógica Experimental Libertador.

Paredes, M., Urbina, W. y Espinosa, N. (2014) **Implementación de un Plan Piloto de Seguridad Bajo de Protocolo IEEE 802.1x para el Departamento de Gestión Tecnológica del Ministerio de Telecomunicaciones**. Escuela Politécnica del Ejército.

Peña, D. (2016) **Diseño e implementación de una red privada virtual (VPN-SSL) utilizando el método de autenticación LDAP en una empresa privada.** [trabajo para especialización]. Universidad Central de Venezuela.

Piloña Ortiz, G. A. (2004). **Guía práctica sobre métodos y técnicas de investigación documental y de campo.** Guatemala, Guatemala: Editores Autores.

Política y objetivos de seguridad. (2021, 14 abril). © IBM Corp. 1999, 2013. Recuperado de: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives

Reglamento de Estudios de Posgrado Conducentes a Títulos Académicos (Resolución No.89-83-791, Universidad Pedagógica Experimental Libertador, Consejo Universitario). (1989, 8 noviembre). Gaceta Universidad Pedagógica Experimental Libertador, Marzo 7, 1990.

Silvera, A. (2022). **Implementación de un sistema de acceso a la red de datos para mejorar el control de acceso de los dispositivos microinformáticos en una empresa de fabricación y comercialización de alimentos de consumo masivo.** [trabajo de grado] Universidad Tecnológica del Perú.

Spamhaus. (2023) **Amenazas en tiempo real a nivel mundial**. Spamhaus Technology. Recuperado de: https://www.spamhaus.com/threat-map/

TACACS. (2011) **The Advantages of TACACS+ for Administrator Authentication.** Recuperado de: https://tacacs.net/wp-content/uploads/2021/10/TACACS_Advantages.pdf

Tamayo y Tamayo, Mario. (2003). **El proceso de la Investigación Científica**. Editorial Limusa, S.A. Grupo Noriega Editores.

Thompson A., Strickland A. (1998) **Administración estratégica**. 18va edición. McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V

Ubicación Avícola La Guásima (2023). Google Maps. https://goo.gl/maps/b8dM86kGDVyNjNWg7

Vargas, A. (2016). **Modelo de Madurez de Seguridad de la Información para el Monitoreo y Análisis del tráfico de redes en la Administración Pública Nacional de Venezuela**. [trabajo de grado para magister]. Universidad Católica Andrés Bello. Repositorio UCAB.

Vieites, A. (2013). **Auditoría de Seguridad Informática.** Edición Original en papel publicada por Editorial RA-MA ISBN.

Westreicher, G (2020, 15 julio). **Recurso.** Recuperado de: Economipedia.com.

APÉNDICE

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

CUADRO TÉCNICO METODOLÓGICO

OBJETIVO GENERAL: Implementar una capa de seguridad en la plataforma CISCO ISE en la empresa Avícola La Guásima, C.A.

OBJETIVO ESPECÍFICO 1	VARIABLE	DIMENSIÓN	INDICADORES	ÍTEMS	FUENTE DE INFORMACIÓN
Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.	Sistema de acceso	Políticas de seguridad	Tipos de políticas	1	Técnica: Entrevista
		Políticas AAA (authentication, authorization, accounting)	Validación	2	
		Medios de acceso a la red	Identificación de dispositivos	3 y 4	
			Tipos de dispositivos conectados	5	

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

INSTRUCCIONES PARA LA GUIA DE ENTREVISTA
• Indique su función dentro de la empresa • Proceda a leer detenidamente cada una de las preguntas • Responda de manera objetiva • En caso de dudas, consulte con la persona encarga de aplicar el cuestionario

N°	Guión de entrevista
1	En la red empresarial, ¿puede usted mencionar las políticas de seguridad en la red y por cuáles medios son implementadas?
2	Desde su experiencia, ¿qué tipos de procesos se utilizan para validar las credenciales de usuarios en la red?
3	¿Qué tipos de métodos se utilizan para identificar los dispositivos conectados?
4	Desde el departamento de telecomunicaciones, ¿cuáles son los métodos que se utilizan para monitorear a los usuarios conectados a la red?
5	En el ámbito de trabajo, ¿puede usted mencionar los diferentes medios para conectarse en la red empresarial?

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTIMADO PROFESOR (A): José Saavedra

Seguidamente se le presenta un guión de entrevista que va dirigido a un panel de expertos de diferentes áreas de trabajo en la Empresa **Avícola La Guásima, C.A.**, ubicada en **Tocuyito, Carabobo**, para un total de tres (03) personas; las respuestas que se obtendrán de la aplicación de este instrumento de recolección de datos van a permitir dar respuesta al objetivo específico número uno (01) de la investigación, que se denomina: **Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.,** de tal manera que permita obtener información de una fuente confiable. Por lo que se solicita a usted de sus buenos oficios para la validación de este instrumento dada su formación académica y experiencia en el ramo industria y académico.

A tal efecto se anexa el cuadro técnico metodológico, el guión de entrevista y el formato de validación.

AUTORA:
Pineda, Yulihannys.
C.I.: 29.727.305.
TUTOR:
Ing. Villarroel, José.
C.I.: 24.193.852

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

VALIDACIÓN DEL INSTRUMENTO (GUIÓN DE LA ENTREVISTA)

Coloque con una (X), en la alternativa que corresponda según opinión sobre los aspectos planteados, anote las observaciones que considere necesario en el recuadro destinado para ello.

Ítems	Redacción de Ítems			Pertinencia de los objetivos		Observaciones
	Clara	Confusa	Tendenciosa	Pertinente	No pertinente	
1	X			V		
2	X			X		
3	X			X		
4	X			X		
5	X			X		
6						
7						
8						
9						
10						

Fecha: 18/01/2023

Firma del Especialista:

Breve descripción del perfil académico del Especialista:	Ingeniero en Computación. Prof. Jose Saavedra.

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTIMADO PROFESOR (A): _____

Seguidamente se le presenta un guión de entrevista que va dirigido a un panel de expertos de diferentes áreas de trabajo en la Empresa **Avícola La Guásima, C.A.**, ubicada en **Tocuyito, Carabobo**, para un total de tres (03) personas; las respuestas que se obtendrán de la aplicación de este instrumento de recolección de datos van a permitir dar respuesta al objetivo específico número uno (01) de la investigación, que se denomina: **Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.,** de tal manera que permita obtener información de una fuente confiable. Por lo que se solicita a usted de sus buenos oficios para la validación de este instrumento dada su formación académica y experiencia en el ramo industria y académico.

A tal efecto se anexa el cuadro técnico metodológico, el guión de entrevista y el formato de validación.

AUTORA:
Pineda, Yulihannys.
C.I.: 29.727.305.
TUTOR:
Ing. Villarroel, José.
C.I.: 24.193.852

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

VALIDACIÓN DEL INSTRUMENTO (GUIÓN DE LA ENTREVISTA)

Coloque con una (X), en la alternativa que corresponda según opinión sobre los aspectos planteados, anote las observaciones que considere necesario en el recuadro destinado para ello.

Ítems	Redacción de Ítems			Pertinencia de los objetivos		Observaciones
	Clara	Confusa	Tendenciosa	Pertinente	No pertinente	
1	X			X		
2	X			X		
3	X			X		
4	X			X		
5	X			X		
6						
7						
8						
9						
10						

Fecha: 19/1/2023

Firma del Especialista:

Breve descripción del perfil académico del Especialista:	El instrumento se puede aplicar

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

ESTIMADO PROFESOR (A): Ana Arenales

Seguidamente se le presenta un guión de entrevista que va dirigido a un panel de expertos de diferentes áreas de trabajo en la Empresa **Avícola La Guásima, C.A.**, ubicada en **Tocuyito, Carabobo**, para un total de tres (03) personas; las respuestas que se obtendrán de la aplicación de este instrumento de recolección de datos van a permitir dar respuesta al objetivo específico número uno (01) de la investigación, que se denomina: **Diagnosticar la situación actual del sistema de acceso a la red empresarial Avícola La Guásima, C.A.,** de tal manera que permita obtener información de una fuente confiable. Por lo que se solicita a usted de sus buenos oficios para la validación de este instrumento dada su formación académica y experiencia en el ramo industria y académico.

A tal efecto se anexa el cuadro técnico metodológico, el guión de entrevista y el formato de validación.

AUTORA:
Pineda, Yulihannys.
C.I.: 29.727.305.
TUTOR:
Ing. Villarroel, José.
C.I.: 24.193.852

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

VALIDACIÓN DEL INSTRUMENTO (GUIÓN DE LA ENTREVISTA)

Coloque con una (X), en la alternativa que corresponda según opinión sobre los aspectos planteados, anote las observaciones que considere necesario en el recuadro destinado para ello.

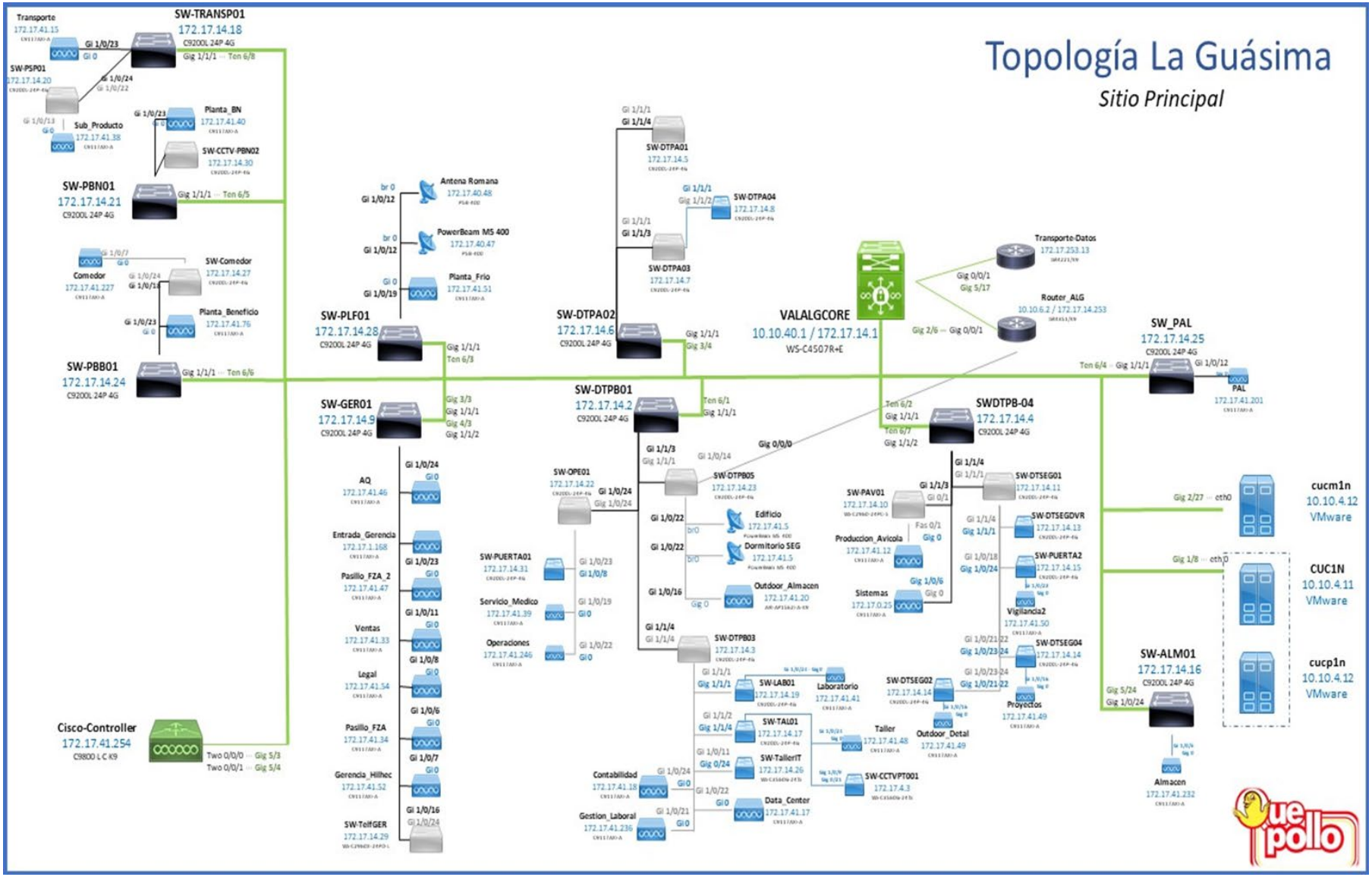
Ítems	Redacción de Ítems			Pertinencia de los objetivos		Observaciones
	Clara	Confusa	Tendenciosa	Pertinente	No pertinente	
1	✓			✓		
2	✓			✓		
3	✓			✓		
4	✓			✓		
5	✓			✓		
6						
7						
8						
9						
10						

Fecha: 20/011 /2023

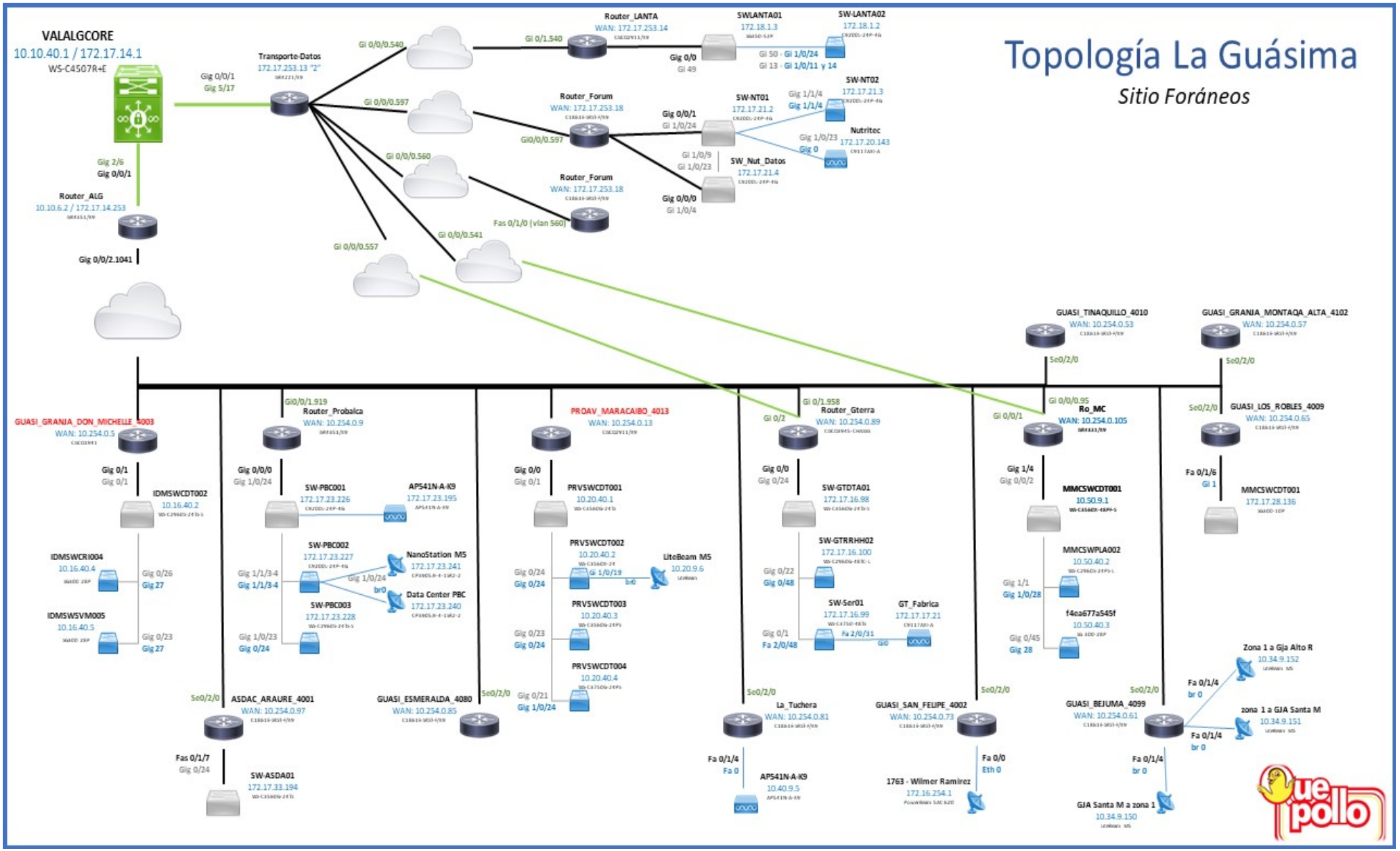
Firma del Especialista:

Breve descripción del perfil académico del Especialista:	Ing. Especialista

ANEXOS


Topología La Guásima
Sitio Principal
Transporte
172.17.41.15
SW-TRANSP01
172.17.14.18
C9200L 24P 4G
SW-PSP01
172.17.14.20
Sub_Producto
172.17.41.38
Planta_BN
172.17.41.40
SW-CCTV-PBN02
172.17.14.30
SW-PBN01
172.17.14.21
C9200L 24P 4G
Comedor
172.17.41.227
SW-Comedor
172.17.14.27
Planta_Beneficio
172.17.41.76
SW-PBB01
172.17.14.24
C9200L 24P 4G
Cisco-Controller
172.17.41.254
C9800 L C K9
Antena Romana
172.17.40.48
PowerBeam M5 400
172.17.40.47
Planta_Frio
172.17.41.51
SW-PLF01
172.17.14.28
C9200L 24P 4G
SW-GER01
172.17.14.9
C9200L 24P 4G
AQ
172.17.41.46
Entrada_Gerencia
172.17.1.168
Pasillo_FZA_2
172.17.41.47
Ventas
172.17.41.33
Legal
172.17.41.54
Pasillo_FZA
172.17.41.34
Gerencia_Hilhec
172.17.41.52
SW-TelfGER
172.17.14.29
SW-DTPA01
172.17.14.5
SW-DTPA04
172.17.14.8
SW-DTPA03
172.17.14.7
SW-DTPA02
172.17.14.6
C9200L 24P 4G
VALALGCORE
10.10.40.1 / 172.17.14.1
WS-C4507R+E
Transporte-Datos
172.17.253.13
Router_ALG
10.10.6.2 / 172.17.14.253
SW_PAL
172.17.14.25
C9200L 24P 4G
PAL
172.17.41.201
SWDTPB-04
172.17.14.4
C9200L 24P 4G
SW-DTPB01
172.17.14.2
C9200L 24P 4G
SW-OPE01
172.17.14.22
SW-DTPB05
172.17.14.23
Edificio
172.17.41.5
Dormitorio SEG
172.17.41.5
Outdoor_Almacen
172.17.41.20
SW-PUERTA01
172.17.14.31
Servicio_Medico
172.17.41.39
Operaciones
172.17.41.246
SW-DTPB03
172.17.14.3
SW-LAB01
172.17.14.19
Laboratorio
172.17.41.41
SW-TAL01
172.17.14.17
Taller
172.17.41.48
SW-TallerIT
172.17.14.26
SW-CCTVPT001
172.17.4.3
Contabilidad
172.17.41.18
Gestion_Laboral
172.17.41.236
Data_Center
172.17.41.17
SW-PAV01
172.17.14.10
Produccion_Avicola
172.17.41.12
Sistemas
172.17.0.25
SW-DTSEG01
172.17.14.11
SW-DTSEGDVR
172.17.14.13
SW-PUERTA2
172.17.14.15
Vigilancia2
172.17.41.50
SW-DTSEG04
172.17.14.14
SW-DTSEG02
172.17.14.14
Proyectos
172.17.41.49
Outdoor_Detal
172.17.41.49
SW-ALM01
172.17.14.16
C9200L 24P 4G
Almacen
172.17.41.232
cucm1n
10.10.4.12
VMware
CUC1N
10.10.4.11
VMware
cucp1n
10.10.4.12
VMware

Anexo A


Topología La Guásima
Sitio Foráneos
VALALGCORE
10.10.40.1 / 172.17.14.1
WS-C4507R+E
Transporte-Datos
172.17.253.13 "2"
Router_ALG
10.10.6.2 / 172.17.14.253
Router_LANTA
WAN: 172.17.253.14
SWLANTA01
172.18.1.3
SW-LANTA02
172.18.1.2
Router_Forum
WAN: 172.17.253.18
SW-NT01
172.17.21.2
SW-NT02
172.17.21.3
Nutritec
172.17.20.143
SW_Nut_Datos
172.17.21.4
Router_Forum
WAN: 172.17.253.18
Fas 0/1/0 (vlan 560)
GUASI_TINAQUILLO_4010
WAN: 10.254.0.53
GUASI_GRANJA_MONTAQA_ALTA_4102
WAN: 10.254.0.57
GUASI_GRANJA_DON_MICHELLE_4003
WAN: 10.254.0.5
IDMSWCDT002
10.16.40.2
IDMSWCRI004
10.16.40.4
IDMSWSVM005
10.16.40.5
Router_Probalca
WAN: 10.254.0.9
SW-PBC001
172.17.23.226
AP541N-A-K9
172.17.23.195
SW-PBC002
172.17.23.227
NanoStation M5
172.17.23.241
Data Center PBC
172.17.23.240
SW-PBC003
172.17.23.228
PROAV_MARACAIBO_4013
WAN: 10.254.0.13
PRVSWCDT001
10.20.40.1
PRVSWCDT002
10.20.40.2
LiteBeam M5
10.20.9.6
PRVSWCDT003
10.20.40.3
PRVSWCDT004
10.20.40.4
Router_Gterra
WAN: 10.254.0.89
SW-GTDTA01
172.17.16.98
SW-GTRRHH02
172.17.16.100
SW-Ser01
172.17.16.99
GT_Fabrica
172.17.17.21
Ro_MC
WAN: 10.254.0.105
MMCSWCDT001
10.50.9.1
MMCSWPLA002
10.50.40.2
f4ea677a545f
10.50.40.3
GUASI_LOS_ROBLES_4009
WAN: 10.254.0.65
MMCSWCDT001
172.17.28.136
ASDAC_ARAURE_4001
WAN: 10.254.0.97
SW-ASDA01
172.17.33.194
GUASI_ESMERALDA_4080
WAN: 10.254.0.85
La_Tuchera
WAN: 10.254.0.81
AP541N-A-K9
10.40.9.5
GUASI_SAN_FELIPE_4002
WAN: 10.254.0.73
1763 - Wilmer Ramirez
172.16.254.1
GUASI_BEJUMA_4099
WAN: 10.254.0.61
Zona 1 a Gja Alto R
10.34.9.152
zona 1 a GJA Santa M
10.34.9.151
GJA Santa M a zona 1
10.34.9.150
que pollo

Anexo B