UPN
UNIVERSIDAD PRIVADA DEL NORTE

FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

IMPLEMENTACIÓN DE CIBERSEGURIDAD EN EL SISTEMA DE CONTROL Y AUTOMATIZACIÓN INDUSTRIAL DENTRO DE LA COMPAÑÍA ELÉCTRICA EL PLATANAL S.A.

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Carlos Joel Melgar Rios

Asesor:

Ing. Eduardo Reyes Rodríguez
https://orcid.org/0000-0003-2050-9616

Lima - Perú

2022

DEDICATORIA

A mi hijo, aunque no lo entiendas ahora yo entendí que seré tu mayor ejemplo

y a mi padre, porque de ti aprendí lo que es la responsabilidad y la disciplina.

AGRADECIMIENTO

A mi esposa, que sin su apoyo no hubiera tenido el tiempo para lograr este trabajo.

A la Jefatura de Mantenimiento de CELEPSA, por confiar en mí en cada uno de los proyectos en mejora de los procesos que gestiona la Gerencia de Operaciones y sobre todo en la que fue nuestra mayor ambición: Diseño e Implementación del Centro de Control CELEPSA.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

Luego de diez años de operación se inició con el proceso de actualización del Sistema SCADA y mejoras en la arquitectura de red industrial de la planta El Platanal. Después del inicio de la pandemia y sumando las restricciones dadas por nuestro gobierno para combatir la pandemia, es donde CELEPSA decide cambiar el proyecto inicial a uno más ambicioso, ahora es centralizar todas las operaciones desde un Centro de Control en Lima.

Este nuevo proyecto consiste en un control remoto de los actuales activos de la empresa distribuidos en el territorio nacional, asegurar y proteger todos los ciberactivos de la nueva red IACS a través del estándar internacional IEC 62443 aplicando contramedidas recomendadas; segregación y segmentación de las redes IACS.

Después del cierre del proyecto y con la puesta en operación del Centro de Control CELEPSA, logramos segregar, segmentar las redes IACS y la gestión remota de sus ciberactivos. Por lo tanto, se ha logrado ampliar las capas de ciberseguridad de los ciberactivos y su gestión remota la nueva red IACS.

Las actividades de contramedida no hubieran sido posible sin tener los conocimientos adquiridos en los más de trece años de experiencia dentro de CELEPSA, además de haber obtenido las competencias profesionales en infraestructura de red, ciberseguridad y protocolos de comunicación dentro del ámbito industrial.

CAPÍTULO I. INTRODUCCIÓN

1.1. CONTEXTO

El presente trabajo que presento con el título "Implementación de Ciberseguridad en el Sistemas de Control y Automatización Industrial dentro de la Compañía Eléctrica El Platanal S.A.", describe el proceso de implementación de las medidas para proteger el Sistema de Control y Automatización Industrial de la Compañía Eléctrica El Platanal S.A. dentro de las operaciones remotas del Centro de Control, trabajo que lo presento como Especialista SCADA y Redes Industriales dentro de la misma compañía.

Luego de diez años de operación de forma local, en el 2020 iniciamos con el proceso de actualizar el Sistema Supervisión Control y Adquisición de Datos (SCADA) y la arquitectura de red de los sistemas de control y automatización industrial para la planta de EL Platanal, sumando a esto las medidas efectuadas por nuestro gobierno central para combatir la pandemia del Coronavirus(COVID-19) tales como restringir el libre tránsito dentro del territorio nacional, prohibir la concentración de personas, el distanciamiento social, cuarentena y el uso obligatorio de mascarillas, es donde la Gerencia de Operaciones decide hacer un cambio en el modelo del proyecto y centralizar todas las operaciones desde un Centro de Control en la oficina principal de la compañía.

1.2. LA EMPRESA

Compañía Eléctrica El Platanal S.A. (CELEPSA), es una empresa constituida en el 2005, con capital íntegramente peruano el corporativo Unión Andina de Cementos S.A. (UNACEM). El objeto social principal de CELEPSA es la generación, y comercialización de energía eléctrica, gestionando el recurso hibrido de manera sustentable y responsable, inyectando al Sistema Eléctrico Interconectado Nacional (SEIN) y distribuida en el mercado eléctrico peruano, teniendo una potencia instalada que asciende a 242 MW al 2022.

1.3. QUE PRODUCIMOS

Toda la energía generada es inyectada al SEIN, que es el conjunto de generadoras, líneas de transmisión y sistemas distribución conectados entre sí; el cual permite la transferencia de energía eléctrica entre los diversos subsistemas eléctricos del Perú. El SEIN es abastecido por un parque de generación conformado por centrales hidráulicas, centrales térmicas y centrales de Recursos Energéticos Renovables (RER) tales como eólicas, fotovoltaicas e hidroeléctricas con capacidad menor a 20 MW.

Los clientes de CELEPSA también están conectados al SEIN y están divididos en dos grupos.

1.3.1. CLIENTES REGULADOS

Cuyos precios son fijados por la autoridad, en este caso el estado. Siendo sus clientes; UNACEM, mineras y plantas de producción.

1.3.2. CLIENTES LIBRES

A los que se les supone capacidad negociadora y la posibilidad de proveerse de electricidad de otras formas, tales como la autogeneración o el suministro directo desde empresas generadoras. Siendo sus clientes; distribuidores de energía.

1.4. MISIÓN Y VISIÓN

1.4.1. MISIÓN

El valor que la empresa añade a todos los grupos de interés, mediante la gestión y el desarrollo de activos e infraestructura energética

1.4.2. VISIÓN

Es ser referente en el sector energético, de excelencia en a la gestión económica, técnica, ambiental y social.

1.5. VALORES ESENCIALES

Nuestros valores nos impulsan a la búsqueda de la excelencia y transparencia en los procesos, y renuevan constantemente nuestra motivación para asumir retos mayores.

1.5.1. INTEGRIDAD

Somos un equipo de profesionales ético, honesto e inclusivo que trabaja con transparencia y cero tolerancias al soborno, la corrupción, la discriminación y cualquier práctica anticompetitiva.

1.5.2. COMPROMISO

Trabajamos con pasión y satisfacción; asumimos la responsabilidad de nuestras decisiones, acciones y resultados.

1.5.3. EXCELENCIA

Trabajamos siempre con calidad, eficiencia e innovación para que nuestro desempeño supere las expectativas de nuestros grupos de interés.

1.6. VALORES DE NEGOCIO

1.6.1. SEGURIDAD Y SALUD

Porque la vida es primero, garantizamos un ambiente seguro y saludable con el liderazgo y compromiso de todos.

1.6.2. SOSTENIBILIDAD

Creamos valor económico, social y ambiental, para construir un mundo en el que nosotros y las futuras generaciones podamos vivir mejor.

1.6.3. ORIENTACION AL CLIENTE

Servimos con pasión a nuestros clientes para que superen con creces sus objetivos.

1.7. ACTIVOS DE LA COMPAÑÍA

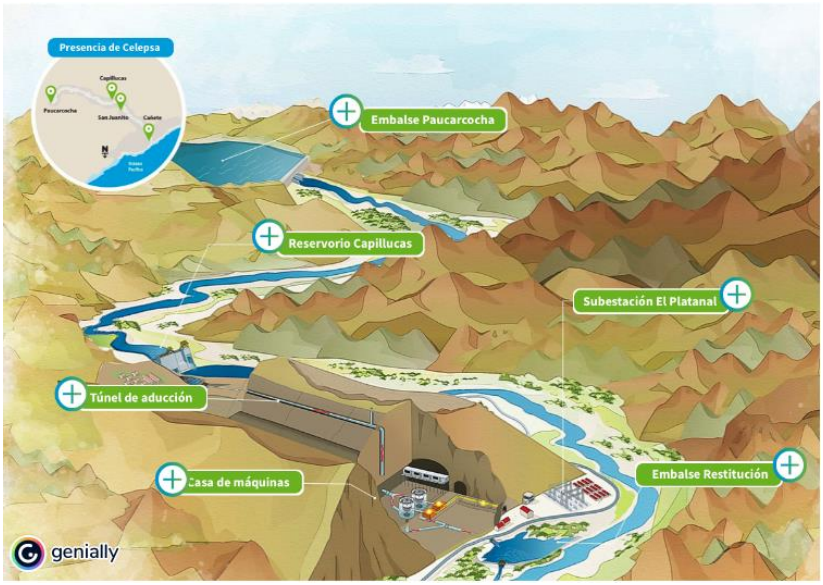
1.7.1. CENTRAL HIDROELÉCTRICA EL PLATANAL

La Central Hidroeléctrica El Platanal (EP), en su principal y primer activo de CELEPSA, con una potencia de generación de 220 MW desde el año 2010, con un aumento de potencia a 222 MW en el 2021, y se ubica en la cuenca del río Cañete, en las provincias de Yauyos y Cañete en el departamento de Lima.

Además, cuenta con las presas de regulación; Capillucas, en el km 95 de la carreta Cañete-Yauyos y Paucarcocha en la laguna con el mismo nombre, en el departamento de Lima.

Figura 1

Infografía de las áreas operativas de la Central Hidroeléctrica El Platanal.



Fuente: Pagina web de CELEPSA

1.7.2. CENTRAL HIDROELÉCTRICA MARAÑON

El segundo activo es la Central Hidroeléctrica Marañón (HM), cumple con el estándar de energía renovable (menor a 20 MW de potencia de generación), aprovecha las aguas del río Marañón, en la provincia de Huamalíes en el Departamento de Huánuco.

Figura 2

Toma aérea de la Central Hidroeléctrica Marañón

Fuente: Pagina web de CELEPSA

1.7.3. CENTRO DE CONTROL CELEPSA (CCC)

Es el último activo de CELEPSA, inaugurado el 18 de junio del 2021 es una moderna plataforma industrial desde la que se monitorea y gestiona de forma remota, en tiempo real, la operación de las centrales hidroeléctricas El Platanal y Marañón, además del despacho económico diario en coordinación con el COES y el servicio a todos sus clientes.

Figura 3

Tomas fotográficas del Centro de Control CELEPSA en Lima.

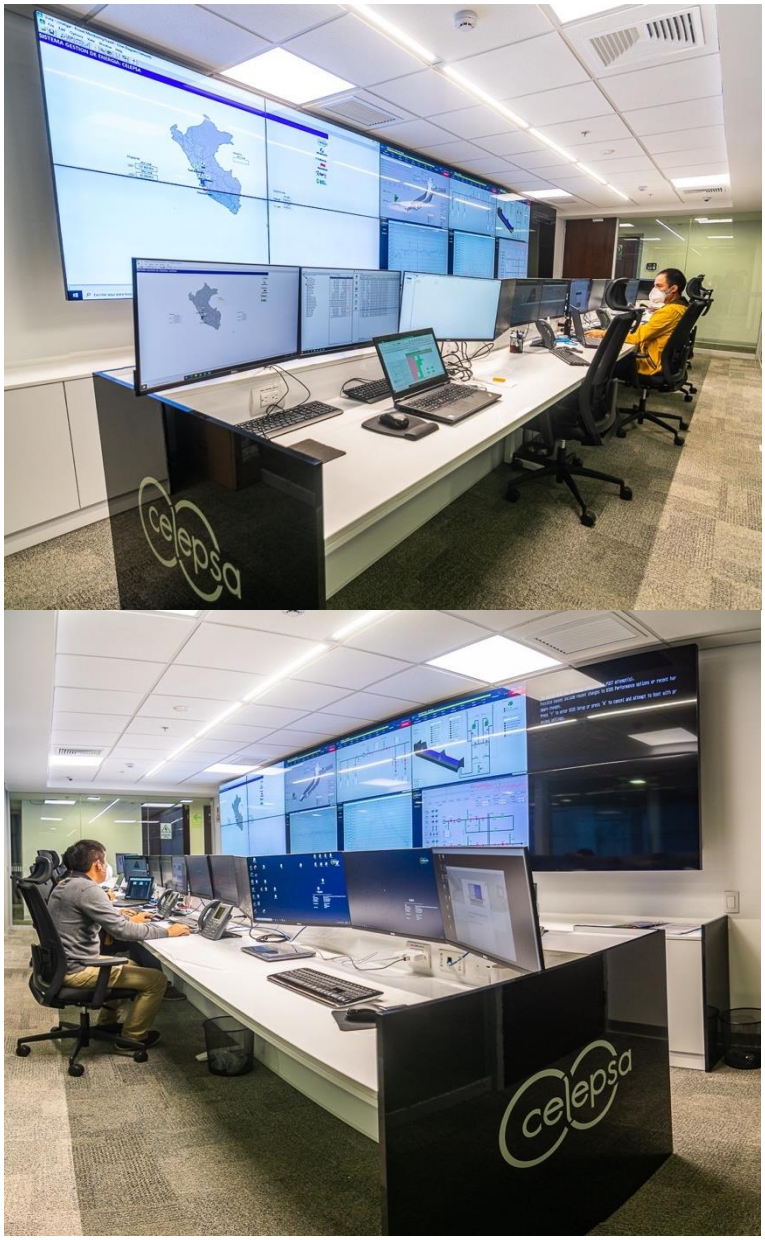


Imagen del CCC con los coordinadores durante las pruebas funcionales.

Fuente: Diseño propio

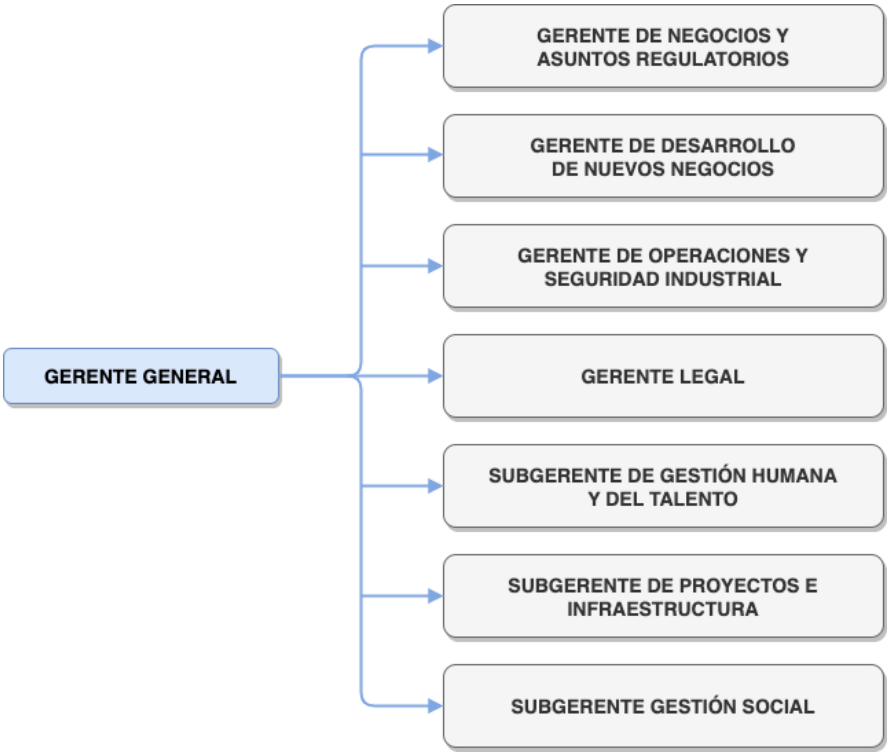
1.8. ORGANIGRAMA

1.8.1. COMITÉ EJECUTIVO

El organigrama del comité ejecutivo de CELEPSA, el cual está conformado por los Gerentes y Subgerente.

Figura 4

En este nivel se toman las decisiones para el buen operar de CELEPSA.



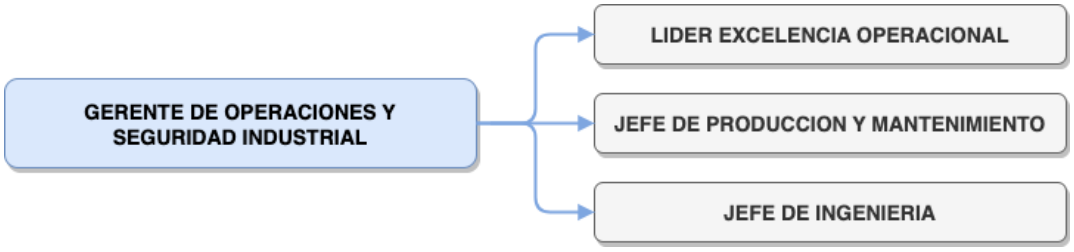
Fuente: Diseño propio

1.8.2. GERENCIA DE OPERACIONES Y SEGURIDAD INDUSTRIAL

Es el gobierno de las operaciones, mantenimiento y la seguridad industrial de la compañía, las “operaciones” es considerado el “negocio” de la compañía.

Figura 5

Organigrama de Producción y Mantenimiento dentro de GOP.



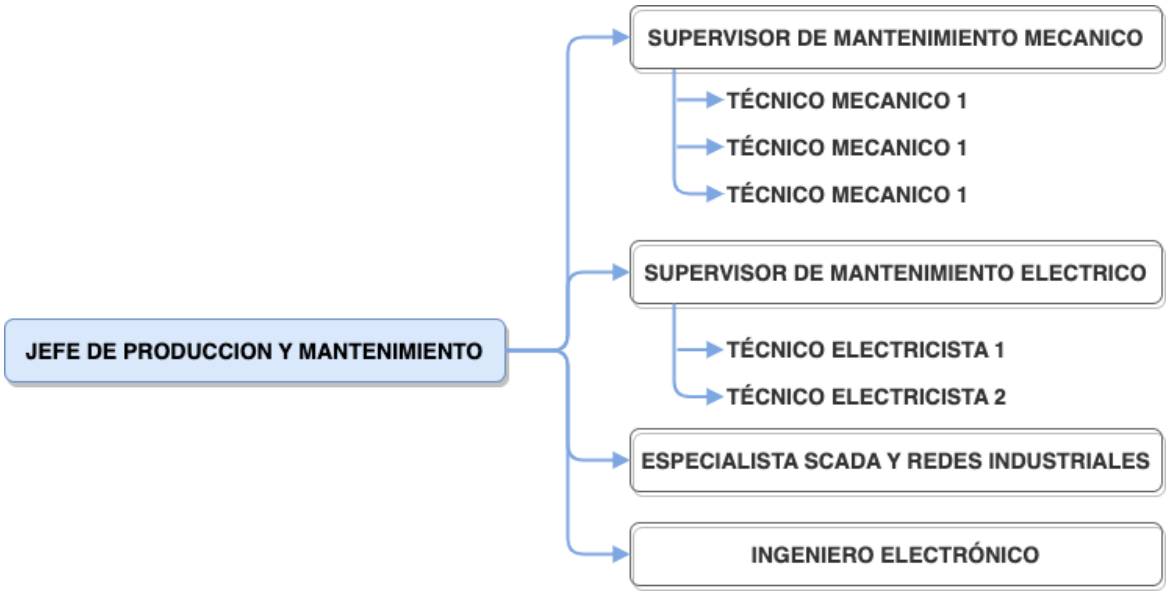
Fuente: Diseño propio

1.8.3. JEFATURA DE PRODUCCION Y MANTENIMIENTO

A este nivel de gobierno se lleva la gestión de la producción y el mantenimiento de las dos operaciones EP y HM.

Figura 6

Organigrama de Jefatura de Producción y Mantenimiento.



Fuente: Diseño propio

1.9. ESPECIALISTA SCADA Y REDES INDUSTRIALES

Mi ingreso a CELEPSA fue en mayo del 2009, en plena construcción de EP dentro de la Gerencia de Operaciones y en el área de Mantenimiento, como Asistente de Automatización, Control y Comunicaciones.

Dejaba mi primer trabajo en una empresa minera con conocimientos en procesos industriales distintos al de mi nuevo puesto y teniendo la carrera técnica de Ingeniería Electrónica, pero con conocimientos de tecnología para sistemas computacionales similares.

Ya tengo más de trece años en CELEPSA, actualmente tengo el puesto de Especialista SCADA y Redes Industriales, dirijo e implemento los proyectos de IACS dentro de la GOP y en estos años transcurridos he logrado obtener el bachiller en Ingeniería de Sistemas de Computaciones, capacitarme en cursos de configuración de PLC, Sistema SCADA de Siemens, sistemas de protección eléctrica, protocolos de comunicación industrial, normas de comunicación para sistemas eléctricos como son: IEC-61850, IEC

60870-5-104 y DNP3, infraestructura de red como el CCNA de Cisco , ciberseguridad para Tecnología de la Información (TI) como Cybersecurity Operations v1.1 de Cisco, aspirante a la Certificación 1: ISA99/IEC 62443 Cybersecurity Fundamentals Specialist, y finalmente un Diplomado en Ciberseguridad y Ciberdefensa en el Centro de Altos Estudios Nacionales (CAEN).

Algo que puedo decir es; loque fusionar mi carrera técnica de ingeniera electrónica con la carrera de ingeniería de sistemas computacionales en el rubro industrial.

Figura 7

Imagen mía en la SSEE El Platanal en el 2010.

Fuente: Diseño propio

CAPÍTULO II. MARCO TEÓRICO

Antes de iniciar el marco de trabajo efectuado es bueno entender algunos conceptos básicos y sobre todo entender la diferencia entre los sistemas de TI y IACS.

2.1. CONCEPTOS BASICOS DE INFORMATICA Y CIBERSEGURIDAD

2.1.1. SEGURIDAD

Se refiere a la capacidad de proteger algo de varias amenazas". (Gunter, Medoff, & O'Brien, 2018).

2.1.2. CIBERSEGURIDAD

Definida como las medidas tomadas para proteger una computadora o sistemas informático contra accesos no autorizados o ataques". (IEC/TS 62443-1-1, 2009).

Prevención de daños, protección y restauración de computadoras, sistemas de comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicaciones por cable y comunicaciones electrónicas, incluida la información contenida en ellos, para garantizar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. (NIST SP 800-53 Rev5, 2020).

2.1.3. TECNOLOGÍA DE LA INFORMACION

Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (El Congreso de Colombia, 2009).

2.1.4. CODIGO MALISIOSO

Programas o códigos escritos con el fin de recopilar información sobre sistemas o usuarios, destruir datos del sistema, proporcionar un punto de apoyo para una mayor intrusión en el sistema, falsificar datos e informes del sistema, o proporcionar molestias que consumen mucho tiempo al personal de operaciones y mantenimiento del sistema. (ISA 62443-1-2, 2018)

2.1.5. AMENAZA

Circunstancia o evento con el potencial de afectar adversamente la operación (incluyendo misión, funciones, imagen o reputación), activos, sistema de control o individuo a través de acceso no autorizado, destrucción, divulgación, modificación de datos y/o denegación de servicio. (ISA 62443-1-2, 2018).

2.1.6. RIESGO

Expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad particular con una consecuencia particular. (ISA 62443-1-2, 2018)

2.1.7. VULNERABILIDAD

Falla o debilidad en el diseño, implementación u operación y administración de los sistemas que podría explotarse para violar la política de integridad y seguridad del sistema. (ISA 62443-1-2, 2018)

2.1.8. SEGURIDAD DE LA INFORMACION

La seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información. La seguridad de la información implica la aplicación y gestión de controles apropiados que implican la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito y la continuidad del negocio sostenido, y minimizar las consecuencias de los incidentes de seguridad de la información. (ISO 27001, 2018).

2.1.8.1. CONFIDENCIALIDAD

Propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. (ISO 27001, 2018)

2.1.8.2. INTEGRIDAD

Propiedad de exactitud y completitud. (ISO 27001, 2018)

2.1.8.3. DISPONIBILIDAD

Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (ISO 27001, 2018)

2.2. STANDARES DE CIBERSEGURIDAD MAS RECONOCIDOS

2.2.1. NERC-CIP

North American Electric Reliability Corporation (NERC) es una autoridad reguladora internacional sin fines de lucro cuya misión es garantizar la confiabilidad del sistema de energía a granel en América del Norte. NERC desarrolla y hace cumplir los estándares de confiabilidad; evalúa anualmente la confiabilidad estacional ya largo plazo; monitorea el sistema de energía a granel a través del conocimiento del sistema; y educa, capacita y certifica al personal de la industria. El área de responsabilidad de NERC abarca los Estados Unidos continentales, Canadá y la parte norte de Baja California, México. NERC es la organización de confiabilidad eléctrica (ERO) para América del Norte, sujeta a la supervisión de la Comisión Federal de Regulación de Energía (FERC) y las autoridades gubernamentales de Canadá. La jurisdicción de NERC incluye usuarios, propietarios y operadores del sistema de energía a granel. (CISA, 2016).

Los estándares de protección de infraestructura crítica (CIP) de NERC proporcionan un conjunto de requisitos y consideraciones para proteger los activos del sistema de energía a granel, pero también son aplicables a otras industrias como mejores prácticas para proteger ICS. (CISA, 2016).

2.2.2. FRAMEWORK NIST ICS

El NIST publicó la primera versión del "Marco para mejorar la ciberseguridad de la infraestructura crítica" el 12 de febrero de 2014. El marco, creado a través de la colaboración entre la industria y el gobierno, consta de estándares, pautas y prácticas para promover la protección de la infraestructura crítica. El enfoque priorizado, flexible, repetible y rentable del marco ayuda a los propietarios y operadores de infraestructura crítica a gestionar mejor los riesgos relacionados con la cibernética. (CISA, 2016).

El marco NIST ICS proporciona un conjunto integral de recomendaciones para asegurar ICS. Las organizaciones pueden usarlo solo o junto con otros estándares NIST,

como su serie de publicaciones especiales (SP), en particular: NIST SP 800-82, “Guía para la seguridad de los sistemas de control industrial (ICS)”. (CISA, 2016).

2.2.3. IEC 62443

El estándar esencial de ciberseguridad en los sistemas de automatización se presenta en el conjunto de estándares, especificaciones e informes técnicos de ciberseguridad IEC 62443. Estos estándares brindan una visión completa de la seguridad cibernética y especifican los conceptos generales, la terminología y las métricas de cumplimiento necesarias para analizar significativamente la seguridad cibernética. Además, brindan instrucciones detalladas para diseñar políticas y procedimientos para desarrollar un enfoque de toda la organización para administrar la seguridad cibernética. Después de describir las políticas centrales de ciberseguridad, el conjunto estándar especifica los requisitos del sistema, incluidas las tecnologías de seguridad requeridas, los niveles de garantía de seguridad para zonas y conductos, y los requisitos de seguridad del sistema y los niveles de garantía de seguridad. (Gunter, Medoff, & O'Brien, 2018).

2.3. CONCEPTOS BASICOS DE CIBERSEGURIDAD EN LA INDUSTRIA

2.3.1. CIBERACTIVO

Dispositivo contenido en el sistema bajo consideración (SUC),eje.: controlador, servidor, estación de ingeniera, etc. (Gunter, Medoff, & O'Brien, 2018).

2.3.2. SISTEMAS DE CONTROL Y AUTOMATIZACION INDUSTRIAL

Colección de personas, hardware, software y políticas involucradas en la operación del proceso industrial y que puede afectar o influir en una operación segura y confiable. (IEC/TS 62443-1-1, 2009)

2.3.3. IACS CYBERSECURITY

Prevención de interferencias intencionales o no intencionales con el correcto funcionamiento de sistemas de control y automatización industrial utilizando computadoras, redes sistemas operativos, aplicaciones. (Gunter, Medoff, & O'Brien, 2018).

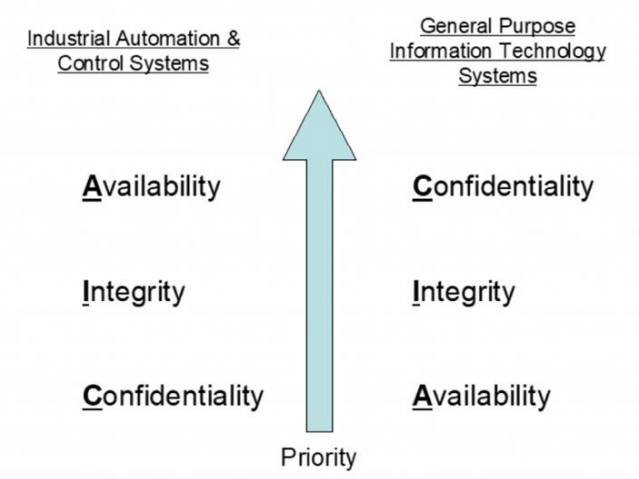
2.4. OBJETIVOS DE CIBERSEGURIDAD TI/IACS

Seguridad de la información tradicionalmente se ha enfocado en lograr los objetivos, confidencialidad, integridad y disponibilidad, que son a menudo abreviado con el acrónico “CIA”. Una estrategia de seguridad de la tecnología de la información para los típicos "back office" o sistemas comerciales puede centrarse principalmente en la confidencialidad y el control de acceso necesario para lograrlo. La integridad podría pasar a la segunda prioridad, que está disponible como la más baja. (IEC/TS 62443-1-1, 2009).

En ambientes IACS, la prioridad general de los objetivos es a menudo diferente, La seguridad en estos sistemas se ocupa principalmente de mantener la disponibilidad de todos los componentes del sistema. La seguridad en estos sistemas se ocupa principalmente de mantener la disponibilidad de todos los componentes del sistema. Son riesgos inherentes asociados con la maquinaria industrial que está controlada, monitoreada o afectada de otra manera por IACS. Por lo tanto, la integridad suele ser la segunda en importancia. Por lo general, la confidencialidad es de menor importancia, porque a menudo los datos están en bruto y deben analizarse en contexto para que tengan algún valor. (IEC/TS 62443-1-1, 2009).

Figura 8

Comparación los objetivos de IACS y TI.



Fuente: (IEC/TS 62443-1-1, 2009).

2.4.1. FUNDAMENTOS DEL DISEÑO: SIETE ATRIBUTOS FUNDAMENTALES

El simple modelo CIA mostrado en la Figura 8 no es adecuado para un mejor entendimiento de los requerimientos para seguridad IACS, existen varios requisitos básicos o fundamentales que se han identificado para la seguridad de la automatización industrial. (IEC/TS 62443-1-1, 2009), y estos son:

1. Control de acceso (AC),

   Control del acceso a dispositivos seleccionados, información o ambos para proteger contra la interrogación no autorizada del dispositivo o la información. (IEC/TS 62443-1-1, 2009).

2. Control de uso (UC),

   Controle el uso de la información del dispositivo seleccionado o ambos para proteger contra la operación no autorizada del dispositivo o la información. (IEC/TS 62443-1-1, 2009).

3. Integridad de datos (DI),

   Garantiza la integridad de los datos en canales de comunicación seleccionados para proteger contra cambios no autorizados. (IEC/TS 62443-1-1, 2009).

4. Confidencialidad de datos (DC),

   Garantiza la confidencialidad de los datos en canales de comunicación seleccionados para proteger contra escuchas. (IEC/TS 62443-1-1, 2009).

5. Restringir flujo de datos (DRF),

   Restringe el flujo de datos en los canales de comunicación para proteger contra la publicación de información a fuentes no autorizadas. (IEC/TS 62443-1-1, 2009).

6. Restrinja el flujo de datos (TRE),

   Responda a la violación de seguridad notificando a la autoridad correspondiente, informando la evidencia forense necesaria de la violación y

tomando automáticamente las medidas correctivas oportunas en medio de una situación crítica o de seguridad crítica. (IEC/TS 62443-1-1, 2009).

7. Disponibilidad de recursos (RA).

   Garantizar la disponibilidad de todos los recursos de la red para protegerse contra ataques de denegación de servicios. (IEC/TS 62443-1-1, 2009).

2.4.2. DEFENSE IN DEPTH

Por lo general, no es posible lograr los objetivos de seguridad mediante el uso de una sola contramedida o técnica. Un enfoque superior es utilizar el concepto de defensa en profundidad, lo que implica la aplicación de múltiples contramedidas en capas o paso a paso. Por ejemplo, los sistemas de detección de intrusos se pueden utilizar para señalar la penetración de un cortafuegos. (IEC/TS 62443-1-1, 2009).

La defensa en profundidad como concepto se originó en la estrategia militar para proporcionar barreras para impedir que los intrusos alcancen sus objetivos mientras se monitorea su progreso y se desarrollan e implementan respuestas al incidente para repelerlos. En el paradigma de la seguridad cibernética, la Defensa en profundidad se correlaciona con medidas de detección y protección diseñadas para impedir el progreso de un intruso cibernético mientras permite que una organización detecte y responda a la intrusión con el objetivo de reducir y mitigar las consecuencias de una infracción. (CISA, 2016)

2.5. CIBERSEGURIDAD EN IACS VS SISTEMAS TI

El standard dominante in la seguridad TI es el ISO/IEC 27002:2006 (antes 17799:2000), Information technology – Security Techniques – Code of practice for information security management, cual es un completo catalogo general de prácticas de seguridad para administración de riesgos de ciberseguridad. (Gunter, Medoff, & O'Brien, 2018).

Desafortunadamente, las prácticas de seguridad diseñadas para el mundo de TI no siempre se transfieren al sistema de control. Mientras que las interrupciones ocasionales son

comunes y toleradas en los sistemas comerciales, se espera que los sistemas de control funcionen durante años sin interrupción. Del mismo modo, la tradición de probar la versión beta de nuevos productos de TI en el campo y recuperarse de los problemas mediante el simple reinicio de los servidores o el cambio contrasta fuertemente con las prácticas de control estándar. Esto no es sorprendente, ya que el impacto de las interrupciones en los sistemas comerciales suele ser la pérdida de datos, mientras que las interrupciones en el entorno de proceso darán como resultado la pérdida de operaciones y producción y pueden causar daños al equipo y al medio ambiente, o incluso enfermedades, lesiones o muerte. (Gunter, Medoff, & O'Brien, 2018).

Comprender las diferencias en las consecuencias para TI y los sistemas de control es la clave para adaptar las políticas de seguridad del sector de TI a los sistemas de control, así como para comprender las implicaciones generales del riesgo en el entorno de control industrial. La cultura de seguridad de TI y las tecnologías que ha creado se basan en la idea de que el rendimiento y la confidencialidad son primordiales y las interrupciones, aunque indeseables, son aceptables. Esto claramente no es cierto para el mundo industrial, donde la necesidad de disponibilidad e integridad de un sistema típicamente dominan todas las demás consideraciones. (Gunter, Medoff, & O'Brien, 2018).

Al aplicar la protección de defensa en profundidad a ICS, se debe tener en cuenta que existen varias diferencias clave entre los entornos de TI tradicionales y los entornos de sistemas de control en relación con la seguridad. La Figura 9 muestra algunos de los temas de seguridad más destacados comunes a la función de seguridad de una organización y describe cómo abordarlos en los dominios de TI en comparación con las arquitecturas que ejecutan ICS. (CISA, 2016).

Figura 9

Temas de seguridad a la función de ciberseguridad.

Security Topic	Information Technology (IT)	Control Systems (ICS)
Anti-virus and Mobile Code	Very common; easily deployed and updated. Users have control over customization and can be asset-based or enterprise-based	Memory requirements can impact on ICS; organizations can only protect legacy systems with after-market solutions; usually requires "exclusion" folders to avoid programs quarantining critical files
Patch Management	Easily defined; enterprise-wide; remote and automated	Long timeline to successful patch installation; OEM-specific; may "break" ICS functionality; asset owners required to define acceptable risk
Technology Support Lifetime	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; usually same vendor over time; product end-of-life creates new security concerns
Testing and Audit Methods	Use modern methods; systems usually resilient and robust to handle assessment methods	Tune testing to the system; modern methods can be inappropriate; equipment may be susceptible to failure during testing
Change Management	Regular and scheduled; aligned with minimum-use periods	Strategic scheduling; nontrivial process due to impact on production
Asset Classification	Common and performed annually; results drive expenditure	Only performed when obligated; accurate inventories uncommon for nonvital assets; disconnect between asset value and appropriate countermeasures
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Focused on system resumption activities; forensics procedures immature (beyond event re-creation); requires good IT/ICS relationships
Physical and Environmental Security	Can range from poor (office systems to excellent (critical IT operations systems)	Usually excellent for critical areas, maturity varies for site facilities based on criticality/culture
Secure Systems Development	Integral part of development process	Historically not an integral part of development process; vendors are maturing but at slower rate than IT; core/flagship ICS solutions difficult to retrofit with security
Security Compliance	Definitive regulatory oversight depending on sector (and not all sectors)	Specific regulatory guidance depending on sector (and not all sectors)

Fuente: (CISA, 2016).

2.5.1. DIFERENTES REQUISITOS

- Los problemas ocurren porque las suposiciones que son válidas en un entorno de TI pueden no ser válidas en la planta. (IEC/TS 62443-1-1, 2009).
- La seguridad cibernética de IACS debe abordar los problemas de seguridad, lo que no suele ser un problema con la seguridad cibernética de TI convencional. (IEC/TS 62443-1-1, 2009).

Tabla 1

Diferentes requisitos de rendimiento

TI	IACS
La respuesta debe ser confiable	La respuesta es crítica en el tiempo
Alto rendimiento	Rendimiento normal
Alto retardo y jitter tolerado	Alto retraso una preocupación seria
Interacción de emergencia menos crítica	Respuesta a emergencias es crítica
Protocolos TI	TI y Protocolos Industriales

El rendimiento en los IACS no es prioridad.

Fuente: (IEC/TS 62443-1-1, 2009)

Tabla 2

Diferentes requisitos de disponibilidad

TI	IACS
Operación programada	Operación continua
Fallas ocasionales toleradas	Fallas intolerables
Reinicio tolerable	Reiniciar puede no ser tolerable
Prueba beta en el campo aceptable	Pruebas exhaustivas de control de calidad en un entorno que no sea de producción
Modificación posible con poco papeleo	Posible que se requiera una certificación formal después de cualquier cambio

La disponibilidad es crítica y libre de fallas, una falla puede ocasionar parada de producción.

Fuente: (IEC/TS 62443-1-1, 2009)

Tabla 3

Diferentes requisitos entorno operativos

TI	IACS
Aplicaciones típicas de oficina.	Operación programada
Estándar sistemas operativos.	Estándar y embebidos sistemas operativos.
Actualizaciones son sencillas.	las actualizaciones son desafiantes y pueden afectar el hardware, la lógica y los gráficos
La tecnología se actualiza a menudo comercial y lista para usar.	Sistemas heredados
Recursos abundantes.	Recursos limitados
Centro de datos, sala de servidores o entorno de oficina	Ambiente industrial

Los IACS emplean firmware o sistemas embebidos de más diferentes marcas

Fuente: (IEC/TS 62443-1-1, 2009)

Tabla 4

Diferentes objetivos de gestión de riesgos

TI	IACS
la confidencialidad e integridad de los datos son primordiales	recuperar reiniciando
el impacto del riesgo es la pérdida de datos, el retraso de la operación comercial	el impacto del riesgo es la pérdida de vidas, equipos o productos
recuperar reiniciando	tolerancia a fallos secuencial

Por ejemplo, el bloque de la pantalla del computador es normal para los sistemas de TI, para los IACS esto es crítico imaginando que por alguna razón el operador las credenciales.

Fuente: (IEC/TS 62443-1-1, 2009).

2.5.2. ABORDANDO LAS DIFERENCIAS

- No deseche todas las tecnologías y prácticas de seguridad de TI y comience desde cero. (IEC/TS 62443-1-1, 2009)
- Explore las tecnologías de seguridad y practique, pero modifíquelas y aprenda a usarlas correctamente en IACS. (IEC/TS 62443-1-1, 2009)
    - IACS utiliza tecnologías TI como Windows, TCP/IP y Ethernet. (IEC/TS 62443-1-1, 2009)
    - Gran parte de la política y la tecnología de TI funcionarán para los sistemas de control. (IEC/TS 62443-1-1, 2009).
    - El entorno de TI no se ocupa de la seguridad, solo de la seguridad. (IEC/TS 62443-1-1, 2009)
- Desarrolle una comprensión clara de cómo las suposiciones y necesidades de IACS difieren de las del entorno de TI. (IEC/TS 62443-1-1, 2009)
    - Identificar y abordar el 10% que difiere desde el principio. (IEC/TS 62443-1-1, 2009).
    - Orientación de seguridad AIC versus CIA. (IEC/TS 62443-1-1, 2009).

2.6. MODELOS PARA REDES DE CONTROL

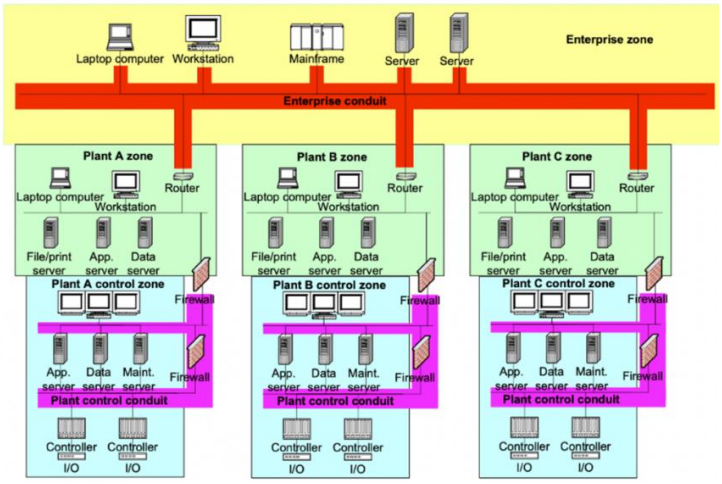
Empleamos esto para una mayor visualización y entendimiento de las redes industriales.

2.6.1. ZONAS Y CONDUCTOS

Un diagrama de zonas y conductos detalla cada componente de una red de control, y todas sus conexiones. Una zona representa una agrupación de activos lógicos o físicos que comparten requisitos de seguridad comunes. Se deben realizar requisitos de seguridad para proteger a cada usuario dentro de la zona y lograr un nivel de seguridad adecuado para la aplicación. Las conexiones entre las zonas se denominan conductos. (Gunter, Medoff, & O'Brien, 2018).

Figura 10

Modelo Zonas y Conductos



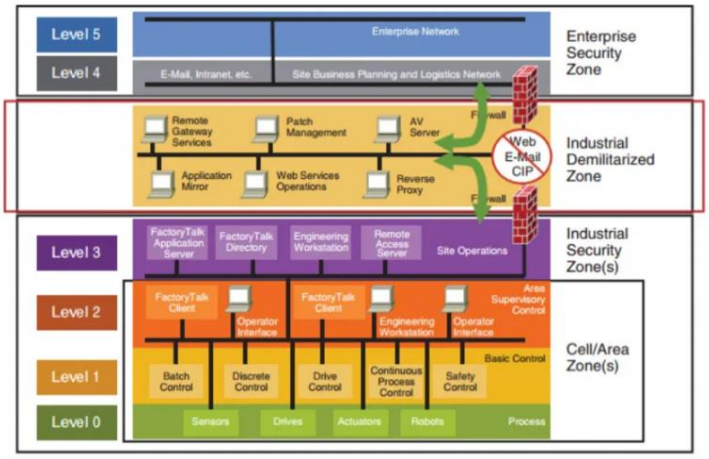
Fuente: (IEC/TS 62443-1-1, 2009)

2.6.2. REFERENCIA PURDUE

El Modelo de Referencia Purdue para fabricas integradas por computadora se utiliza para comprender mejor las redes informáticas al segmentarlas en niveles que van desde el nivel 0 hasta el nivel 5. (Gunter, Medoff, & O'Brien, 2018).

Figura 11

Modelo de referencia Purdue



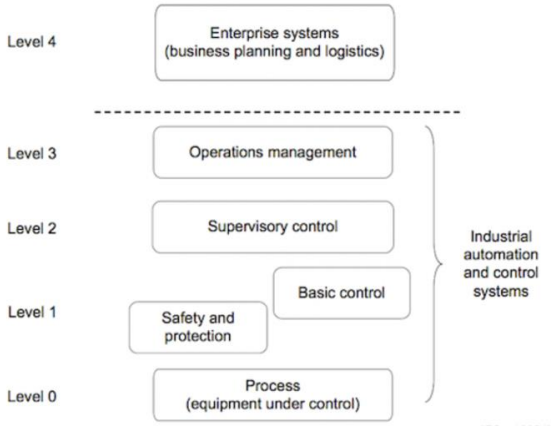
Fuente: (Gunter, Medoff, & O'Brien, 2018)

2.6.3. REFERENCIA ISA 99 STANDARDS

Este es como un Modelo Purdue en que separa la red de control en niveles, sin embargo, él se lleva a cabo de manera diferente en los modelos. Además, el modelo de

referencia presta especial atención a qué nivel comprende el IACS, y es un enfoque útil para comprender los diferentes niveles dentro del sistema de control.

Figura 12
Modelo de referencia ISA 99

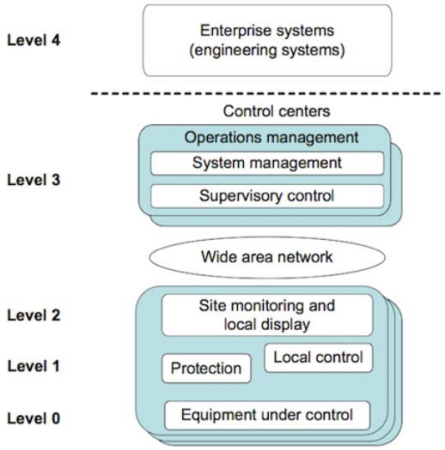


Fuente: (IEC/TS 62443-1-1, 2009)

2.6.4. REFERENCIA SCADA

Se puede usar una vista ligeramente diferente del modelo de referencia para las aplicaciones SCADA. (IEC/TS 62443-1-1, 2009)

Figura 13
Modelo de referencia SCADA.



Fuente: (IEC/TS 62443-1-1, 2009)

2.7. ABORDANDO LOS EQUIPOS DE RED

2.7.1.1. SWITCH

Son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red

dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí. (Cisco, 2022).

2.7.1.2. ROUTERS

Un router recibe y envía datos en redes informáticas. Los routers a veces se confunden con los concentradores de red, los módems o los switches de red. No obstante, los routers pueden combinar las funciones de estos componentes y conectarse con estos componentes para mejorar el acceso a Internet o ayudar a crear redes empresariales. (Cisco, 2022).

2.8. ARQUITECTURA DE RED

2.8.1. AQUITECTURA LAN

Una red de área local (LAN) es una colección de dispositivos conectados entre sí en una ubicación física, como un edificio, una oficina o un hogar. Una LAN puede ser pequeña o grande, desde una red doméstica con un usuario hasta una red empresarial con miles de usuarios y dispositivos en una oficina o escuela. (Cisco, 2022)

2.8.2. AQUITECTURA WAN

Una parte de una red más grande que implementa principalmente tecnología OSI de capa 1 y 2, conecta sitios que normalmente se encuentran alejados y utiliza un modelo comercial en el que un consumidor (individuo o empresa) debe arrendar la WAN a un proveedor de servicios (a menudo una empresa de telecomunicaciones). (Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2020).

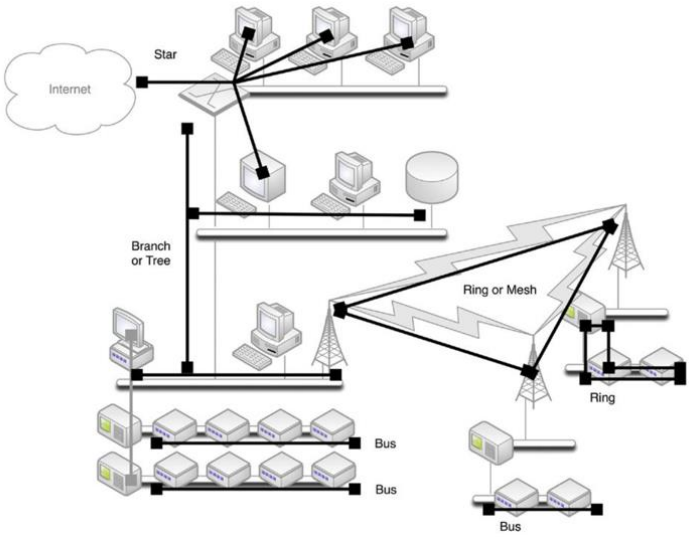
2.8.3. TOPOLOGIAS

Las redes industriales suelen estar muy distribuidas y varían considerablemente en todos los aspectos, incluida la capa de enlace y los protocolos de red utilizados, así como la topología. En las redes comerciales, sin embargo, las redes Ethernet y TCP/IP son omnipresentes y utilizan una variedad de topologías en estrella, árbol e incluso malla completa. La ubicuidad de Ethernet y TCP/IP lo convierte en el "pegamento" que conecta otros SCADA y sistemas de control industrial. Las redes de sistemas de control industrial y

SCADA pueden utilizar topologías de bus, anillo, estrella y árbol según el tipo específico de proceso de control que esté en funcionamiento y los protocolos específicos que se utilicen. (Knapp, Industrial Network Security- Second Edition , 2015).

Figura 14

Topología en Redes IACS.



Fuente: (Knapp, Industrial Network Security , 2011).

2.9. REQUISITOS DE DISEÑO FUNDACIONAL

Los conocimientos y habilidades necesarios para diseñar un sistema de protección cibernética eficaz y manejable incluyen una comprensión detallada de las actividades fundamentales y los fundamentos del diseño. consideraciones tecnológicas y todos los estándares de ciberseguridad relevantes.

2.9.1. CONTRAMEDIDAS

Aquí hay cinco contramedidas clave que las organizaciones pueden usar para impulsar actividades en entornos ICS. La aplicación de estos pasos allanará el camino hacia un entorno de seguridad más sólido y reducirá significativamente el riesgo para los sistemas operativos. (CISA, 2016)

1. Identifique, minimice y asegure todas las conexiones de red al ICS. (CISA, 2016)

2. Fortalezca el ICS y los sistemas de soporte al deshabilitar servicios, puertos y protocolos innecesarios; habilitar las funciones de seguridad disponibles; e implementar prácticas sólidas de gestión de la configuración. (CISA, 2016)
3. Supervise y evalúe continuamente la seguridad del ICS, las redes y las interconexiones. (CISA, 2016)
4. Implemente un enfoque de defensa en profundidad basado en el riesgo para proteger los sistemas y redes ICS.
5. Gestionar al ser humano: identificar claramente los requisitos para el ICS; establecer expectativas de desempeño; responsabilizar a las personas por su desempeño; (CISA, 2016).

2.9.2. ESTRATEGIAS DE DEFENSA EN PROFUNIDAD

Esta sección analiza algunas de las soluciones y estrategias disponibles y recomendadas para la seguridad de defensa en profundidad, como se describe en la Figura 15. Las organizaciones deben usar estas soluciones y estrategias en combinación para crear capas de defensa, habilitando la funcionalidad de ICS y brindando la protección más sólida. disponible para activos críticos. (CISA, 2016). En esta implementación nos centremos en la ICS Network Arquitecture y ICS Network Perimeter Security.

Figura 15

Elementos de la estrategia de Defense-in-Depth.

Defense in Depth Strategy Elements	
Risk Management Program	· Identify Threats · Characterize Risk · Maintain Asset Inventory
Cybersecurity Architecture	· Standards/ Recommendations · Policy · Procedures
Physical Security	· Field Electronics Locked Down · Control Center Access Controls · Remote Site Video, Access Controls, Barriers
ICS Network Architecture	· Common Architectural Zones · Demilitarized Zones (DMZ) · Virtual LANs
ICS Network Perimeter Security	· Firewalls/ One-Way Diodes · Remote Access & Authentication · Jump Servers/ Hosts
Host Security	· Patch and Vulnerability Management · Field Devices · Virtual Machines
Security Monitoring	· Intrusion Detection Systems · Security Audit Logging · Security Incident and Event Monitoring
Vendor Management	· Supply Chain Management · Managed Services/ Outsourcing · Leveraging Cloud Services
The Human Element	· Policies · Procedures · Training and Awareness

Fuente: (CISA, 2016).

2.9.3. SEGMENTACIÓN Y SEGREGACIÓN

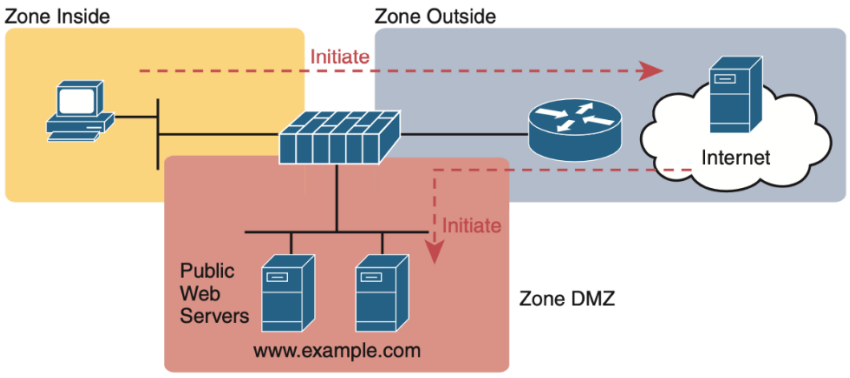
La segmentación de red implica dividir una red en redes más pequeñas; mientras que la segregación de red implica desarrollar y hacer cumplir un conjunto de reglas para controlar las comunicaciones entre hosts y servicios específicos. (ACSC, 2021).

2.9.4. ZONAS DESMILITARIZADAS (DMZ)

Es una red común y limitada de servidores que une dos o más zonas con el fin de controlar el flujo de datos entre zonas. El propósito de una zona desmilitarizada es hacer cumplir la política de redes internas para información externa y proporcionar fuentes externas no confiables con acceso restringido para divulgar información mientras se protege la red interna de ataques externos. (ISA 62443-1-2, 2018)

En un diseño perimetral de Internet en una empresa, se reservan una o más subredes como un lugar para ubicar servidores que deberían permitir a los usuarios de Internet iniciar conexiones a esos servidores. Los dispositivos en la DMZ generalmente se encuentran detrás de un firewall. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

Figura 16
Infografía de una DMZ.

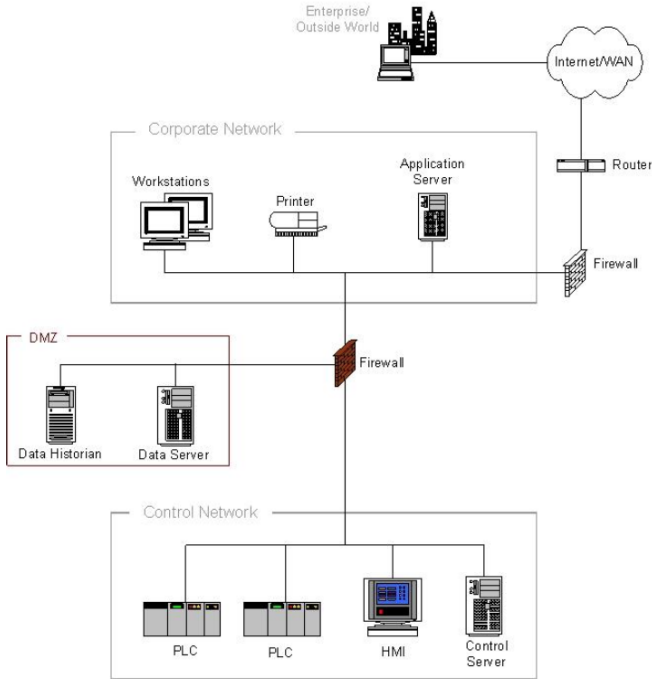


Fuente: (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

Una mejora significativa es el uso de firewalls con la capacidad de establecer una DMZ entre las redes corporativas y de control. Cada DMZ contiene uno o más componentes críticos, como el historial de datos, el punto de acceso inalámbrico o los sistemas de acceso remoto y de terceros. En efecto, el uso de un firewall compatible con DMZ permite la creación de una red intermedia. La creación de una DMZ requiere que el cortafuegos ofrezca tres o más interfaces, en lugar de las típicas interfaces públicas y privadas. Una de las interfaces está conectada a la red corporativa, la segunda a la red de control y las interfaces restantes a los dispositivos compartidos o inseguros, como el servidor histórico de datos o los puntos de acceso inalámbrico en la red DMZ. Se recomienda implementar un control continuo del tráfico de entrada y salida en la DMZ. Además, se recomiendan conjuntos de reglas de firewall que solo permitan conexiones entre la red de control y la DMZ iniciadas por dispositivos de la red de control. (NIST SP 800-82 Rev2, 2015).

Figura 17

Uso de dos firewalls para implementar un DMZ

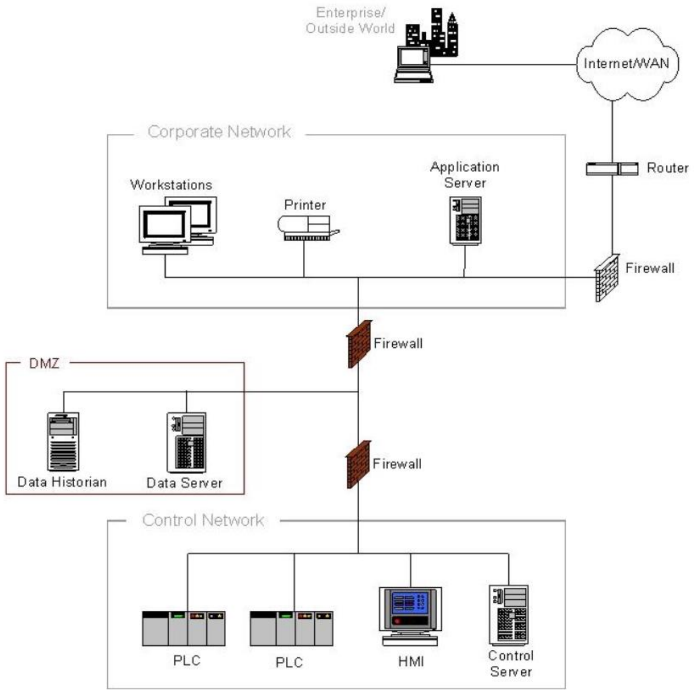


Fuente: (NIST SP 800-82 Rev2, 2015)

Los servidores comunes, como el historial de datos, están situados entre los cortafuegos en una zona de red similar a la DMZ, a veces denominada capa del Sistema de ejecución de fabricación (MES). Como en las arquitecturas descritas anteriormente, el primer cortafuegos bloquea paquetes arbitrarios para que no pasen a la red de control de los historiadores compartidos. El segundo firewall puede evitar que el tráfico no deseado de un servidor comprometido entre en la red de control y evitar que el tráfico de la red de control afecte a los servidores compartidos. (NIST SP 800-82 Rev2, 2015)

Figura 18

Uso de dos firewalls para implementar un DMZ



Fuente: (NIST SP 800-82 Rev2, 2015)

2.9.5. REDES VIRTUALES

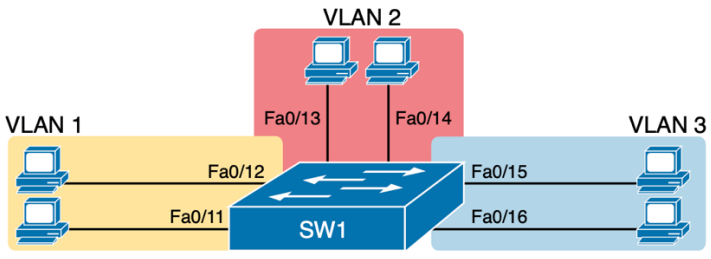
2.9.5.1. VLAN

Las Redes Virtuales (VLAN) proveen seguridad, segmentación, flexibilidad, permiten agrupar usuarios de un mismo dominio de broadcast con independencia se ubicación física de red. Usando la tecnología VLAN se pueden agrupar lógicamente puerto del switch y a los usuarios conectados a ellos en grupos de trabajo con interés en común.

Las VLAN pueden extenderse a múltiples switch por medio de enlaces troncales que se encargan de transportar tráfico a múltiples VLAN. (Ariganello, 2014).

Figura 19

Red con un switch y tres VLAN.



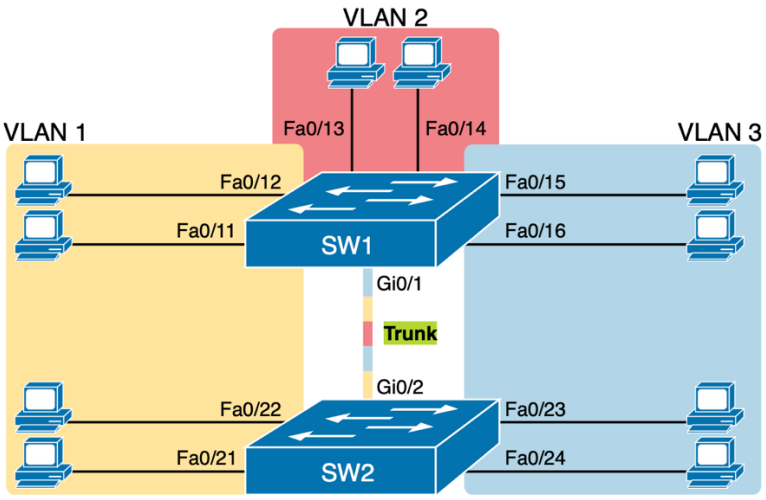
Fuente: (Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2020)

2.9.5.2. TRONCAL O TRUNK

Muchas veces es necesario agrupar usuarios de la misma VLAN que se encuentran ubicados en diferentes zonas, para conseguir esta comunicación los switches utilizan un enlace troncal. Para que los switches envíen información sobre las VLAN que tienen configuradas a. través de enlaces troncales es necesario que las tramas sean identificadas con el propósito de saber a qué VLAN pertenecen. (Ariganello, 2014).

Figura 20

Red con dos switches y tres VLAN.



Fuente: (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

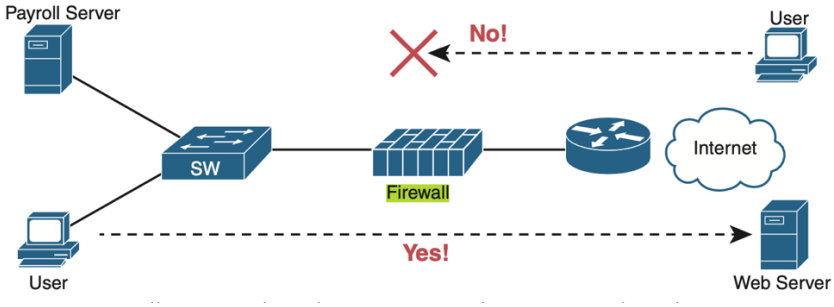
2.10. DISPOSITIVOS SEGURIDAD DE REDES

2.10.1.1. FIREWALL AND IPS

Un dispositivo de conexión entre redes que restringe el tráfico de comunicación de datos entre dos redes conectadas. Un firewall puede ser una aplicación instalada en una computadora de propósito general o una plataforma dedicada (aparato), que reenvía o rechaza/elimina paquetes en una red. Por lo general, los cortafuegos se utilizan para definir los límites de las zonas. Los cortafuegos generalmente tienen reglas que restringen qué puertos están abiertos. (ISA 62443-1-2, 2018).

Figura 21

El firewall como protección perimetral.



Fuente: (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

Un sistema de prevención de intrusiones (IPS) tradicional puede ubicarse en la ruta que toman los paquetes a través de la red y puede filtrar paquetes, pero toma sus decisiones con una lógica diferente. El IPS primero descarga una base de datos de firmas de explotación. Cada firma define diferentes valores de campo de encabezado que se encuentran en secuencias de paquetes utilizados por diferentes "amenaza". Luego, el IPS puede examinar los paquetes, compararlos con las firmas de explotación conocidas y notar cuándo los paquetes pueden ser parte de una explotación conocida. Una vez identificado, el IPS puede registrar el evento, descartar paquetes o incluso redirigir los paquetes a otra aplicación de seguridad para un examen más detenido. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020).

2.10.1.2. FIREWALL NEXT GENERATION

Un firewall de próxima generación (NGFW) es un dispositivo de seguridad de red que proporciona capacidades más allá de un cortafuegos tradicional con estado. Mientras que un firewall tradicional generalmente proporciona una inspección de estado del tráfico de red entrante y saliente, un firewall de próxima generación incluye características adicionales como reconocimiento y control de aplicaciones, prevención integrada de intrusiones e inteligencia de amenazas proporcionada por la nube. (Cisco, 2022).

Un dispositivo de firewall con funciones avanzadas, incluida la capacidad de ejecutar muchas funciones de seguridad relacionadas en el mismo dispositivo de firewall (IPS,

detección de malware, terminación de VPN), junto con una inspección profunda de paquetes con Visibilidad y control de aplicaciones (AVC) y la capacidad de realice el filtrado de URL en comparación con los datos recopilados sobre la confiabilidad y el riesgo asociado con cada nombre de dominio. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

2.10.1.3. CONTROLES DE ACCESO Y AUTENTICACION

En la mayoría de las redes ICS, varios usuarios diferentes utilizan muchos sistemas diferentes, y se debe acceder a los sistemas rápidamente según lo requieran las operaciones del sistema. Las prácticas corporativas de autenticación, autorización y administración de cuentas pueden ser problemáticas para los ICS, ya que los ICS están "siempre encendidos", por lo que detener el sistema para que los usuarios cierren sesión y vuelvan a iniciar sesión generalmente no es una opción viable. Además, los procesos de autenticación proporcionados por los proveedores de ICS pueden estar limitados. Administrar muchos usuarios en ubicaciones dispares se convierte en un desafío a medida que se agrega y elimina el acceso al sistema y los roles de los usuarios cambian. El mismo proceso de autenticación puede controlar el acceso a muchos sistemas (HMI, dispositivos de campo, servidores SCADA) y redes (LAN de subestaciones remotas), que pueden requerir el uso de credenciales compartidas. Los propietarios de activos pueden controlar el acceso a los sistemas ICS mediante un enfoque distribuido o centralizado. La administración de acceso distribuido requiere que cada sistema realice la autenticación por separado. Cada sistema usa un conjunto separado de cuentas de usuario, credenciales y roles. Este enfoque, si bien es una buena solución para implementaciones pequeñas de ICS, no se escala bien para organizaciones grandes. Las organizaciones normalmente utilizan la administración de cuentas centralizada para manejar grandes cantidades de usuarios y cuentas. (CISA, 2016).

2.10.1.4. SEGURIDAD DEL HOST

El nivel de host o estación de trabajo implementa otra capa de seguridad. Los cortafuegos protegen la mayoría de los dispositivos dentro de una red de intrusiones desde el exterior; sin embargo, un buen modelo de seguridad requiere capas de defensa de varios niveles. Esto es especialmente importante para los clientes HMI que se conectan a la red desde fuera del límite de la red ICS de confianza, ya sea a través de una conexión VPN o por cualquier otro medio. Asegurar completamente la red significa asegurar también todos los hosts. (CISA, 2016)

Los requisitos para la seguridad del host son bien conocidos para proteger una máquina/host mientras se instalan y utilizan varios sistemas operativos y aplicaciones. Las siguientes pautas brindan algunas recomendaciones que las organizaciones deben considerar como parte de una política de seguridad para las operaciones del sistema para ayudar a mantener seguros los ICS. En general, considere los siguientes pasos para cada host o dispositivo ICS que se coloque en la red OT, independientemente del sistema operativo:

- Instale y configure un firewall basado en host. (CISA, 2016).
- Elija contraseñas seguras para todas las cuentas en el sistema y cambie cualquier cuenta predeterminada o conocida en el dispositivo (preferiblemente, imponga contraseñas seguras y vencimiento de contraseña a través de las capacidades del sistema operativo). (CISA, 2016).
- Cambie las contraseñas en un horario predefinido, generalmente cada 30 y no más de 90 días. (CISA, 2016).
- Instale protectores de pantalla con intervalos cortos y con un requisito de contraseña para iniciar sesión cuando sea posible. Instale y mantenga actualizados los parches del sistema operativo y del firmware del hardware. (CISA, 2016).

- Configurar y monitorear registros en el dispositivo. (CISA, 2016).
- Deshabilite los servicios y cuentas que no utilice o que ya no sean necesarios. (CISA, 2016).
- Reemplace los servicios inseguros (como telnet, Shell remoto (RSH) or login) con alternativas más seguras como SSH. (CISA, 2016).
- Restrinja el acceso a los servicios que no se pueden deshabilitar, cuando sea posible. (CISA, 2016).
- Realice y pruebe copias de seguridad del sistema de manera coherente si no se controla de forma centralizada. (CISA, 2016).
- Asegure las computadoras y otros dispositivos portátiles y móviles que no estén continuamente conectados a la red. (CISA, 2016).

Los mismos requisitos indicados anteriormente también se aplican a estos dispositivos, cuando sea factible, independientemente de las plataformas y las técnicas de gestión utilizadas. (CISA, 2016).

Los PLC y otras tecnologías de control operativo, en general, no admiten muchas prácticas de protección y mecanismos de seguridad recomendados basados en host. Los controles de defensa en profundidad para esos dispositivos generalmente se aplican a nivel de red. Sin embargo, muchos sistemas HMI se basan en plataformas comunes y los administradores deben bloquearlos (por ejemplo, deshabilitar los servicios innecesarios, deshabilitar los puertos innecesarios, restringir el acceso, usar el bloqueo del núcleo) en la mayor medida posible y garantizar la funcionalidad continua. (CISA, 2016).

Los propietarios de activos deben eliminar cualquier software instalado de forma nativa en el sistema que no necesiten o usen. Por ejemplo, una HMI utilizada para comando y Control no necesita paquetes de software corporativo estándar, como procesadores de textos, hojas de cálculo y clientes de correo electrónico. (CISA, 2016).

Las configuraciones del sistema deben administrarse activamente durante todo el ciclo de vida del sistema. Hay una serie de técnicas que las organizaciones pueden utilizar, como la creación de una imagen segura para configurar nuevos equipos, la reconstrucción de equipos que solo contienen el software requerido y la configuración de dispositivos con solo los servicios y puertos requeridos. (CISA, 2016).

2.11. PROTOCOLOS Y NORMAS DE COMUNICACIÓN

Comprender cómo funcionan las redes industriales requiere una comprensión básica de los protocolos de comunicaciones subyacentes que se utilizan, dónde se utilizan y por qué. Existen muchos protocolos altamente especializados que se utilizan para la automatización y el control industriales, la mayoría de los cuales están diseñados para brindar eficiencia y confiabilidad para respaldar los requisitos económicos y operativos de las arquitecturas de sistemas de control industrial (ICS) de gran tamaño. Los protocolos industriales están diseñados para operación en tiempo real para soportar operaciones de precisión que involucran comunicación determinista de datos de monitoreo y control. (Knapp, Industrial Network Security- Second Edition , 2015).

Industrial Ethernet es un término utilizado para hacer referencia a la adaptación del estándar IEEE 802.3 Ethernet a las aplicaciones de automatización industrial en tiempo real. Uno de los principales objetivos de estas extensiones es avanzar hacia mecanismos de comunicación más “sincrónicos” para evitar colisiones de datos y minimizar la inestabilidad inherente a las comunicaciones “asincrónicas” como Ethernet estándar. Esto permitirá que la tecnología se implemente en aplicaciones críticas que dependen del tiempo, como la seguridad y el control de movimiento industrial. (Knapp, Industrial Network Security- Second Edition , 2015).

2.11.1. INDUSTRIAL ETEHERNET (IE) DE SIEMENS

Es la variante de Ethernet adecuada para aplicaciones industriales y sus características:

- Comunicación optimizada entre componentes de automatización y comunicación simultánea según TCP/IP (estándar abierto). (SIEMENS, 2022)
- Componentes de red para la aplicación en entornos industriales duros (polvo, humedad, vibraciones,). (SIEMENS, 2022).

2.11.2. ICCP (PROTOCOLO DE COMUNICACIONES ENTRE CENTROS DE CONTROL)

También conocido como TASE.2 o IEC60870-6, pero más comúnmente denominado simplemente ICCP, es un protocolo diseñado para la comunicación entre centros de control dentro de la industria de servicios eléctricos. (Knapp, Industrial Network Security- Second Edition , 2015)

El ICCP define la comunicación entre dos centros de control utilizando un modelo cliente-servidor. Un centro de control (el servidor) contiene datos de aplicación y funciones definidas. Otro centro de control (el cliente) emite solicitudes para leer desde el servidor con respuestas de servidor adecuadas. Las comunicaciones sobre ICCP se producen utilizando un formato común para garantizar la interoperabilidad. ICCP puede operar esencialmente sobre cualquier protocolo de red, incluido TCP/IP; sin embargo, comúnmente se implementa usando el transporte ISO en el puerto 102/TCP, como se define en RFC 1006. ICCP es efectivamente un protocolo punto a punto debido al uso de una "tabla bilateral" que define explícitamente un acuerdo entre dos con - centros de control conectados con un enlace ICCP. (Knapp, Industrial Network Security- Second Edition , 2015)

2.11.3. IEC 60870-5-104

IEC se refiere a una colección de estándares producidos por IEC, o IEC, para proporcionar un estándar abierto para la transmisión de información y control de telemetría SCADA. El estándar proporciona una descripción funcional detallada para equipos y

sistemas de telecontrol para controlar procesos geográficamente extendidos, en otras palabras, para sistemas SCADA. (Clarke, Reyders, & Wright, 2004).

El estándar IEC 60870-5-104, también conocido por IEC 104, es un protocolo industrial, extensión del IEC 60870-5-101, para abreviar IEC 101, que se encarga exclusivamente del telecontrol, monitorización y comunicaciones relacionadas con el sistema SCADA. En general, es utilizado en el sector eléctrico para la automatización de subestaciones y centrales de generación. El protocolo IEC 104 mejora la versión IEC 101 en los servicios proporcionados en la capa de red, de transporte, física y de enlace del modelo OSI, ya que permite una conectividad o acceso total a la red mediante TCP/IP. (incibe-cert, 2018).

El protocolo IEC 104 es el encargado de transportar la información desde las RTU (Unidad Terminal Remota), IED (Dispositivos Electrónicos Inteligentes), Gateway o servidores de comunicaciones hasta el sistema SCADA. (incibe-cert, 2018)

El funcionamiento del protocolo IEC 104 es el siguiente:

- La estación de control, comúnmente con rol maestro, es la encargada de iniciar las comunicaciones o enviar comandos a dispositivos o aplicaciones; estos datos transmitidos van en una sola dirección, llamada de control. (incibe-cert, 2018).
- Las subestaciones o estaciones controladas serán los dispositivos remotos que transmiten los datos recogidos a las estaciones de control. Esta dirección de envío se conoce por el nombre de supervisión. Al ser dependientes de la estación de control, reciben el nombre de esclavos. (incibe-cert, 2018).

2.11.4. SERVICIOS DE TI / IACS

¿Qué puertos utilizan los distintos servicios para la transmisión de datos a través de TCP y UDP y qué hay que tener en cuenta a la hora de utilizar routers y cortafuegos? (SIEMENS, 2021)

Cuando se transmiten datos a través de TCP y UDP, los diferentes servicios utilizan cada uno su propio puerto.Si los datos se transmiten a través de routers o se utilizan firewall, el puerto debe estar habilitado en el router o el cortafuegos según el servicio utilizado. (SIEMENS, 2021).

Tabla 5

Principales servicios usados en este proyecto.

Service	Protocol Name	Destination Port	IP Version	Description
SSH	TCP	22	IPv4	Secure Shell (SSH), also Secure File Transfer Protocol (SFTP) secure CLI access ("secure FTP")
HTTP	TCP	80	IPv4	Hypertext Transfer Protocol (HTTP)
SIMATIC-S7	TCP	102	IPv4	Transport Service Access Point (ISO-TSAP) used by SIMATIC S7
HTTPS	TCP	443	IPv4	Hyper Text Transfer Protocol Secure (HTTPS) is used for the communication with the webserver of a device, e. g. S7-CPU, CP or CU, via Transport Layer Seurity (TLS).
Remote Desktop	TCP	3389	IPv4	Windows Remote Desktop
ALM	TCP	4410	IPv4	Automation License Manager (License service)

DCOM	TCP	135	IPv4	This service is required to initialize OPC (DA) connections. The communication via OPC (DA) is based on DCOM and uses unspecified ports assigned by the system. This should be taken into consideration when using OPC (DA) and creating rules for the firwall.
Archiving	TCP	139	IPv4	Used by WinCC Flexible RT for archiving on a server
VNC Server	TCP	5900	IPv4	Used by Sm@rtServer application (Server)
NTP / SNTP	TCP UDP	123	IPv4	Network Time Protocol (NTP) is a standard for time synchronization in IP-based networks. Simple Network Time Protocol (SNTP) is a simplified version of the NTP.

Fuente: (SIEMENS, 2021)

2.12. GLOSARIO

- **CENTRO DE CONTROL**

Ubicación central utilizada para operar un conjunto de activos. Las industrias de infraestructura generalmente usan uno o más centros de control para supervisar o coordinar sus operaciones. SI hay varios centros de control (por ejemplo, un centro de respaldo en un sitio separado), generalmente están conectados entre sí a través de una WAN. El centro de control contiene las computadoras anfitrionas SCADA y los dispositivos de visualización del operador asociados, además del sistema de información auxiliar, como un historial. En algunas industrias, el término "sala de control" puede usarse más comúnmente. (ISA 62443-1-2, 2018).

- **DOMINIO DE DIFUSIÓN**

Incluye el conjunto de todos los dispositivos conectados a la LAN, de modo que cuando cualquiera de los dispositivos envía una trama de difusión, todos los demás dispositivos obtienen una copia de la trama. (Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2020).

- **ETHERNET**

Ethernet es el standard para redes (LAN) en las oficinas. (SIEMENS, 2022).

- **GATEWAY**

En un host IP, la dirección IP de algún enrutador al que el host envía paquetes cuando la dirección de destino del paquete está en una subred. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020).

- **HMI (INTERFAZ HOMBRE-MAQUINA)**

Es la interfaz de usuario para los procesos de un sistema de control industrial. Una HMI traduce de manera efectiva las comunicaciones hacia y desde los PLC, RTU y otros activos industriales a una interfaz legible por humanos, que utilizan los operadores de sistemas de control para administrar y monitorear procesos. (Knapp, Industrial Network Security- Second Edition , 2015)

- **LAN (RED DE AREA LOCAL)**

Incluye todos los dispositivos de usuario, servidores, conmutadores, enrutadores, cables y puntos de acceso inalámbrico en una ubicación. Una LAN incluye todos los dispositivos en el mismo dominio de transmisión. (Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2020)

- **PLC (CONTOLADOR LOGICO PROGRAMABLE)**

Generalmente controlan procesos en tiempo real, por lo que están diseñados para una eficiencia simple. Por ejemplo, en la fabricación de plástico, puede ser necesario inyectar un catalizador en una tina cuando la temperatura alcanza un valor muy específico. Si la sobrecarga de procesamiento u otra latencia introduce un retraso en

la ejecución de la lógica del PLC, sería muy difícil programar con precisión las inyecciones, lo que podría generar problemas de calidad. Por esta razón, la lógica utilizada en los PLC suele ser muy simple y se programa de acuerdo con un conjunto de lenguajes estándar internacional definido por IEC-61131-3. (Knapp, Industrial Network Security- Second Edition , 2015)

- **PUTTY**

Es un cliente SSH y telnet, desarrollado originalmente por Simón Tatham para la plataforma Windows. PuTTY es un software de código abierto que está disponible con código fuente y está desarrollado y respaldado por un grupo de voluntarios. (Putty, s.f.).

- **RTU (UNIDAD TERMINAL REMOTA)**

Es un dispositivo que combina capacidades de comunicación remota con lógica programable para el control de procesos en ubicaciones remotas. (Knapp, Industrial Network Security- Second Edition , 2015).

- **SCADA (SUPERVISIÓN CONTROL Y ADQUISICION DE DATOS)**

Tipo de sistema de monitoreo y control distribuido débilmente acoplado comúnmente asociado con sistemas de transmisión y distribución de energía eléctrica, tuberías de petróleo y gas, y sistemas de agua y alcantarillado. (ISA 62443-1-2, 2018).

- **SECURE SHELL (SSH)**

Un protocolo de capa de aplicación TCP/IP que admite la emulación de terminal entre un cliente y un servidor, mediante el intercambio dinámico de claves y el cifrado para mantener la privacidad de las comunicaciones. (Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2020)

- **SUC (SISTEMA BAJO CONSIDERACIÓN)**

Colección de activos para el propósito de una evaluación de riesgos cibernéticos. Un SUC consiste en un conjunto de una o más zonas y sus conductos relacionados en la

cual todos los activos de un SUC están dentro de una zona o de un conducto. (ISA 62443-1-2, 2018)

- **SIMATIC NET**

Representa una variedad de componentes de red que están disponibles para la realización innovadora y consistente de soluciones de automatización bajo el paraguas de "Totally Integrated Automation". PROFINET es el protocolo más utilizado por los componentes de SIMATIC NET en el contexto de Industrial Ethernet. (SIEMENS, 2021)

- **VPN (VIRTUAL PRIVATE NETWORK)**

Es un conjunto de protocolos de seguridad que, cuando son implementados por dos dispositivos a cada lado de una red no segura como Internet, pueden permitir que los dispositivos envíen datos de forma segura. Las VPN brindan privacidad, autenticación de dispositivos, servicios anti-reproducción y servicios de integridad de datos. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

- **VIRTUAL MACHINE**

máquina virtual Una instancia de un sistema operativo, que se ejecuta en el hardware del servidor que utiliza un hipervisor para asignar un subconjunto del hardware del servidor (CPU, RAM, disco y red) a esa máquina virtual. (Odom, CCNA 200-301 Official Cert Guide, Volume 2, 2020)

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

3.1. OBJETIVO

3.1.1. OBJETIVO PRINCIPAL

Implementar Ciberseguridad en el Sistemas de Control y Automatización Industrial dentro de la Compañía Eléctrica El Platanal S.A.

3.1.2. OBJETIVOS ESPECIFICOS

- Segregación entre las redes IACS y TI.
- Segmentación de la red IACS.
- Gestión centralizada de los ciberactivos de IACS.

3.2. RED IACS HASTA EL 2020

El inicio de operación comercial fue en mazo del 2010, y no fue hasta el año 2020 donde iniciamos con el proceso de upgrade del Sistema SCADA y Ciberseguridad IACS; segregación de las redes TI e IACS y su segmentación como principales actividades.

Diez años la red IACS de EP era la VLAN 220 de TI, donde esta área gestiona la comunicación con las otras áreas operativas de la planta San Juanito y la ciberseguridad era en la capa superiores.

Tabla 6

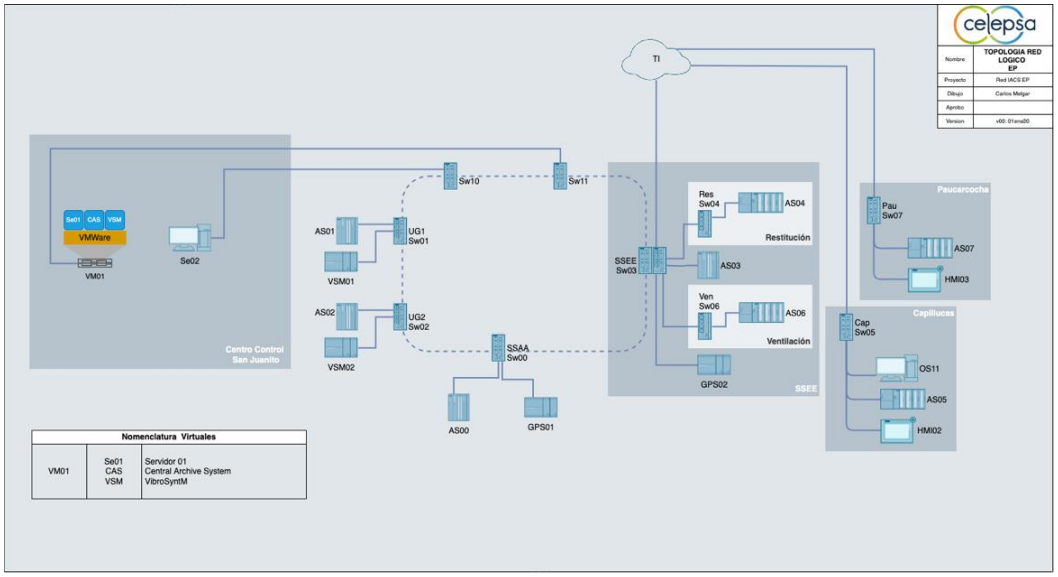
VLAN de las redes destinada para el IACS, antes del proyecto.

Red IACS	Segmento de Red
El Platanal	192.168.220/24
Capillucas	192.168.222/24
Paucarcocha	192.168.224/24
Marañón	192.168.226/24

Cada una de estas VLAN era gestionada por TI.
Fuente: Propia

Figura 22

Arquitectura de control L2 para EP hasta el año 2020.

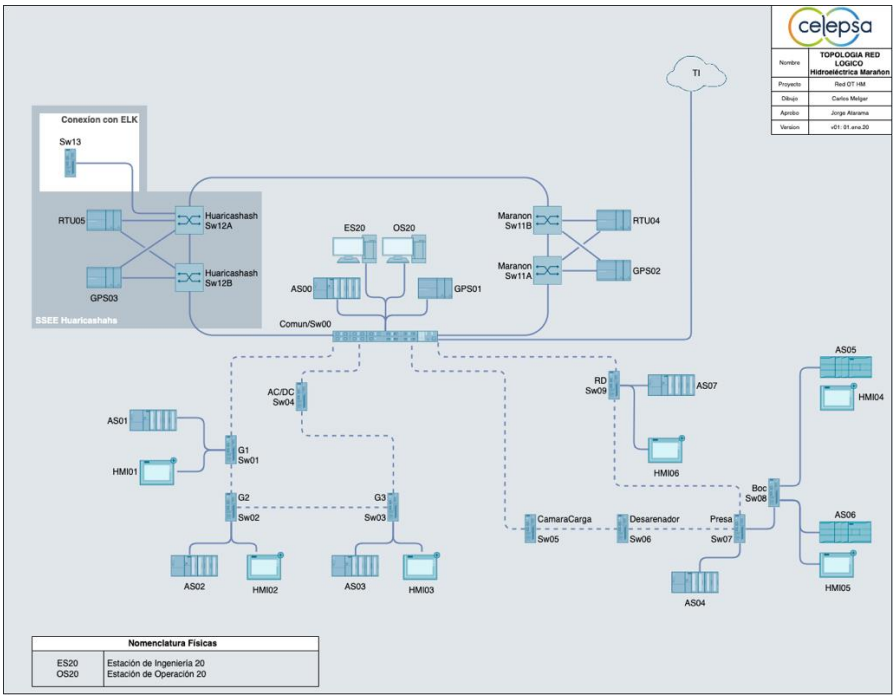


El Sw03 está directamente conectado a la red de TI, es decir no existe una segregación entre la red IACS y la red de TI.

Fuente: Propia

Figura 23

Arquitectura de control L2 para HM hasta el año 2020.



El Sw00 está directamente conectado a la red de TI, es decir no existe una segregación entre la red OT IACS y la red de TI.

Fuente: Propia

Para este proyecto se adquirieron equipos de TI de infraestructura de red, infraestructura de servidores como host para virtualizar, sistemas operativos Windows y antivirus. También se adquirieron equipos de uso industrial como switch, firewall y licencias de upgrade SCADA y procesadores de comunicación para los PLCs.

Como parte de la implementación de ciberseguridad IACS de CELEPSA abordaremos las actividades principales de configuración de los firewall, switch y políticas entre las áreas operativas de Centro de Control CELEPSA, EP y HM, tomando como referencia la norma IEC 62443.

3.3. DESARROLLO DEL PROYECTO

Con el fin de establecer un orden en las actividades que se efectuaron, se estableció una secuencia de atención y actividades, la primera área operativas atendida fue el Centro de Control CELEPSA en Lima, como segundo fue: Planta El Platanal en Cañete y la último fue: Planta Hidro Marañón en Huánuco. Esto obedeció al traslado de mi persona a cada área operativa.

3.4. REDES IACS: CENTRO DE CONTROL CELEPSA

En esta área operativa no se contaba con una red IACS. Por lo que se diseñó e implementó esta nueva red IACS con las contramedidas recomendadas por la IEC 62443.

3.4.1. REQUERIMIENTOS DE EQUIPOS

Se compraron los ciberactivos necesarios para segregar y segmentar la red IACS del CCC y estos son expuestas en la Tabla 7 de forma general:

Tabla 7
Necesidad de equipos de red y seguridad perimetral para la implementación de la red IACS en Lima.

Requerimientos	Modelo	Marca	Tag
Switch	C9200	Cisco	CESW01A/B
Firewall	1570R	Check Point	CEFW01A/B

Fuente: Propia

3.4.1.1. SWITCH 9200

Los switches Cisco® Catalyst® 9200 Series amplían el poder de las redes basadas en intención y la innovación de hardware y software Catalyst 9000 a un conjunto más amplio de implementaciones. Con su pedigrí familiar, los switches de la serie Catalyst 9200 ofrecen simplicidad sin concesiones: es seguro, está siempre encendido y simplifica la TI. Como componentes fundamentales de la arquitectura de red digital de Cisco, los switches Catalyst de la serie 9200 ayudan a los clientes a simplificar la complejidad, optimizar la TI y reducir los costos operativos al aprovechar la inteligencia, la automatización y la experiencia humana que ningún otro proveedor puede ofrecer, independientemente de dónde se encuentre en la intención. viaje basado en redes. Los switches de la serie Catalyst 9200 brindan funciones de seguridad que protegen la integridad del hardware y del software y todos los datos que fluyen a través del switch. Proporciona resiliencia que mantiene su negocio en funcionamiento sin problemas. Con capacidad PoE+ completa, redundancia de energía y ventiladores, enlaces ascendentes modulares, compatibilidad con funciones de capa 3 y parches en frío, los switches de la serie Catalyst 9200 son la solución sin paralelo de la industria con resiliencia diferenciada y arquitectura progresiva para un acceso rentable a las sucursales.

Sus características principales: Layer 2, Routed Access (RIP, EIGRP Stub, OSPF - 1000 routes), PBR, PIM Stub Multicast (1000 routes), PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1X, MACsec-128, CoPP, SXP, IP SLA Responder y Model-driven telemetry, sampled NetFlow, SPAN, RSPAN.

Figura 24

Mostramos imagen de un switch 9200 comprado para el gabinete IACS en el Data Center de CELEPSA-La Victoria.

Fuente: Propia

3.4.1.2. FIREWALL 1570R

El Check Point 1570R (consulte la hoja de datos) es el miembro resistente de la familia de dispositivos de seguridad 1500 que ofrece seguridad de nivel empresarial en una serie de puertas de enlace de seguridad todo en uno simples y asequibles. Estos dispositivos de seguridad incluyen un paquete de seguridad integral y el último software R80 para dispositivos SMB.

El firewall de próxima generación (NGFW) Check Point 1570R protege la infraestructura crítica y los sistemas de control industrial (ICS) sin afectar las operaciones. Nuestros NGFW identifican y protegen más de 70 protocolos SCADA (Control de supervisión y adquisición de datos) y ICS estándar y patentados. Esto incluye los protocolos más populares utilizados en los sectores de servicios públicos y energía, sectores de fabricación, sistemas de gestión de edificios y dispositivos IoT (Internet de las cosas).

El diseño de estado sólido del 1570R Rugged funciona en temperaturas que van desde menos 40 °C hasta 75 °C, lo que lo hace ideal para proteger cualquier aplicación industrial: plantas de energía y fabricación, instalaciones de petróleo y gas, flotas marítimas, sistemas de administración de edificios y más.

El 1570R está certificado para las especificaciones industriales IEEE 1613 e IEC 61850-3 para calor, vibración e inmunidad a la interferencia electromagnética (EMI). Además, el 1570R está certificado para operación marítima según IEC-60945 e IACS E10 y cumple con DNV-GL-CG-0339.

Sus características principales de la 1570R en hardware

- Diseño sin ventilador basado en aluminio
- Alámbrico y WiFi + LTE
- Conectividad
    - LAN: 8x1GbE

  - WAN: puerto 1x1GbE / SFP
  - DMZ: puerto 1x1GbE / SFP
  - Admite Flexiport (el puerto LAN puede funcionar como WAN)
- Dos fuentes de energía
  - Adaptador de corriente (12 V, 40 W de grado comercial e industrial de 120 W -40 a 70 grados C)
  - Estos adaptadores de corriente se venden por separado y no forman parte de la caja del 1570R.
  - Bloque de terminales de 3 pines, 12 V-72 VCC y -48 VCC, suministrado por la infraestructura de energía del cliente
  - Redundancia de energía (cuando los dos anteriores están conectados)
- Sobremesa, montaje en pared y carril DIN (2 tipos de montaje - posterior e inferior)
- Puerto de consola USB tipo C
- Puerto USB 3.0
- Compatibilidad con tarjeta SD
- Compatibilidad con el protocolo ICS/SCADA
  - BACNet, CIP, DNP3, IEC-60870-5-104, IEC 60870-6 (ICCP), IEC 61850, MMS, ModBus, OPC DA y UA, Profinet, Step7 (Siemens) y más; 1400+ en total. Vea la lista completa en appwiki.checkpoint.com.
- Certificado para operar en condiciones adversas
  - Industrial: IEEE 1613, IEC 61850-3, IEC 60945, EN/IEC 60529, calor e inmunidad a interferencias electromagnéticas
  - Robusto: EN/IEC 60529, IEC 60068-2-27 choque, IEC 60068-2-6 vibración
  - Marítimo (proceso de certificación en curso): IEC-60945 B, IACS E10:1991, DNV-GL 2.4, DNV-GL-CG-0339, IEC 61162-460

- Rango de temperatura de funcionamiento: -40 ºC ~ 75 ºC (-40 ºF ~ 167 ºF)
- Clasificación IP (protección de ingreso): IP30

- Protección Integral
  - Cortafuegos de próxima generación.
  - VPN de sitio a sitio
  - VPN de acceso remoto
  - Control de aplicaciones y filtrado web
  - Prevención de intrusiones, Antivirus y Anti-robot
  - Antispam Emulación de amenazas SandBlast (sandboxing)
  - Reconocimiento de dispositivos Inspección de correo electrónico

Figura 25

Mostramos imagen de un NGFW comprado para el gabinete IACS en el Data Center de CELEPSA.

Fuente: Propia

Para un mayor detalle de los ciberactivos comprados estos se adquirieron con los detalles mostrados en la Tabla 8 para los swicthes y Tabla 9 para los firewalls.

Tabla 8

Requerimientos de swicthes empleados para la implementación de la red IACS del CCC.

Numero de Parte	Descripción	Cantidad
C9200L-24T-4G-E	Catalyst 9200L 24-port data, 4 x 1G, Network Essentials	2
C9200L-NW-E-24	C9200L Network Essentials, 24-port license	2
PWR-C5-125WAC/2	125W AC Config 5 Power Supply - Secondary Power Supply	2
CAB-TA-NA	North America AC Type A Power Cable	4

C9200L-DNA-E-24	C9200L Cisco DNA Essentials,24-port Term license	2
C9200L-DNA-E-24-3Y	C9200L Cisco DNA Essentials, 24-port, 3 Year Term license	2
NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	2
C9200-STACK-BLANK	Catalyst 9200 Blank Stack Module	4

Fuente: Propia.

Tabla 9

Requerimientos de firewalls empleados para la implementación de la red IACS del CCC.

Numero de Parte	Descripción	Cantidad
CPAP-SG1570R-SNBT	1570R Ruggedized Next Generation Appliance with DC power	2
CPES-SS-STANDARD-ADD	Standard Direct Enterprise Support For 1 Year 1	1

Fuente: Propia

3.4.2. CONFIGURACIONES DE EQUIPOS

Primero se efectuó el inventario de todos los SUC detallando como mínimo: Nombre, dirección IP, mascara y gateway.

Por temas de ciberseguridad ocultaremos la dirección IP de cada ciberactivo de este proyecto, pero para una equivalencia indicaremos que los tres primeros octetos de la dirección IP será representado por una letra de abecedario, de los cuales:

- El primer octeto representara su área operativa.
- El tercer octeto representara a la VLAN que pertenece.
- El cuarto octeto representa la dirección del host.

Tabla 10

SUC que pertenecen a la VLAN 1, dentro de la red IACS de CCC, identificación y direccionamiento IP.

Nombre	Tag	Equipo	IP	Gateway
Firewall 01V	FW01V	Firewall	A.A.A.1/*	
Firewall 01A	FW01A	Firewall	A.A.A.2/*	
Firewall 01B	FW01B	Firewall	A.A.A.3/*	
Switch DMZ	sw02	Switch	A.A.A.41/*	A.A.A 1
Consola	FW01c	Switch	A.A.A.250/*	A.A.A.1
Switch #1A	sw01A	Switch	A.A.A.251/*	A.A.A.1
Switch #1B	sw01B	Switch	A.A.A.252/*	A.A.A.1

Direccionamiento IP equivalente de la infraestructura de red IACS dentro de la VLAN 1.

Fuente: Propia

Tabla 11

SUC del CCC, identificación y direccionamiento IP.

Nombre	Tag	VLAN	IP
Network Perfomance Montoring	OSNPM	1	A.A.A.4
Estacion Ingenieria #1	ES01	1	A.A.A.8
Estacion Ingenieria #2	ES02	1	A.A.A.9
Servidor #1	Se01	1	A.A.A.10
Servidor #2	Se02	1	A.A.A 12
Servidor #3	Se03	1	A.A.A.13
VM01	VM01	1	A.A.A 20
VM02	VM02	1	A.A.A.22
VM03	VM03	1	A.A.A 23
GPS	GPS01	1	A.A.A.30
Servidor-Estación Operación #1	OSS01A	230	A.A.B.4
Servidor-Estación Operación #2	OSS01B	230	A.A.B.5
Process Historian / IF	PHS	230	A.A.B.10
Servidor-Estación Operación #1	OSS01A	231	A.A.C.4
Servidor-Estación Operación #2	OSS01B	231	A.A.C.5
Cliente-Estación Operación #1	OSC01	231	A.A.C.6
Cliente-Estación Operación #2	OSC02	231	A.A.C.7
Cliente-Estación Operación #3	OSC03	231	A.A.C.8
Cliente-Estación Operación #4	OSC04	231	A.A.C.9
Process Historian	PHS	231	A.A.C.10
Estación Ingeniería	ES01	231	A.A.C.12
Host	*	232	A.A.D.*
Cliente: Estación Gestión de Energía	PMEC01	233	A.A.E.4
Estación Video Wall	SVW01	234	A.A.F.4
Estación Comunicación #1	CS01A	235	A.A.G.4
Estación Comunicación #2	CS01B	235	A.A.G.5
Estación Comunicación #1	CS01A	87	A.A.H.87
Estación Comunicación #2	CS01B	87	A.A.H.88
Estación Comunicación #1	CS01A	88	A.A.I.87
Estación Comunicación #2	CS01B	88	A.A.I.88
Estación Comunicación #1	CS01A	199	A.A.J.108
Estación Comunicación #2	CS01B	199	A.A.J.108

Direccionamiento IP equivalente de los equipos de Control de la red IACS.

Fuente: Propia

3.4.2.1. CONFIGURACION DE LOS FIREWALL CON EL OBJETIVO DE SEGREGAR LA RED IACS DEL CCC

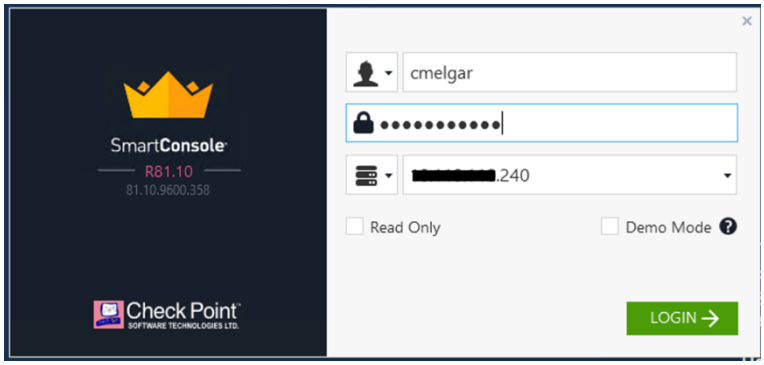
Con el objetivo de segregar la red IACS y la red TI, se usó y se configuro los dos Firewall de la Tabla 9, además se habilito la gestión de rutas entre VLAN para las comunicaciones entre ellas, y después se detallaron y aplicaron las políticas de ciberseguridad para esta red IACS del CCC.

De manera referencial se indica los pasos que se efectuaron para la configuración de los firewalls.

1. Se conecta a la consola de administración de los firewalls, desde el escritorio se buscó su acceso directo: Smart Console.
2. Se escribe las credenciales y dirección IP de fábrica de la consola.

Figura 26

Ventana inicial para el acceso a la configuración de la de los firewalls

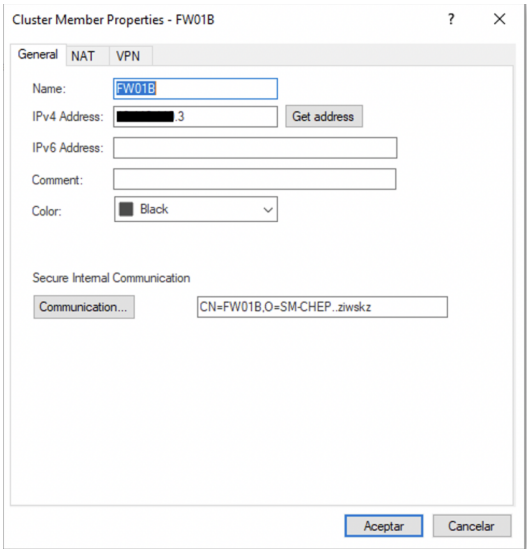


Fuente: Propia

3. En la Barra de Navegación, se hizo selección en “Gateways & Servers”
4. Se hizo clic en “New” y se seleccionó “Gateway”.
5. Se abrió la ventana de propiedades de “Check Point Gateway” y nos mostró la pantalla: Propiedades Generales. Se escribió el nombre del host: FW1A y su dirección IP: A.A.A.2.
6. Se repitió el paso 5, solo que en esa oportunidad se escribió el host: FW1B y su dirección IP. A.A.A.3.

Figura 27

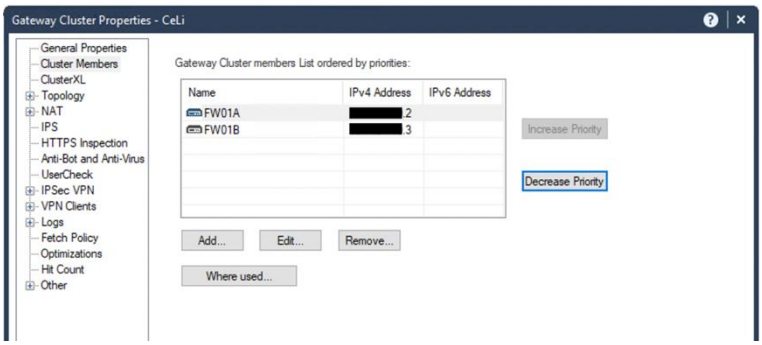
Ventana donde se agregó el firewall para la red IACS del CCC.



Fuente: Propia

Figura 28

Visualización de los firewalls ya integrados a nivel de clúster para la red IACS del CCC.



Detalle de los dos firewalls integrados para la segregación.

7. En “Topología”, se escribió los registros de la Tabla 12.

Tabla 12

Direccionamiento IP para el tráfico de VLAN para la red IACS del CCC.

Función	Gateway	Puerto	Puerto	Conexión
Cluster	LAN1	LAN1	LAN1	
	A.A.A.1	A.A.A.2	A.A.A.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.230	LAN3.230	LAN3.230	
	A.A.B.1	A.A.B.2	A.A.B.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.231	LAN3.231	LAN3.231	

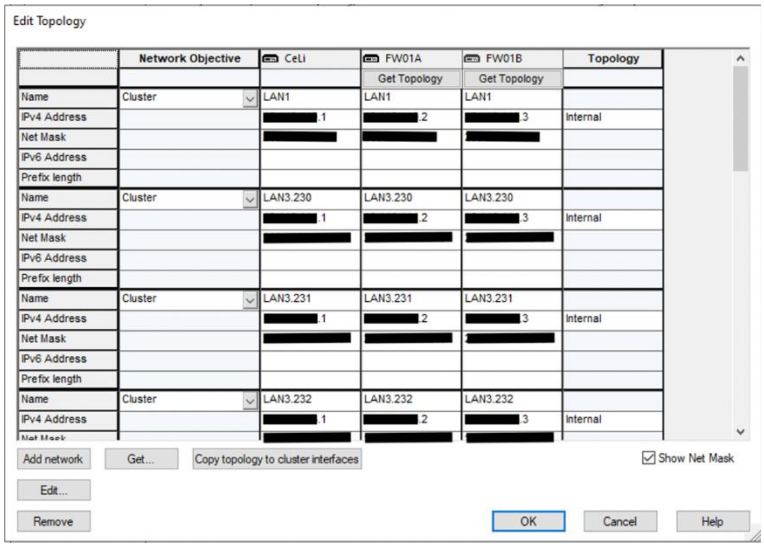
	A.A.C.1	A.A.C.2	A.A.C.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.232	LAN3.232	LAN3.232	
	A.A.D.1	A.A.D.2	A.A.D.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.233	LAN3.233	LAN3.233	
	A.A.E.1	A.A.E.2	A.A.E.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.234	LAN3.234	LAN3.234	
	A.A.F.1	A.A.F.2	A.A.F.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.235	LAN3.235	LAN3.235	
	A.A.G.1	A.A.G.2	A.A.G.3	Internal
	mascara	mascara	mascara	
Cluster	LAN4.87	LAN4.87	LAN4.87	
	A.A.H.9	A.A.H.10	A.A.H.11	Internal
	mascara	mascara	mascara	
Cluster	LAN4.88	LAN4.88	LAN4.88	
	A.A.I.9	A.A.I.10	A.A.I.11	Internal
	mascara	mascara	mascara	
Cluster	LAN4.199	LAN4.199	LAN4.199	
	A.A.J.9	A.A.J.10	A.A.J.11	Internal
	mascara	mascara	mascara	
Cluster	WAN	WAN	WAN	
	A.A.Z.3	A.A.Z.4	A.A.Z.5	External
	mascara	mascara	mascara	
1st Sync		LAN2	LAN2	
		A.A.K.1	A.A.K.2	Internal
		mascara	mascara	

Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

Figura 29

Visualización de las redes agregadas a los firewalls para la red IACS del CCC.



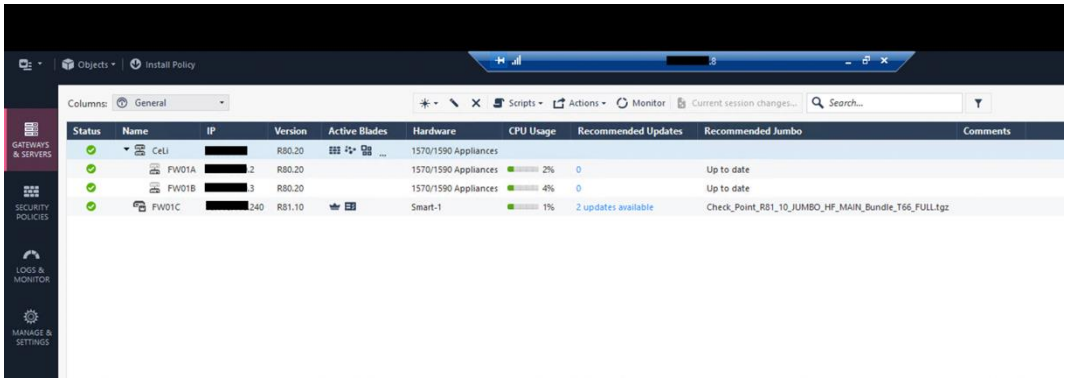
Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

8. Se retornó a “Gateways & Servers y se verifico el detalle de los dos firewalls: FW01A y FE01B.

Figura 30

Visualización del detalle de los dos firewalls de la red IACS del CCC.



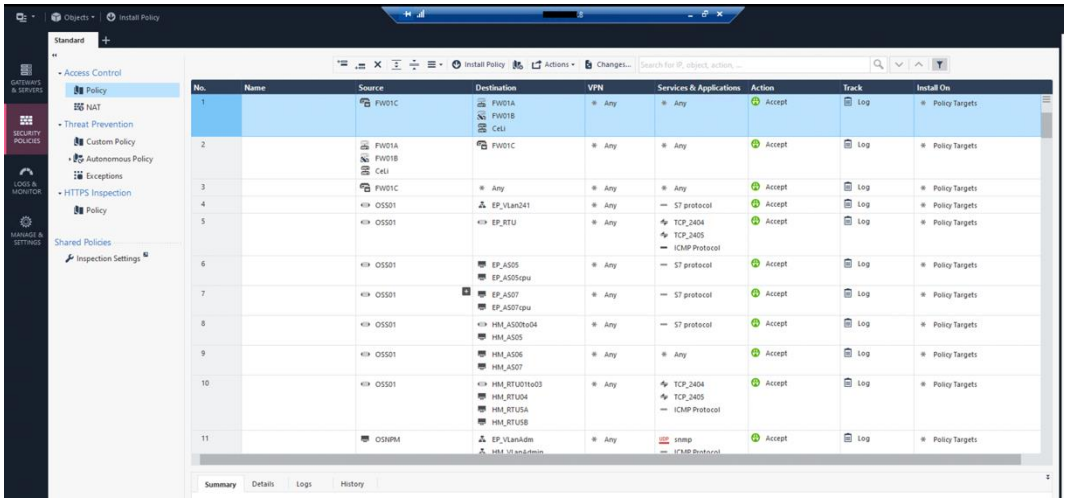
Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

9. En la Barra de Navegación, se hizo selección en “Security Policies”, se agregó nuestras políticas de ciberseguridad de la Tabla 13.

Figura 31

Visualización de las políticas de los dos firewalls de la red IACS del CCC.

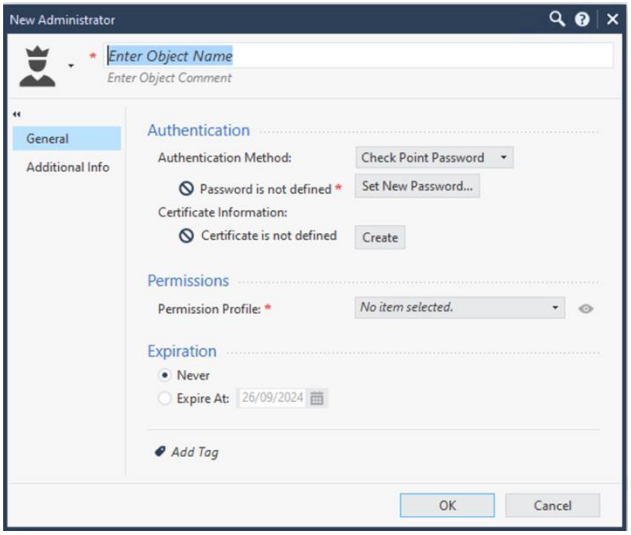


Fuente: Propia

10. En la Barra de Navegación, se hizo selección en “Manage & Settings” luego en “Permissions y Administration”, se agregó nuestro usuario cmelgar como super usuario.

Figura 32

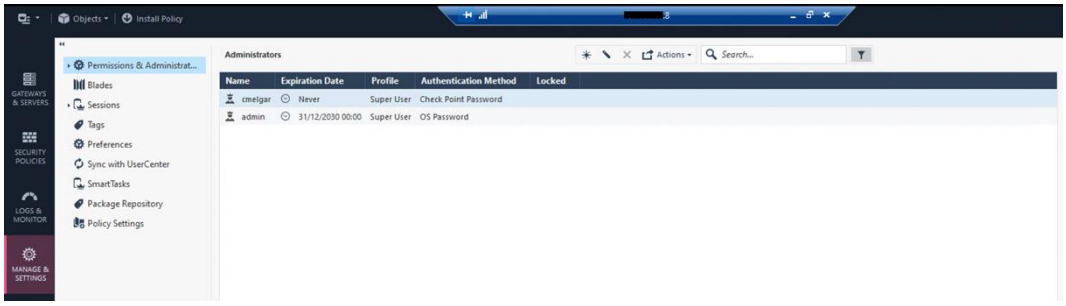
Ventana de nuevo usuario de acceso a la consola de la red IACS del CCC.



Fuente: Propia

Figura 33

Ventana donde se muestra los Administradores de los firewalls de la red IACS del CCC.



Fuente: Propia

Figura 34

Mostramos los dos firewalls 1570R instalado en el gabinete IACS en el Data Center de CELEPSA.

Fuente: Propia

3.4.2.2. CONFIGURACION DE LOS SWITCH CON EL OBJETIVO DE SEGMENTAR LA RED IACS DEL CCC

Después que se terminó con la segregación de la red IACS y la red TI. Se inicio la actividad en los switches que consistió en: programación básica y el uso de VLAN. Este ultimó que permitió la conectividad entre los SUC de la misma VLAN y la conexión entre SUC permitidos de diferentes VLAN. De manera breve se efectuaron los siguientes pasos para la programación de los dos switches.

1. Se conectó el cable de consola al switch CESW01A al puerto serial de nuestra estación de trabajo. Luego haremos lo mismo para el CESW01B.

Figura 35

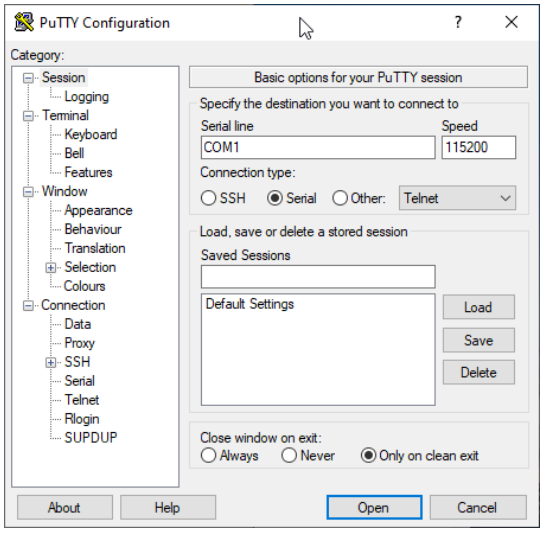
Cable de consola empleado para la configuración inicial de los switches de cisco.

Fuente: Propia

2. Se inició Putty en nuestra estación de trabajo con los parámetros de la Figura 36, que es el establecido para los equipos Cisco.

Figura 36

Aplicativo de escritorio que se empleó para una conexión CLI a los switches de cisco.



Fuente: Propia

3. Se escribió los siguientes comandos en el CLI, del switch CESW01A:

```
Switch# enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname CESW01A

CESW01A (config)# enable secret contraseñaPrivilegiada

CESW01A (config)# line console 0
CESW01A (config-line)# password contraseñaConsola
CESW01A (config-line)# login
CESW01A (config-line)# exit

CESW01A (config)# ip domain name iacs.com
CESW01A (config)# username user privilege 15 secret 0 contraseña
CESW01A (config)# crypto key generate rsa
        1024 y enter
```

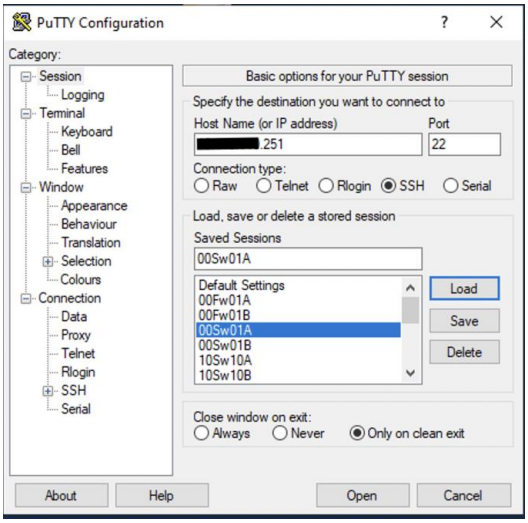
```
CESW01A (config)# ip ssh version 2
CESW01A (config)# line vty 0 15
CESW01A (config-line)# login local
CESW01A (config-line)# exit

CESW01A (config)# service password-encryption

CESW01A (config)# interface vlan1
CESW01A (config-if)# ip address A.A.A.251 mascara
CESW01A (config-if)# no sh
CESW01A (config-if)# exit

CESW01A (config)# ip default-gateway A.A.A.251

CESW01A (config)# vlan 199
CESW01A (config-vlan)# name ICCP
CESW01A (config)# vlan 230
CESW01A (config-vlan)# name SCADA
CESW01A (config)# vlan 231
CESW01A (config-vlan)# name tSCADA
CESW01A (config)# vlan 232
CESW01A (config-vlan)# name PME
CESW01A (config)# vlan 233
CESW01A (config-vlan)# name tPME
CESW01A (config)# vlan 234
CESW01A (config-vlan)# name VM
CESW01A (config)# vlan 235
CESW01A (config-vlan)# name CS
CESW01A (config)# vlan 21
CESW01A (config-vlan)# name TI

CESW01A (config-vlan)# end

CESW01A (config)# interface range Gi1/1-3
CESW01A (config-if)# switchport mode trunk
CESW01A (config-if)# switchport trunk allowed vlan all
CESW01A (config)# interface range Gi1/4-8
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 1
CESW01A (config)# interface range Gi1/9-10
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 230
CESW01A (config)# interface range Gi1/11-12
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 231
CESW01A (config)# interface range Gi1/13-14
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 233
CESW01A (config)# interface Gi1/15
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 230
CESW01A (config)# interface Gi1/16
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 233
CESW01A (config)# interface range Gi1/17-18
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 234
CESW01A (config)# interface Gi1/19
CESW01A (config-if)# switchport mode trunk
CESW01A (config-if)# switchport trunk allowed vlan all
CESW01A (config)# interface Gi1/20
```

```
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 199
CESW01A (config)# interface rangeGi1/21-22
CESW01A (config-if)# switchport mode trunk
CESW01A (config-if)# switchport trunk allowed vlan all
CESW01A (config)# interface Gi1/23
CESW01A (config-if)# switchport mode access
CESW01A (config-if)# switchport access vlan 21
CESW01A (config)# interface Gi1/24
CESW01A (config-if)# switchport mode trunk
CESW01A (config-if)# switchport trunk allowed vlan all

CESW01A (config-vlan)# end

CESW01A (config)# ntp server direcciónIPGPS
CESW01A (config)# clock time LIM -5

CESW01A (config)# logging direcciónIPdelSysLog
CESW01A (config)# logging trap 4
CESW01A (config)# source-interfaceGi1/9
CESW01A (config)# end

CESW01A (config)# do wr
```

4. Se Verifico la correcta configuración del switch CESW01A, desde la Estación de ingeniería, equipo que gestiona todos los accesos de los ciberactivo.

Figura 37

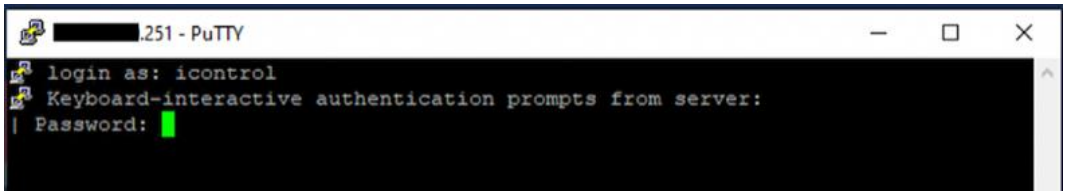
Consola del software Putty para el acceso al CLI del switch CESW10A, usando el protocolo SHH.



Fuente: Propia

Figura 38

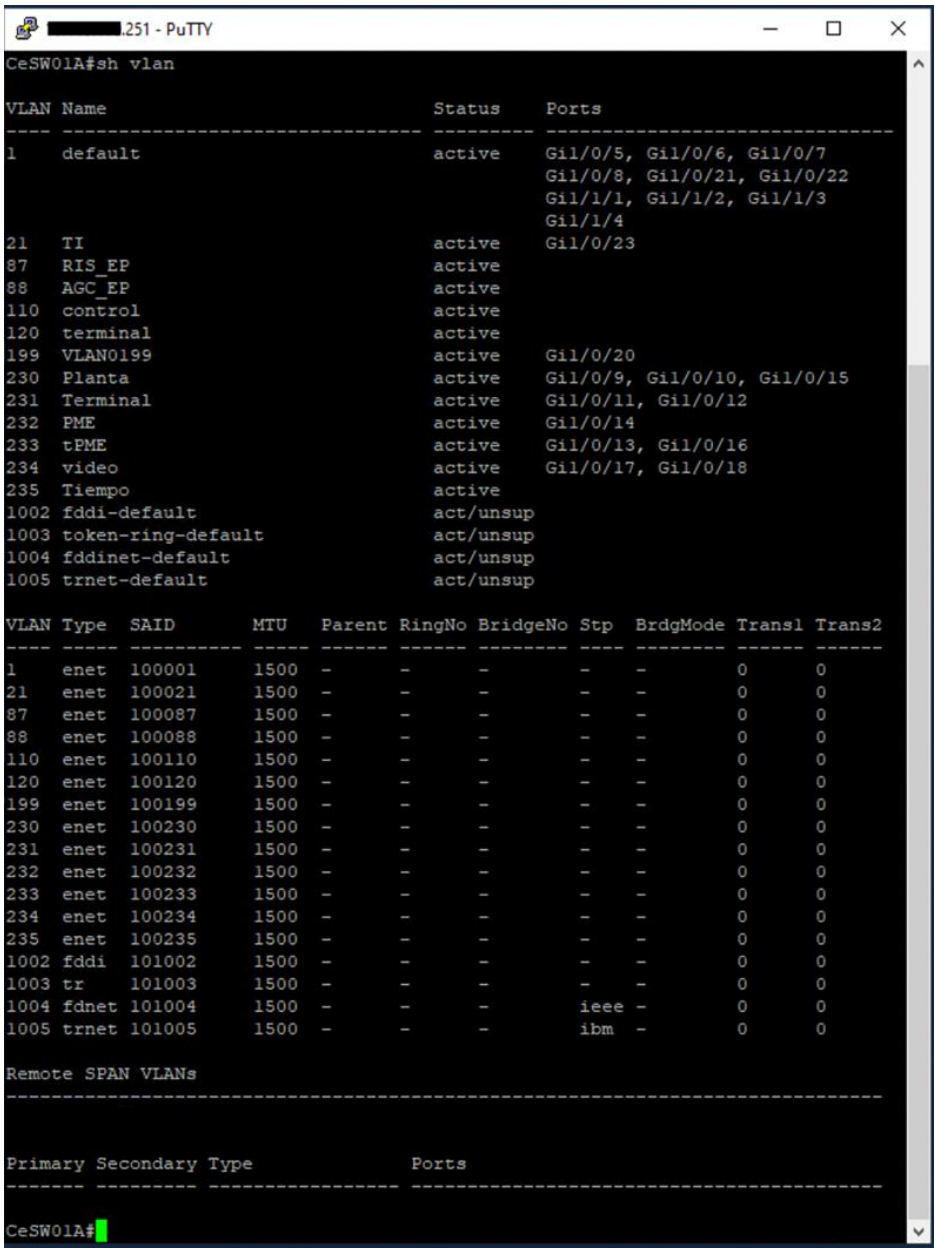
CLI que solicito las credenciales para acceso al switch CESW10A.



Fuente: Propia

Figura 39

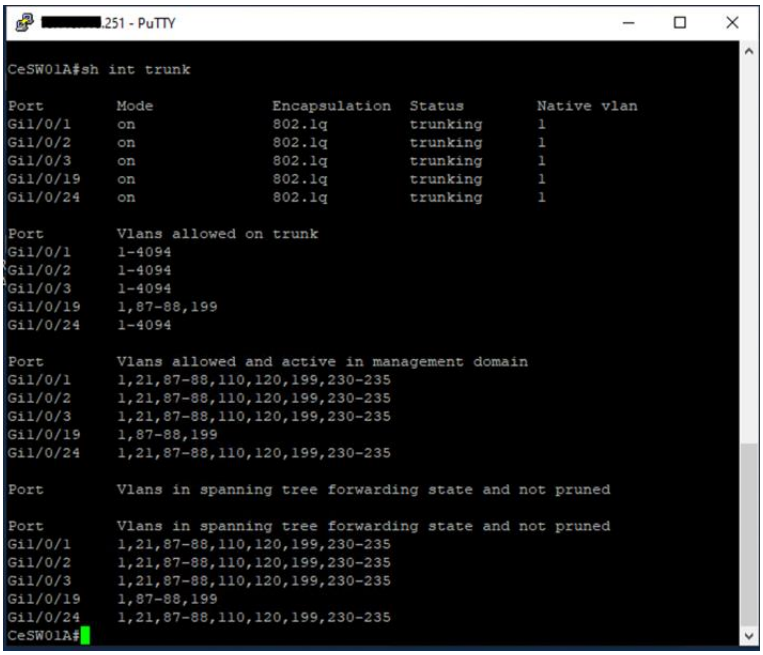
CLI que mostro las VLAN creadas en el switch CESW10A.



Fuente: Propia

Figura 40

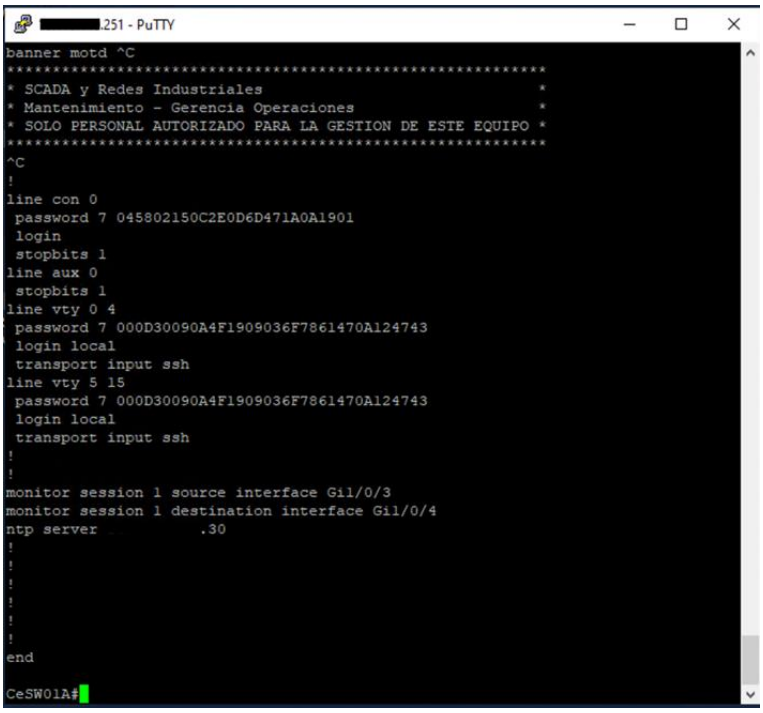
Interfaces troncales creadas en el switch CESW10A.



Fuente: Propia

Figura 41

Encriptación de credenciales que fue creada en el switch CESW10A.



Fuente: Propia

5. Luego que se concluyó con la programación del switch CESW01A, se escribió los siguientes comandos en el CLI, del switch CESW01B:

```
Switch# enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname CESW01B

CESW01B (config)# enable secret contraseñaPrivilegiada

CESW01B (config)# line console 0
CESW01B (config-line)# password contraseñaConsola
CESW01B (config-line)# login
CESW01B (config-line)# exit

CESW01B (config)# ip domain name iacs.com
CESW01B (config)# username user privilege 15 secret 0 contraseña
CESW01B (config)# crypto key generate rsa
               1024 y enter
CESW01B (config)# ip ssh version 2
CESW01B (config)# line vty 0 15
CESW01B (config-line)# login local
CESW01B (config-line)# exit

CESW01B (config)# service password-encryption

CESW01B (config)# interface vlan1
CESW01B (config-if)# ip address A.A.A.251
CESW01B (config-if)# no sh
CESW01B (config-if)# exit

CESW01B (config)# ip default-gateway A.A.A.1

CESW01B (config)# vlan 199
CESW01B (config-vlan)# name ICCP
CESW01B (config)# vlan 230
CESW01B (config-vlan)# name SCADA
CESW01B (config)# vlan 231
CESW01B (config-vlan)# name tSCADA
CESW01B (config)# vlan 232
CESW01B (config-vlan)# name PME
CESW01B (config)# vlan 233
CESW01B (config-vlan)# name tPME
CESW01B (config)# vlan 234
CESW01B (config-vlan)# name VM
CESW01B (config)# vlan 235
CESW01B (config-vlan)# name CS
CESW01B (config)# vlan 21
CESW01B (config-vlan)# name TI

CESW01B (config-vlan)# end

CESW01B (config)# interface range Gi1/1-3
CESW01B (config-if)# switchport mode trunk
CESW01B (config-if)# switchport trunk allowed vlan all
CESW01B (config)# interface range Gi1/4-8
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 1
CESW01B (config)# interface range Gi1/9-10
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 230
CESW01B (config)# interface range Gi1/11-12
```

```
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 231
CESW01B (config)# interface range Gi1/13-14
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 233
CESW01B (config)# interface Gi1/15
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 230
CESW01B (config)# interface Gi1/16
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 233
CESW01B (config)# interface range Gi1/17-18
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 234
CESW01B (config)# interface Gi1/19
CESW01B (config-if)# switchport mode trunk
CESW01B (config-if)# switchport trunk allowed vlan all
CESW01B (config)# interface Gi1/20
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 199
CESW01B (config)# interface rangeGi1/21-22
CESW01B (config-if)# switchport mode trunk
CESW01B (config-if)# switchport trunk allowed vlan all
CESW01B (config)# interface Gi1/23
CESW01B (config-if)# switchport mode access
CESW01B (config-if)# switchport access vlan 21
CESW01B (config)# interface Gi1/24
CESW01B (config-if)# switchport mode trunk
CESW01B (config-if)# switchport trunk allowed vlan all

CESW01B (config-vlan)# end

CESW01B (config)# ntp server direcciónIPGPS
CESW01B (config)# clock time LIM -5

CESW01B (config)# logging direcciónIPdelSysLog
CESW01B (config)# logging trap 4
CESW01B (config)# source-interfaceGi1/9
CESW01B (config)# end

CESW01B (config)# do wr
```

Figura 42

Se muestra los dos switches; CESW01A y CESW01B instalado en el gabinete IACS en el Data Center de CELEPSA.

Fuente: Propia

3.4.3. POLITICAS DE CIBERSEGURIDAD PARA CCC

Después que se concluyó con la configuración a los firewalls y la programación a los switches que fueron indicados en el Capítulo 3.4.1, se ingresó las políticas de seguridad con el fin de ampliar la defensa en profundidad para la protección de la red IACS del CCC. Si esta actividad no hubiera sido efectuada, implicaba tener la red abierta para una conexión abierta a cualquier host, esto quiere decir: todas las redes IACS se comunicarían contra todas las redes IACS del CCC y posiblemente con la red TI.

Tabla 13

Detalle de las políticas de seguridad que fue aplicado en la red IACS del CCC.

No.	Source	Destination	Services & Applications
1	FW01C	FW01A FW01B CeLi	Any
2	FW01A FW01B CeLi	FW01C	Any
3	FW01C	Any	Any
4	OSS01	EP_VLan241	S7 protocol
5	OSS01	EP_RTU	TCP_2404 TCP_2405 ICMP Protocol
6	OSS01	EP_AS05 EP_AS05cpu	S7 protocol
7	OSS01	EP_AS07 EP_AS07cpu	S7 protocol
8	OSS01	HM_AS00to04 HM_AS05	S7 protocol
9	OSS01	HM_AS06 HM_AS07	Any
10	OSS01	HM_RTU01to03 HM_RTU04 HM_RTU5A HM_RTU5B	TCP_2404 TCP_2405 ICMP Protocol

11	OSNPM	EP_VLanAdm HM_VLanAdmin EP_VLan241 EP_VLan111 EP_VLan112 CP_ES30 EP_Fw10cons EP_Fw10	snmp ICMP Protocol
12	ES01	EP_Fw10cons	ICMP Protocol
13	ES01	EP_VLanAdm	https http
14	ES01	EP_ES10 EP_PG10	Remote_Desktop_Protocol ICMP Protocol
15	ES01	EP_Fw10	TCP_4434
16	ES01	EP_SwOT EP_Sw10	ssh_version_2
17	ES01	EP_OSS11A EP_OSS11B EP_BD11 EP_OS11	Remote_Desktop_Protocol
18	ES01	EP_VLan241	S7 protocol ICMP Protocol
19	ES01	EP_RTU	S7 protocol TCP_2404 TCP_2405
20	ES01	EP_VLan245	S7 protocol
21	ES01	EP_VLan246	S7 protocol
22	ES01	EP_AS05 EP_AS05cpu	S7 protocol ICMP Protocol
23	ES01	EP_OS10	ICMP Protocol Remote_Desktop_Protocol TightVNC
24	ES01	EP_AS07 EP_AS07cpu EP_HMI07	S7 protocol ICMP Protocol ssh_version_2 https http
25	ES01	HM_SwOT HM_Sw20	ssh_version_2 telnet http https

26	ES01	HM_SwOT	ssh_version_2 telnet http https
27	ES01	HM_SwOT	telnet http https ssh_version_2 ICMP Protocol
28	ES01	HM_Sw20	ssh_version_2 ICMP Protocol
29	ES01	HM_ESP20 HM_OS20	Remote_Desktop_Protocol smb ICMP Protocol
30	ES01	ES02	smb
31	ES02	HM_VLanAdmin	https http ssh_version_2 smb ICMP Protocol Remote_Desktop_Protocol
32	ES02	HM_AS00to04 HM_AS05	S7 protocol
33	ES02	HM_AS06 HM_AS07	S7 protocol
34	ES02	HM_ESP20 HM_OS20	Remote_Desktop_Protocol
35	ESP01	EP_VLanAdm	https http ssh_version_2 smb ICMP Protocol Remote_Desktop_Protocol
36	ESP01	HM_VLanAdmin	Remote_Desktop_Protocol
37	ESP01	HM_OS20 HM_ESP20	smb ICMP Protocol Remote_Desktop_Protocol

38	ESP01	HM_RTU04 HM_RTU5A HM_RTU5B	Any
39	10.110.112.12	DMZ_CSS	Any
40	OSS01t	DMZ_CSS	ICMP Protocol
41	ES01	DMZ_PMES	Remote_Desktop_Protocol ICMP Protocol
42	ES01	172.17.0.121	Any
43	ES01	172.17.0.111	Any
44	ES01	CP_ESC1	RDP rdp2tcp ICMP Protocol
45	ES01	172.17.0.122	Any
46	ES01	172.17.0.112	Any
47	ES01	172.17.0.101	Any
48	ES01	172.17.0.102	Any
49	ES01	CP_ESC3	Any
50	ES01	CP_OSC3	Any
51	ES02	CP_AS01 CP_HMI01	ICMP Protocol TCP_ABB
52	ES02	CP_AS02 CP_HMI02	ICMP Protocol TCP_ABB
53	ES02	CP_AS03 CP_HMI03	ICMP Protocol TCP_ABB
54	ES02	CP_AS00 CP_HMI00	ICMP Protocol TCP_ABB
55	ES02	CP_AS04cpu CP_AS04	ICMP Protocol S7 protocol
56	ES02	CP_AS05 CP_AS05cpu	ICMP Protocol S7 protocol
57	ES02	CP_AS06cpu CP_AS06	S7 protocol ICMP Protocol
58	ES02	CP_IOAC CP_IOLoadCh CP_HMI05 CP_HMI06 CP_PMBusBar CP_PMSST CP_PMG04 CP_PMG05	ICMP Protocol S7 protocol

59	OSS01	CP_AS04cpu CP_AS04	ICMP Protocol S7 protocol
60	OSS01	CP_AS05cpu CP_AS05	ICMP Protocol S7 protocol
61	OSS01	CP_AS06cpu CP_AS06	S7 protocol ICMP Protocol
62	ES01 ES02	CP_Se30	ICMP Protocol snmp https
63	ES01 ES02	CP_VM30	ICMP Protocol snmp https
64	OSNPM	CP_VM30	ICMP Protocol snmp https
65	ES01	CP_ES30	ICMP Protocol S7 protocol TCP_2408 Remote_Desktop_Protocol
66	ES01	172.16.0.101	Any
67	ES01	CP_Wks02	Any
68	ES02	CP_ES30	ICMP Protocol S7 protocol TCP_2408 Remote_Desktop_Protocol
69	OSS01	CP_ES30	ICMP Protocol S7 protocol TCP_2404 TCP_2405 TCP_48050
70	OSNPM	EP_OSS11A	Any
71	OSNPM	EP_OSS11B	Any

72	ES02	EP_VLan240 EP_VLan241 EP_VLan242 EP_VLan243 EP_VLan244 EP_VLan245 EP_VLan246 EP_VLan247	ICMP Protocol S7 protocol
73	ES02	EP_ES10	Remote_Desktop_Protocol ICMP Protocol
74	ES02	EP_ES10	Remote_Desktop_Protocol
75	ES02	EP_OS10	Remote_Desktop_Protocol
76	ES02	EP_AS07 EP_AS07cpu EP_HMI07	S7 protocol ICMP Protocol ssh_version_2 https http
77	OS01	DMZ_PMES	TCP_48050 ICMP Protocol

Fuente: Propia

3.5. REDES IACS: PLATANAL

En esta área operativa se segregó la red de TI y la red IACS, se cambiaron la totalidad de los switches debido a que no manejaban VLAN, además se implementó las contramedidas recomendadas por el IEC 62443.

3.5.1. REQUERIMIENTOS DE EQUIPOS

Se compraron los ciberactivos necesarios para segregar y segmentar la red IACS del EP y estos son expuestas en la Tabla 14 de forma general:

Tabla 14
Necesidades de equipos de red y seguridad perimetral para la implementación de la red IACS de EP.

Requerimientos	Modelo	Marca	Tag
Switch	EI 3200	Cisco	EPSW10A/B
Switch	EI 2000	Cisco	EPSW00/1/2/3
Firewall	1570R	Check Point	CEFW01A/B

Fuente: Propia

Para un mayor detalle de los ciberactivos comprados estos se adquirieron con los detalles mostrados en la Tabla 15 y Tabla 16 para los switch y Tabla 17 para los firewalls.

Tabla 15
Requerimientos de swicthes empleados para la implementación de la red IACS de EP.

Numero de Parte	Descripción	Cantidad
IE-3200-8T2S-E	Catalyst IE3200 w/ 8 GE Copper & 2 GE SFP, Fixed System, NE 2	2
PWR-IE65W-PC-DC	POE DC Input Power Module for IE3000/2000	2
IOT-UTILITIES	Utilities Industry Solutions; For tracking only.	2
IOT-SUBSTATION	Substation Automation; For tracking only.	2
IE3200-DNA-E	Cisco DNA Essentials license for IE3200 Series	2
IE3200-DNA-E-3Y	IE 3200 DNA Essentials, 3 Year Term license	2
GLC-FE-100FX-RGD=	100Base-FX Multi ModeRugged SFP	4

Fuente: Propia

Figura 43

Mostramos imagen de un switch IE3200 de cisco, instalado en el gabinete IACS, con TAG CDA10 en el EP de CELEPSA.

Fuente: Propia

Tabla 16

Requerimientos de switch para la implementación de la red IACS de EP.

Numero de Parte	Descripción	Cantidad
IE-2000-8TC-B	IE2000 with 8FE Copper ports and 2FE uplinks (Lan Base)	4
IOT-UTILITIES	Utilities Industry Solutions; For tracking only.	4
IOT-SUBSTATION	Substation Automation; For tracking only.	4
STK-RACK-DINRAIL=	19" DINRAIL kit to replace STK-RACKMNT-2955=	4
GLC-FE-100FX-RGD=	100Base-FX Multi ModeRugged SFP	8

Fuente: Propia

Figura 44

Mostramos imagen de un switch IE2000 de cisco, instalado en cada UAC en EP.

Fuente: Propia

Tabla 17

Requerimientos de firewalls empleados para la implementación de la red IACS de EP.

Numero de Parte	Descripción	Cantidad
CPAP-SG1570R-SNBT	1570R Ruggedized Next Generation Appliance with DC power	2
CPES-SS-STANDARD-ADD	Standard Direct Enterprise Support For 1 Year 1	1

Fuente: Propia

3.5.2. CONFIGURACIONES DE EQUIPOS

Primero se efectuó el inventario de todos los SUC detallando como mínimo: Nombre, dirección IP, mascara y gateway.

Tal y como se hizo para la red IACS del CCC, por temas de ciberseguridad ocultaremos la dirección IP de cada ciberactivo de este proyecto, pero para una equivalencia indicaremos que los tres primeros octetos de la dirección IP será representado por una letra de abecedario, de los cuales:

- El primer octeto representara su área operativa.
- El tercer octeto representara a la VLAN que pertenece.
- El cuarto octeto representa la dirección del host.

Tabla 18

SUC que pertenecen a la VLAN 240, dentro de la red IACS de EP, identificación y direccionamiento IP.

Nombre	Tag	Equipo	IP	Gateway
Firewall 10V	FW10V	Firewall	B.B.A.1/*	-
Firewall 10A	FW10A	Firewall	B.B.A.2/*	-
Firewall 10B	FW10B	Firewall	B.B.A.3/*	-
Switch 00	SW00	Switch L2	B.B.A.10/*	B.B.A.1
Switch 01	SW01	Switch L2	B.B.A.11/*	B.B.A.1
Switch 02	SW02	Switch L2	B.B.A.12/*	B.B.A.1
Switch 03	SW03	Switch L2	B.B.A.13/*	B.B.A.1
Switch 04	SW04	Switch L2	B.B.A.19/*	B.B.A.1
Switch 05	SW04	Switch L2	B.B.A.19/*	B.B.A.1
Switch 07	SW04	Switch L2	B.B.A.19/*	B.B.A.1
Consola FW	FW10c	Switch L2	B.B.A.250/*	B.B.A.1
Switch 10A	SW10A	Switch L2	B.B.A.251/*	B.B.A.1
Switch 10B	SW10B	Switch L2	B.B.A.252/*	B.B.A.1

Direccionamiento IP equivalente de la infraestructura de red IACS dentro de la VLAN 240.

Fuente: Propia

Tabla 19

SUC de EP, identificación y direccionamiento IP.

Nombre	Tag	VLAN	IP
PLC #5	AS05	111	B.A.A.4
PLC #5	AS05	111	B.A.A.235
PLC #8	AS08	111	B.A.A.238
HMI 02	HMI2	111	B.A.A.12
PLC #7	AS07	112	B.A.B.217
HMI 03	HMI3	112	B.A.B.234
Host	*	240	B.B.C.*
PLC #0	AS00	241	B.B.D.4
PLC #1	AS01	241	B.B.D.5
PLC #2	AS02	241	B.B.D.6
PLC #3	AS03	241	B.B.D.7
PLC #4	AS04	241	B.B.D.8
PLC #6	AS06	241	B.B.D.9
ZPU5000 #01	ZPU01	241	B.B.D.10
ZPU5000 #02	ZPU02	241	B.B.D.11
HMI 01	HMI1	241	B.B.D.12
PLC #5.1	AS05 PN	241	B.B.D.16
GPS	GPS	241	B.B.D.20
RTU 00	RTU00	242	B.B.E.4
RTU 01	RTU01	242	B.B.E.5
RTU 02	RTU02	242	B.B.E.6
RTU 03	RTU03	242	B.B.E.7
RTU 04	RTU04	242	B.B.E.8
Recloser	Recloser	243	B.B.F.11
Medidor #03	EMU03	100	B.B.B.4
Medidor #04	EMU04	100	B.B.B.5
Medidor #0A	EMU00A	100	B.B.B.6
Medidor #01	EMU01	100	B.B.B.7
Medidor #02	EMU02	100	B.B.B.8
Medidor #05	EMU05	100	B.B.B.10
Medidor #06	EMU06	100	B.B.B.11
GPS 01	GPS01	100	B.B.B.13
Medidor #07	EMU07	101	*.*.*.4
GPS 02	GPS02	244	B.B.G.4
GPS 03	GPS03	244	B.B.G.5
PLC #2	AS02	245	B.B.H.4

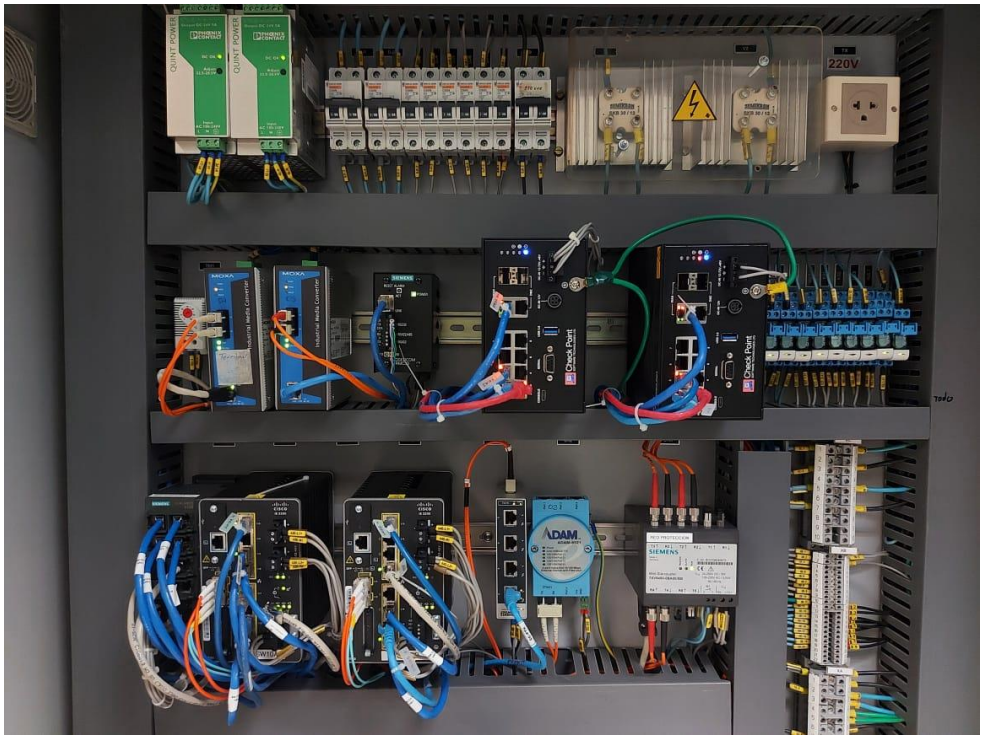
PLC 1.2	AS12	245	B.B.H.5
PLC 1.3	AS13	245	B.B.H.6
PLC 1.4	AS14	245	B.B.H.7
PLC 1.5	AS15	245	B.B.H.8
HMI 1.1	HMI11	245	B.B.H.9
HMI 1.2	HMI12	245	B.B.H.10
HMI 1.3	HMI13	245	B.B.H.11
HMI 1.4	HMI14	245	B.B.H.12
PLC 2.2	AS01	246	B.B.I.4
PLC 2.3	AS08	246	B.B.I.5
PLC 2.4	AS09	246	B.B.I.6
PLC 2.5	AS10	246	B.B.I.7
PLC 2.6	AS11	246	B.B.I.8
HMI 2.1	HMI21	246	B.B.I.9
HMI 2.2	HMI22	246	B.B.I.10
HMI 2.3	HMI23	246	B.B.I.11
HMI 2.4	HMI24	246	B.B.I.12

Direccionamiento IP equivalente de los equipos de Control de la red IACS.

Fuente: Propia

Figura 45

Mostramos el NGFW y los switches instalados en el Tablero con Tag CDA10 en EP.



Fuente: Propia

3.5.2.1. CONFIGURACION DE LOS FIREWALL CON EL OBJETIVO DE SEGREGAR LA RED IACS DE EL PATANAL

Tal y como se efectuó en el CCC, con el objetivo de segregar la red IACS y la red TI, se usó y se configuro los dos Firewall de la Tabla 17, además se habilito la gestión de rutas entre VLAN para las comunicaciones entre ellas, y después se detallaron y aplicaron las políticas de ciberseguridad para esta red IACS del CCC.

Repetimos los pasos que se efectuó en el Capítulo 3.4.2.1, pero en el paso 7, se ingresó la siguiente tabla 20

Tabla 20
Direccionamiento IP para el tráfico de VLAN para la red IACS del EP.

Función	Gateway	Puerto	Puerto	Conexión
Cluster	LAN1	LAN1	LAN1	
	B.B.A.1	B.B.A.2	B.B.A.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.100	LAN3.100	LAN3.100	
	B.B.B.1	B.B.B.2	B.B.B.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.240	LAN3.240	LAN3.240	
	B.B.C.1	B.B.C.2	B.B.C.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.241	LAN3.241	LAN3.241	
	B.B.D.1	B.B.D.2	B.B.D.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.242	LAN3.242	LAN3.242	
	B.B.E.1	B.B.E.2	B.B.E.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.243	LAN3.243	LAN3.243	
	B.B.F.1	B.B.F.2	B.B.F.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.244	LAN3.244	LAN3.244	
	B.B.G.1	B.B.G.2	B.B.G.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.245	LAN3.245	LAN3.245	
	B.B.H.1	B.B.H.2	B.B.H.3	Internal
	mascara	mascara	mascara	
Cluster	LAN3.246	LAN3.246	LAN3.246	
	B.B.I.1	B.B.I.2	B.B.I.3	Internal

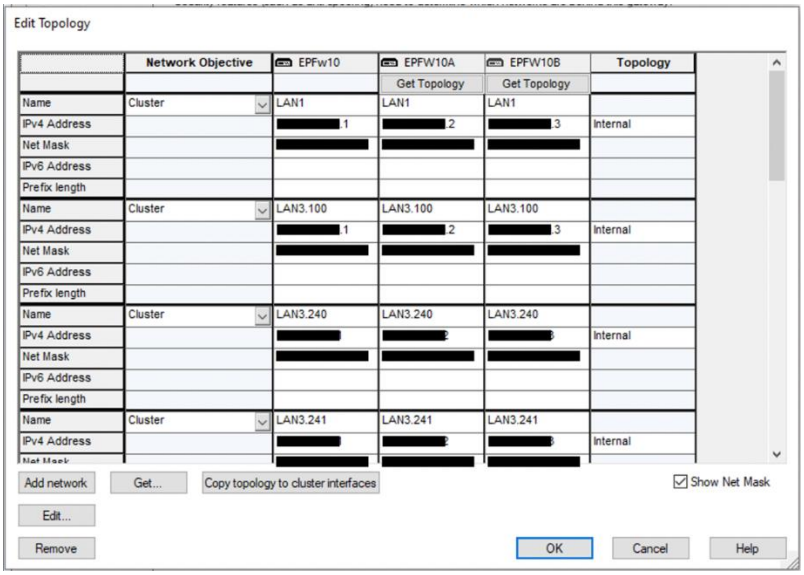
	mascara	mascara	mascara	
Cluster	LAN3.247	LAN3.247	LAN3.247	
	B.B.J.1	B.B.J.2	B.B.J.3	Internal
	mascara	mascara	mascara	
Cluster	WAN	WAN	WAN	
	B.B.Z.3	B.B.Z.4	B.B.Z.5	External
	mascara	mascara	mascara	
1st Sync		LAN2	LAN2	
		B.B.K.2	B.B.K.1	Internal
		mascara	mascara	

Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

Figura 46

Visualización de las redes que fueron agregadas a los firewalls para la red IACS del EP.

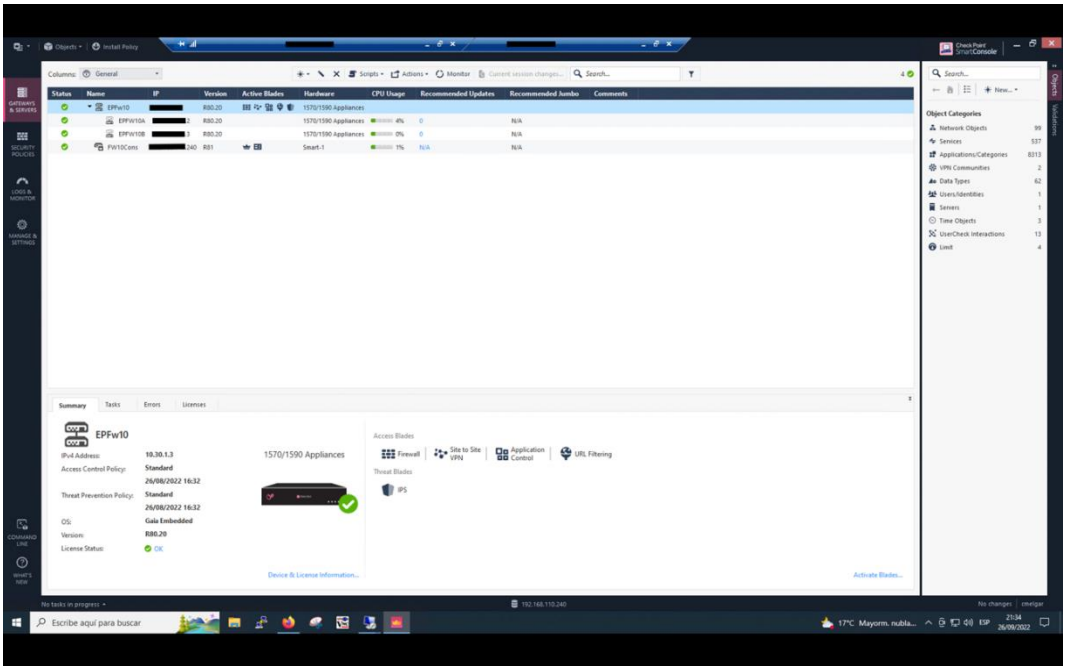


Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

Figura 47

Visualización de los firewalls integrados para la red IACS de E.

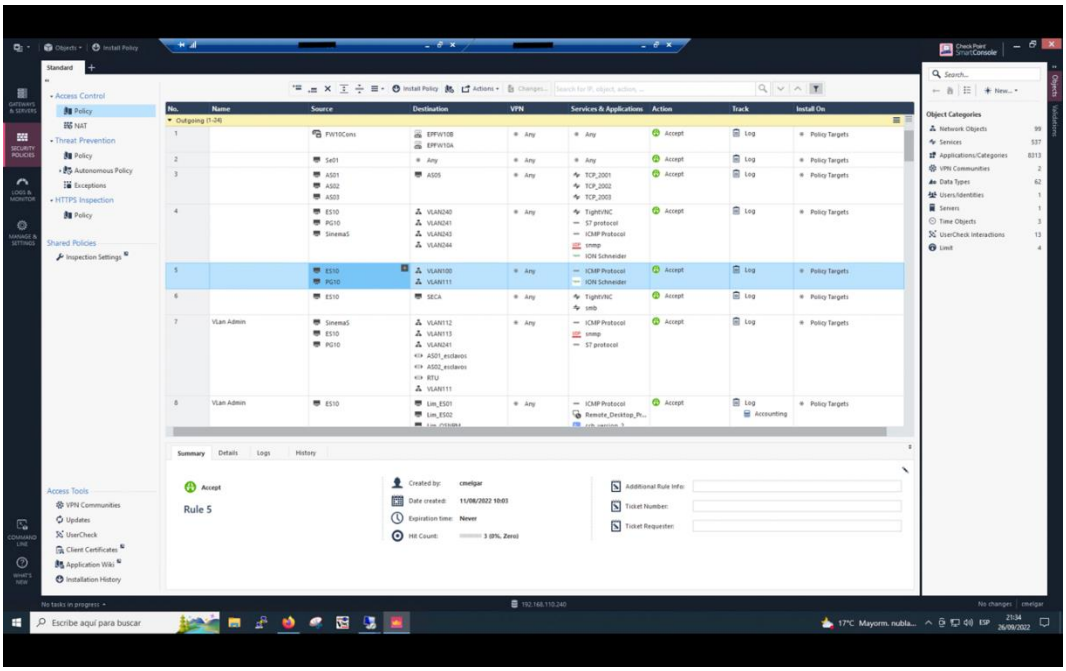


Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

Figura 48

Visualización de las políticas de los dos firewalls integrados de la red IACS del EP.



Fuente: Propia

Se siguió con repetir el paso 10 del Capítulo 3.4.2.1.

3.5.2.2. CONFIGURACION DE LOS SWITCHES CON EL OBJETIVO DE SEGMENTAR LA RED IACS DE EP

Después que se terminó con la segregación de la red IACS y la red TI, se inició la actividad en los switches que consistió en: programación básica y el uso de VLAN. Este ultimó que permitió la conectividad entre los SUC de la misma VLAN y la conexión entre SUC permitidos de diferentes VLAN. De manera breve se efectuaron los siguientes pasos para la programación de los dos switches.

1. Efectuamos los pasos 1 y 2 del Capítulo 3.4.2.2.
2. Escribir los siguientes comandos en el CLI, del switch EPSW10A:

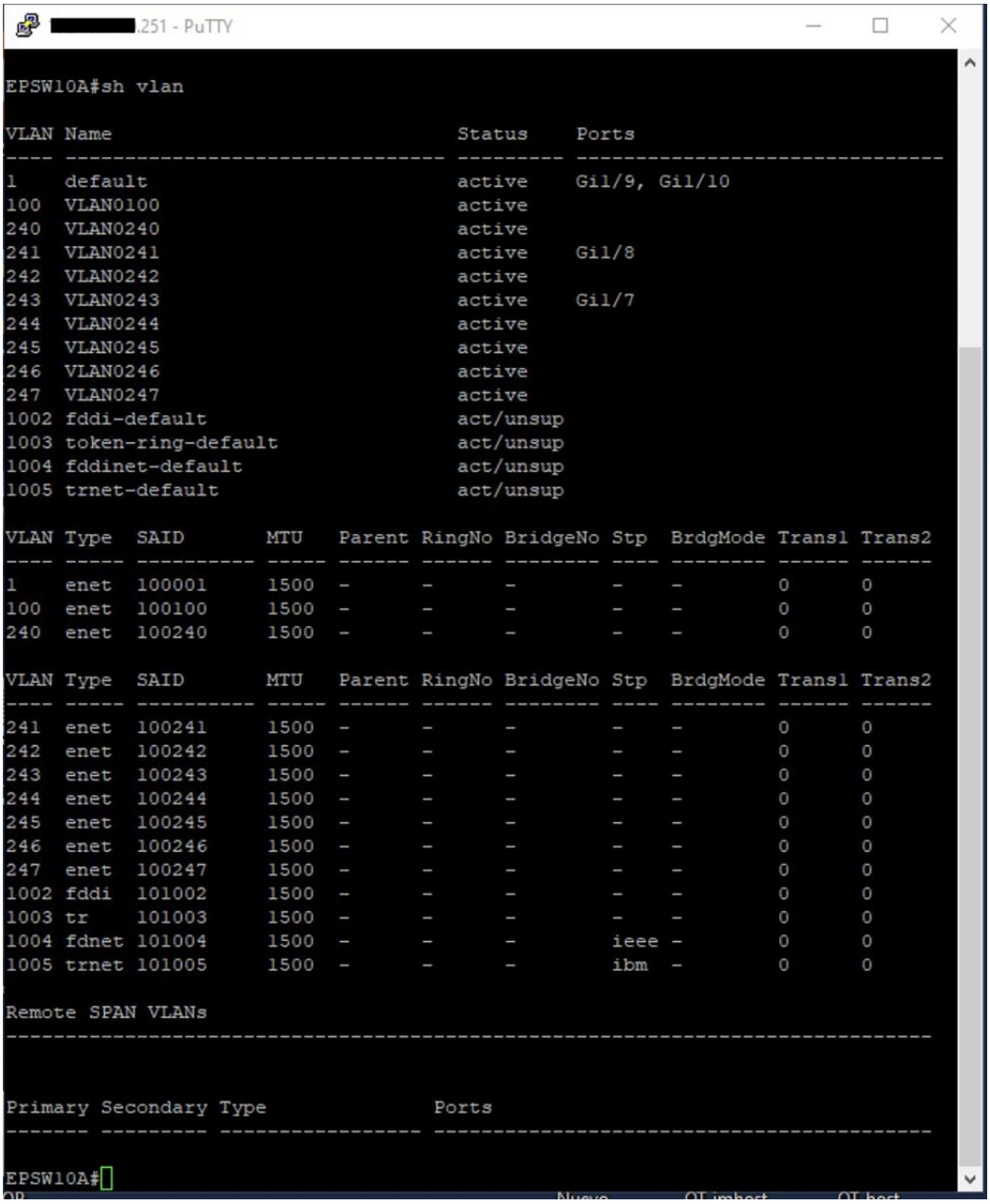
```
Switch# enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname EPSW10A

EPSW10A (config)# enable secret contraseñaPrivilegiada

EPSW10A(config)# line console 0
EPSW10A (config-line)# password contraseñaConsola
EPSW10A (config-line)# login
EPSW10A (config-line)# exit

EPSW10A (config)# ip domain name iacs.com
EPSW10A (config)# username user privilege 15 secret 0 contraseña
EPSW10A (config)# crypto key generate rsa
        1024 y enter
EPSW10A (config)# ip ssh version 2
EPSW10A (config)# line vty 0 15
EPSW10A (config-line)# login local
EPSW10A (config-line)# exit

EPSW10A (config)# service password-encryption

EPSW10A (config)# interface vlan 1
EPSW10A (config-if)# ip address B.B.A.251 mascara
EPSW10A (config-if)# no sh
EPSW10A (config-if)# exit

EPSW10A (config)# ip default-gateway B.B.A.1

EPSW10A (config)# interface Gi1/1
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all
EPSW10A (config)# interface Gi1/2
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all
EPSW10A (config)# interface Gi1/3
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all
```

```
EPSW10A (config)# interface Gi1/5
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all
EPSW10A (config)# interface Gi1/6
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all


EPSW10A (config)# interface Gi1/7
EPSW10A (config-if)# switchport mode access
EPSW10A (config-if)# switchport access vlan 243
EPSW10A (config)# interface Gi1/8
EPSW10A (config-if)# switchport mode access
EPSW10A (config-if)# switchport access vlan 241
EPSW10A (config)# interface range Gi1/9-10
EPSW10A (config-if)# switchport mode trunk
EPSW10A (config-if)# switchport trunk allowed vlan all
EPSW10A (config-vlan)# end

EPSW10A (config)# ntp server direcciónIPGPS
EPSW10A (config)# clock time LIM -5

EPSW10A (config)# logging direcciónIPdelSysLog
EPSW10A (config)# logging trap 4
EPSW10A (config)# source-interfaceGi1/9
EPSW10A (config)# end

EPSW10A (config)# do wr
```

3. Se Verifico la correcta configuración del switch EPSW01A, desde la Estación de Ingeniería 01, equipo que gestiona todos los accesos de los ciberactivo desde el CCC.

Figura 49

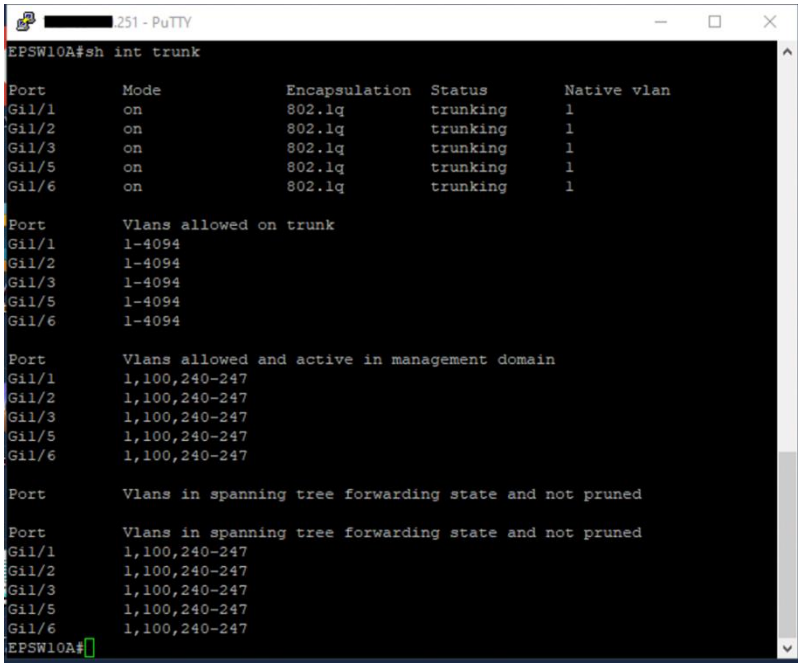
CLI que muestra las VLAN creadas en el switch EPSW10A.



Fuente: Propia

Figura 50

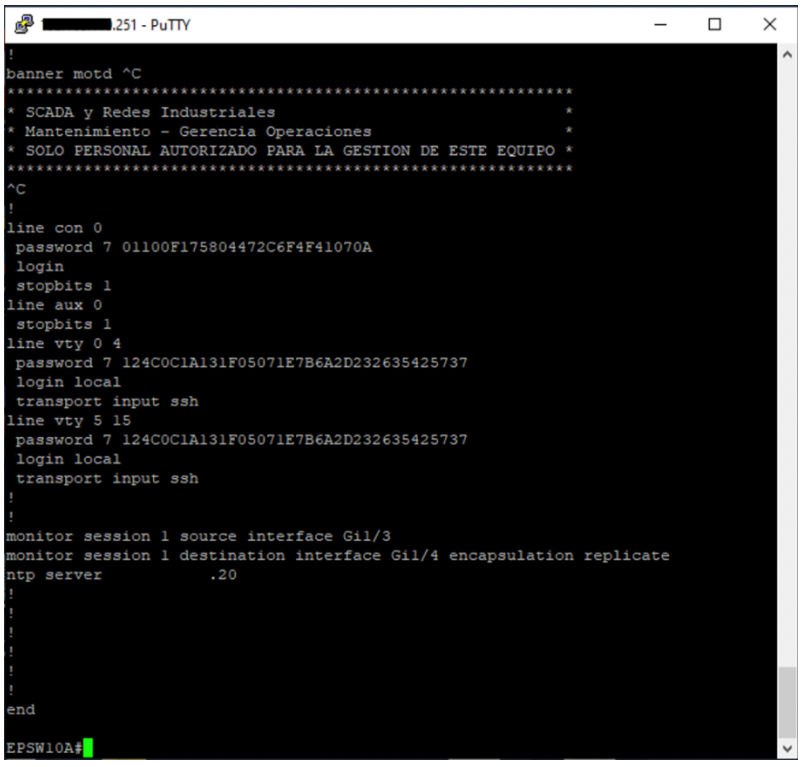
Interfaces troncales creadas en el switch EPSW10A.



Fuente: Propia

Figura 51

Encriptación de credenciales que fue creada en el switch EPSW10A.



Fuente: Propia

4. Luego que se concluyó con la programación del switch EPSW01A, se escribió los siguientes comandos en el CLI, del switch EPSW01B:

```
Switch# enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname EPSW10B

EPSW10B (config)# enable secret contraseñaPrivilegiada

EPSW10B (config)# line console 0
EPSW10B (config-line)# password contraseñaConsola
EPSW10B (config-line)# login
EPSW10B (config-line)# exit

EPSW10B (config)# ip domain name iacs.com
EPSW10B (config)# username user privilege 15 secret 0 contraseña
EPSW10B (config)# crypto key generate rsa
       1024 y enter
EPSW10B (config)# ip ssh version 2
EPSW10B (config)# line vty 0 15
EPSW10B (config-line)# login local
EPSW10B (config-line)# exit

EPSW10B (config)# service password-encryption

EPSW10B (config)# interface vlan 1
EPSW10B (config-if)# ip address B.B.A.252 mascara
EPSW10B (config-if)# no sh
EPSW10B (config-if)# exit

EPSW10B (config)# ip default-gateway B.B.A.1

EPSW10B (config)# interface Gi1/1
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
EPSW10B (config)# interface Gi1/2
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
EPSW10B (config)# interface Gi1/3
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
EPSW10B (config)# interface Gi1/5
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
EPSW10B (config)# interface Gi1/6
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
EPSW10B (config)# interface Gi1/7
EPSW10B (config-if)# switchport mode access
EPSW10B (config-if)# switchport access vlan 243
EPSW10B (config)# interface Gi1/8
EPSW10B (config-if)# switchport mode access
EPSW10B (config-if)# switchport access vlan 241
EPSW10B (config)# interface range Gi1/9-10
EPSW10B (config-if)# switchport mode trunk
EPSW10B (config-if)# switchport trunk allowed vlan all
```

```
EPSW10B (config-vlan)# end

EPSW10B (config)# ntp server direcciónIPGPS
EPSW10B (config)# clock time LIM -5

EPSW10B (config)# logging direcciónIPdelSysLog
EPSW10B (config)# logging trap 4
EPSW10B (config)# source-interfaceGi1/9
EPSW10B (config)# end

EPSW10B (config)# do wr
```

5. Después de la configuración efectuada en los switches EPSW10A/B, se efectuó lo propio en los switch EPSA00/01/02/03, pero temas de repetitividad solo mostraremos las líneas del EPSA00/01.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname EPSW00

EPSW00 (config)# enable secret contraseñaPrivilegiada

EPSW00(config)# line console 0
EPSW00 (config-line)# password contraseñaConsola
EPSW00 (config-line)# login
EPSW00 (config-line)# exit

EPSW00 (config)# ip domain name iacs.com
EPSW00 (config)# username user privilege 15 secret 0 contraseña
EPSW00 (config)# crypto key generate rsa
       1024 y enter
EPSW00 (config)# ip ssh version 2
EPSW00 (config)# line vty 0 15
EPSW00 (config-line)# login local
EPSW00 (config-line)# exit

EPSW00 (config)# service password-encryption

EPSW00 (config)# interface vlan1
EPSW00 (config-if)# ip address b.b.b.10 mascara
EPSW00 (config-if)# no sh
EPSW00 (config-if)# exit

EPSW00 (config)# ip default-gateway b.b.b.1

EPSW00 (config)# vlan 100
EPSW00 (config-vlan)# name ION
EPSW00 (config)# vlan 240
EPSW00 (config-vlan)# name SCADA
EPSW00 (config)# vlan 241
EPSW00 (config-vlan)# name Terminal
EPSW00 (config)# vlan 242
EPSW00 (config-vlan)# name IEC
EPSW00 (config)# vlan 243
EPSW00 (config-vlan)# name Electricidad
EPSW00 (config)# vlan 244
EPSW00 (config-vlan)# name VSM
EPSW00 (config)# vlan 245
```

```
EPSW00 (config-vlan)# name AS01
EPSW00 (config)# vlan 246
EPSW00 (config-vlan)# name AS02
EPSW00 (config)# vlan 247
EPSW00 (config-vlan)# name SCADAt
EPSW00 (config-vlan)# end

EPSW00 (config)# interfaceGi1/1
EPSW00 (config-if)# switchport mode access
EPSW00 (config-if)# switchport access vlan 240
EPSW00 (config)# interfaceGi1/2
EPSW00 (config-if)# switchport mode access
EPSW00 (config-if)# switchport access vlan 241
EPSW00 (config)# interfaceGi1/3
EPSW00 (config-if)# switchport mode access
EPSW00 (config-if)# switchport access vlan 242
EPSW00 (config)# interface rangeGi1/4-7
EPSW00 (config-if)# switchport mode access
EPSW00 (config-if)# switchport access vlan 241
EPSW00 (config)# interfaceGi1/8
EPSW00 (config-if)# switchport mode access
EPSW00 (config-if)# switchport access vlan 20
EPSW00 (config)# interface rangeGi1/9-10
EPSW00 (config-if)# switchport mode trunk
EPSW00 (config-if)# switchport trunk allowed vlan all
EPSW00 (config-vlan)# end

EPSW00 (config)# ntp server direcciónIPGPS
EPSW00 (config)# clock time LIM -5

EPSW00 (config)# logging direcciónIPdelSysLog
EPSW00 (config)# logging trap 4
EPSW00 (config)# source-interfaceGi1/9
EPSW00 (config)# end

EPSW00 (config)# do wr
```

6. Línea de código que fue escrito en el EPSW01 del UAC de UG1:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname EPSW01

EPSW01 (config)# enable secret contraseñaPrivilegiada

EPSW01(config)# line console 0
EPSW01 (config-line)# password contraseñaConsola
EPSW01 (config-line)# login
EPSW01 (config-line)# exit

EPSW01 (config)# ip domain name iacs.com
EPSW01 (config)# username user privilege 15 secret 0 contraseña
EPSW01 (config)# crypto key generate rsa
       1024 y enter
EPSW01 (config)# ip ssh version 2
EPSW01 (config)# line vty 0 15
EPSW01 (config-line)# login local
EPSW01 (config-line)# exit

EPSW01 (config)# service password-encryption
```

```
EPSW01 (config)# interface vlan1
EPSW01 (config-if)# ip address b.b.b.11 mascara
EPSW01 (config-if)# no sh
EPSW01 (config-if)# exit

EPSW01 (config)# ip default-gateway b.b.b.1

EPSW01 (config)# vlan 100
EPSW01 (config-vlan)# name ION
EPSW01 (config)# vlan 240
EPSW01 (config-vlan)# name SCADA
EPSW01 (config)# vlan 241
EPSW01 (config-vlan)# name Terminal
EPSW01 (config)# vlan 242
EPSW01 (config-vlan)# name IEC
EPSW01 (config)# vlan 243
EPSW01 (config-vlan)# name Electricidad
EPSW01 (config)# vlan 244
EPSW01 (config-vlan)# name VSM
EPSW01 (config)# vlan 245
EPSW01 (config-vlan)# name AS01
EPSW01 (config)# vlan 246
EPSW01 (config-vlan)# name AS02
EPSW01 (config)# vlan 247
EPSW01 (config-vlan)# name SCADAt
EPSW01 (config-vlan)# end

EPSW01 (config)# interfaceGi1/1
EPSW01 (config-if)# switchport mode access
EPSW01 (config-if)# switchport access vlan 240
EPSW01 (config)# interfaceGi1/2
EPSW01 (config-if)# switchport mode access
EPSW01 (config-if)# switchport access vlan 241
EPSW01 (config)# interfaceGi1/3
EPSW01 (config-if)# switchport mode access
EPSW01 (config-if)# switchport access vlan 242
EPSW01 (config)# interface rangeGi1/4-7
EPSW01 (config-if)# switchport mode access
EPSW01 (config-if)# switchport access vlan 241
EPSW01 (config)# interfaceGi1/8
EPSW01 (config-if)# switchport mode access
EPSW01 (config-if)# switchport access vlan 20
EPSW01 (config)# interface rangeGi1/9-10
EPSW01 (config-if)# switchport mode trunk
EPSW01 (config-if)# switchport trunk allowed vlan all
EPSW01 (config-vlan)# end

EPSW01 (config)# ntp server direcciónIPGPS
EPSW01 (config)# clock time LIM -5

EPSW01 (config)# logging direcciónIPdelSysLog
EPSW01 (config)# logging trap 4
EPSW01 (config)# source-interfaceGi1/9
EPSW01 (config)# end
EPSW01 (config)# do wr
```

3.5.3. POLITICAS DE CIBERSEGURIDAD PARA EP

Después que se concluyó con la configuración a los firewalls y la programación a los switches que fueron indicados en el Capítulo 3.5.1, se ingresó las políticas de seguridad con el fin de ampliar la defensa en profundidad para la protección de la red IACS de EP. Si esta actividad no hubiera sido efectuada, implicaba tener la red abierta para una conexión abierta a cualquier host, esto quiere decir: todas las redes IACS se comunicarían contra todas las redes IACS del EP y posiblemente con la red TI

Tabla 21

Políticas de seguridad para la red IACS del EP.

No.	Source	Destination	Services & Applications
1	FW10Cons	EPFW10B EPFW10A	Any
2	AS01 AS02 AS03	AS05	TCP_2001 TCP_2002 TCP_2003
3	ES10 PG10 SinemaS	VLAN240 VLAN241 VLAN243 VLAN244	TightVNC S7 protocol ICMP Protocol snmp ION Schneider
4	ES10 PG10	VLAN100 VLAN111	ICMP Protocol ION Schneider
5	ES10	SECA	TightVNC smb
6	SinemaS ES10 PG10	VLAN112 VLAN113 VLAN241 AS01_esclavos AS02_esclavos RTU VLAN111	ICMP Protocol snmp S7 protocol

7	ES10	Lim_ES01 Lim_ES02 Lim_OSNPM Lim_ESP01	ICMP Protocol Remote_Desktop_Protocol ssh_version_2 smb http https
8	PG10	Lim_VLanAdm	ICMP Protocol Remote_Desktop_Protocol ssh_version_2 smb http https
9	PG11	VLAN113	Any
10	ES10	Lim_PHS	https http smb
11	OSS11	CP_AS04cpu CP_AS04	ICMP Protocol S7 protocol
12	OSS11	CP_AS06cpu CP_AS06	ICMP Protocol S7 protocol
13	OSS11	CP_AS05cpu CP_AS05	ICMP Protocol S7 protocol
14	OSS11	CP_ES30	S7 protocol CP_OS30IEC CP_OS30OPCUA ICMP Protocol
15	OSS11A OSS11B	VLAN241	S7 protocol
16	OSS11A OSS11B	RTU	TCP_2404_5
17	OSS11A OSS11B	AS05 AS05cpu	S7 protocol
18	OSS11A OSS11B	AS07	S7 protocol
19	OSS11A OSS11B	VLAN113	S7 protocol

20	ES10	OSS11A OSS11B BD10	Remote_Desktop_Protocol ICMP Protocol smb
21	ES10	EP_RePa_EMete	TCP_22222
22	ES10	OSC11 OSC12	ICMP Protocol Remote_Desktop_Protocol
23	OSC11 OSC12	OSS11A OSS11B	smb

Fuente: Propia

3.6. REDES IACS: MARAÑON

En esta área operativa se segregó la red de TI y la red IACS, adquirimos dos switches y se empleó los switches que ya existían, además se implementó las contramedidas recomendadas por el IEC 62443.

3.6.1. REQUERIMIENTOS DE EQUIPOS

Se compraron los ciberactivos necesarios para segregar y segmentar la red IACS de HM y estos son expuestas en la Tabla 23 de forma general:

Tabla 22
Necesidad de equipos de red y seguridad perimetral empleados para la implementación de la red IACS en HM.

Requerimientos	Modelo	Marca	Tag
Switch	EI 2000	Cisco	HMSW10A/B
Firewall	PA-220	Palo Alto	HMFW20A/B

Fuente: Propia

Para un mayor detalle de los ciberactivos comprados estos se adquirieron con los detalles mostrados en la Tabla 23 para los switches.

Tabla 23
Requerimientos de swicthes empleados para la implementación de la red IACS de HM

Numero de Parte	**Descripción**	**Cantidad**
IE-2000-4T-B	IE2000 Switch with 6 FE Copper ports (Lan Base License)	2
PWR-IE65W-PC-DC	POE DC Input Power Module for IE3000/2000	2
IOT-UTILITIES	Utilities Industry Solutions; For tracking only.	2
IOT-SUBSTATION	Substation Automation; For tracking only.	2
STK-RACK-DINRAIL=		1

Fuente: Propia

Figura 52

Mostramos imagen de un switch IE2000 de cisco, instalado en el gabinete IACS, con TAG Common en HM.

Fuente: Propia

Tabla 24

Firewall empleados para la implementación de la red IACS de HM.

Numero de Parte	Descripción	Cantidad
PA-220	Next Generation Appliance with DC power	2

Fuente: Propia

3.6.2. CONFIGURACIONES DE EQUIPOS

Primero se efectuó el inventario de todos los SUC detallando como mínimo: Nombre, dirección IP, mascara y gateway.

Tal y como se hizo para la red IACS del CCC, por temas de ciberseguridad ocultaremos la dirección IP de cada ciberactivo de este proyecto, pero para una equivalencia indicaremos que los tres primeros octetos de la dirección IP será representado por una letra de abecedario, de los cuales:

- El primer octeto representara su área operativa.
- El tercer octeto representara a la VLAN que pertenece.
- El cuarto octeto representa la dirección del host.

Tabla 25

SUC que pertenecen a la VLAN 260, dentro de la red IACS de HM, identificación y direccionamiento IP.

Nombre	Tag	Equipo	IP	Gateway
Firewall 20	FW20V	Firewall	C.C.A.1	
Firewall 20A	FW20A	Firewall	C.C.A.2	

Firewall 20B	FW20B	Firewall	C.C.A.3	
Switch 00	sw00	Switch	C.C.A.10	C.C.A.1
Switch 01	sw01	Switch	C.C.A.11	C.C.A.1
Switch 02	sw02	Switch	C.C.A.12	C.C.A.1
Switch 03	sw03	Switch	C.C.A.13	C.C.A.1
Switch 04	sw04	Switch	C.C.A.14	C.C.A.1
Switch 05	sw05	Switch	C.C.A.15	C.C.A.1
Switch 06	sw06	Switch	C.C.A.16	C.C.A.1
Switch 07	sw07	Switch	C.C.A.17	C.C.A.1
Switch 08	sw08	Switch	C.C.A.18	C.C.A.1
Switch 09	sw09	Switch	C.C.A.19	C.C.A.1
Switch 11A	sw11A	Switch	C.C.A.20	C.C.A.1
Switch 11B	sw11B	Switch	C.C.A.21	C.C.A.1
Switch 12A	sw12A	Switch	C.C.A.22	C.C.A.1
Switch 12B	sw12B	Switch	C.C.A.23	C.C.A.1
Switch 13	sw13	Switch	C.C.A.24	C.C.A.1
Switch 10A	sw10A	Switch	C.C.A.251	C.C.A.1
Switch 10B	sw10B	Switch	C.C.A.252	C.C.A.1

Direccionamiento IP equivalente de la infraestructura de red IACS dentro de la VLAN 260.

Fuente: Propia

Tabla 26

SUC de HM, identificación y direccionamiento IP.

TAG	RED	VLAN	IP
OS20	Terminal	260	C.C.B.4
ES01	Planta	261	C.C.C.4
ES02	Planta	261	C.C.C.5
ES03	Planta	261	C.C.C.6
ES04	Planta	261	C.C.C.7
ES05	Planta	261	C.C.C.8
ES06	Planta	261	C.C.C.9
ES07	Planta	261	C.C.C.10
ES08	Planta	261	C.C.C.11
ES09	Planta	261	C.C.C.12
MU02	Planta	261	C.C.C.13
MU03	Planta	261	C.C.C.14
MU04	Planta	261	C.C.C.15
MU05	Planta	261	C.C.C.16
MU06	Planta	261	C.C.C.17
MU07	Planta	261	C.C.C.18
MU08	Planta	261	C.C.C.19
MU09	Planta	261	C.C.C.20
MU10	Planta	261	C.C.C.21

MU11	Planta	261	C.C.C.22
HMI01	Planta	261	C.C.C.23
HMI02	Planta	261	C.C.C.24
HMI03	Planta	261	C.C.C.25
HMI04	Planta	261	C.C.C.26
HMI05	Planta	261	C.C.C.27
HMI06	Planta	261	C.C.C.28
MU01	Planta	261	C.C.C.29
AS00	Planta	261	C.C.C.30
AS01	Planta	261	C.C.C.31
AS02	Planta	261	C.C.C.32
AS03	Planta	261	C.C.C.33
AS04	Planta	261	C.C.C.34
AS05	Planta	261	C.C.C.35
AS06	Planta	261	C.C.C.36
AS07	Planta	261	C.C.C.37
RTU00	IEC	262	C.C.D.4
RTU01	IEC	262	C.C.D.5
RTU02	IEC	262	C.C.D.6
RTU03	IEC	262	C.C.D.7
RTU04	Protección	263	C.C.E.4
PU08A	Protección	263	C.C.E.5
PU08B	Protección	263	C.C.E.6
PU07A	Protección	263	C.C.E.7
PU07B	Protección	263	C.C.E.8
Qualitrol	Protección	263	C.C.E.9
Hydran	Protección	263	C.C.E.10
RTU05	Protección	263	C.C.E.11
PU09A	Protección	263	C.C.E.12
PU09B	Protección	263	C.C.E.13
PU10A	Protección	263	C.C.E.14
PU10B	Protección	263	C.C.E.15
PU11A	Protección	263	C.C.E.16
PU11B	Protección	263	C.C.E.17
PU12	Protección	263	C.C.E.18
PU13	Protección	263	C.C.E.19
PU01B	Protección	263	C.C.E.20
PU02B	Protección	263	C.C.E.21
PU03B	Protección	263	C.C.E.22
PU04	Protección	263	C.C.E.23
PU05	Protección	263	C.C.E.24
PU06	Protección	263	C.C.E.25
EMU00	Medición	103	C.C.F.4
EMU02	Medición	103	C.C.F.5
EMU01	Medición	103	C.C.F.6
EMU03	Medición	103	C.C.F.7

EMU04	Medición	103	C.C.F.8
EMU05	Medición	103	C.C.F.9
GPS01	Tiempo	264	C.C.G.4
GPS02	Tiempo	264	C.C.G.5
GPS02	Tiempo	264	C.C.G.6
GPS03	Tiempo	264	C.C.G.7
HMI01	HMI	265	C.C.H.4
HMI02	HMI	265	C.C.H.5
HMI03	HMI	265	C.C.H.6
HMI04	HMI	265	C.C.H.7
HMI05	HMI	265	C.C.H.8
HMI06	HMI	265	C.C.H.9
HMI07	HMI	265	C.C.H.10
HMI08	HMI	265	C.C.H.11
HMI09	HMI	265	C.C.H.12
HMI10	HMI	265	C.C.H.13
HMI11	HMI	265	C.C.H.14
HMI012	HMI	265	C.C.H.15
HMI013	HMI	265	C.C.H.16
MU01	Multifunción	266	C.C.I.4
MU02	Multifunción	266	C.C.I.5
MU03	Multifunción	266	C.C.I.6
MU04	Multifunción	266	C.C.I.7
MU05	Multifunción	266	C.C.I.8
MU06	Multifunción	266	C.C.I.9
MU07	Multifunción	266	C.C.I.10
MU08	Multifunción	266	C.C.I.11
MU09	Multifunción	266	C.C.I.12
MU10	Multifunción	266	C.C.I.13
MU11	Multifunción	266	C.C.I.14
MU12	Multifunción	266	C.C.I.15
MU13	Multifunción	266	C.C.I.16

Direccionamiento IP equivalente de los equipos de Control de la red IACS.

Fuente: Propia

3.6.2.1. CONFIGURACION DE LOS FIREWALL CON EL OBJETIVO DE SEGREGAR LA RED IACS DEL HM

Tal y como se efectuó en EP, con el objetivo de segregar la red IACS y la red TI, se usó y se configuro los dos Firewall de la Tabla 25, además se habilito la gestión de rutas entre VLAN para las comunicaciones entre ellas, y después se detallaron y aplicaron las políticas de ciberseguridad para esta red IACS de HM.

Repetimos los pasos que se efectuó en el Capítulo 3.5.2.1, pero en el paso 7, se ingresó la siguiente tabla 20

Tabla 27

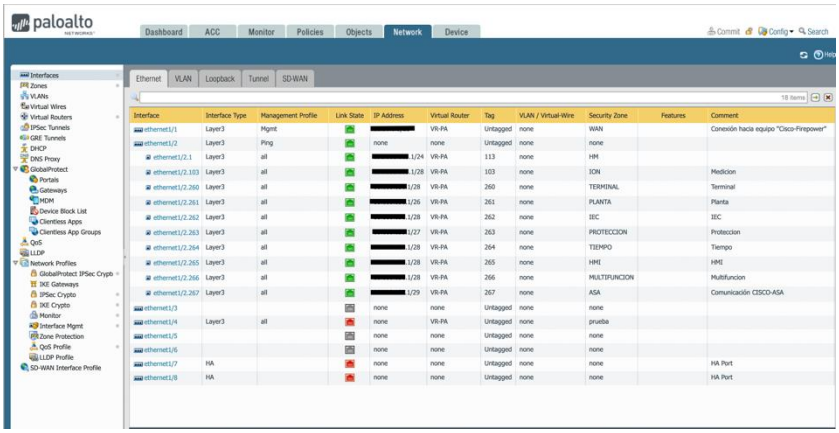
Direccionamiento IP para el tráfico de VLAN para la red IACS de HM.

Interface	Interface Type	IP Address	Tag	Security Zone
ethernet1/1	L3_PHYSICAL	10.50.1.3/28	Untagged	WAN
ethernet1/2	L3_PHYSICAL		Untagged	
ethernet1/2.1	L3_LOGICAL	192.168.113.1/24	113	HM
ethernet1/2.103	L3_LOGICAL	192.168.103.1/28	103	Medición
ethernet1/2.260	L3_LOGICAL	10.110.130.1/28	260	Terminal
ethernet1/2.261	L3_LOGICAL	10.110.131.1/26	261	Planta
ethernet1/2.262	L3_LOGICAL	10.110.132.1/28	262	IEC
ethernet1/2.263	L3_LOGICAL	10.110.133.1/27	263	Protección
ethernet1/2.264	L3_LOGICAL	10.110.134.1/28	264	Tiempo
ethernet1/2.265	L3_LOGICAL	10.110.135.1/28	265	HMI
ethernet1/2.266	L3_LOGICAL	10.110.136.1/28	266	Multifunción
ethernet1/2.267	L3_LOGICAL	10.110.137.1/29	267	ASA
ethernet1/3	UNUSED		Untagged	
ethernet1/4	L3_PHYSICAL		Untagged	
ethernet1/5	UNUSED		Untagged	
ethernet1/6	UNUSED		Untagged	
ethernet1/7	HA		Untagged	
ethernet1/8	HA		Untagged	

Fuente: Propia

Figura 53

Visualización de las redes agregadas al firewall para la red IACS de HM.



Por ciberseguridad solo mostramos el último octeto de la dirección IP.

Fuente: Propia

3.6.2.2. CONFIGURACION DE LOS SWITCHES CON EL OBJETIVO DE SEGMENTAR LA RED IACS DE HM

Después que se terminó con la segregación de la red IACS y la red TI, se inició la actividad en los switches que consistió en: programación básica y el uso de VLAN. Este ultimó que permitió la conectividad entre los SUC de la misma VLAN y la conexión entre SUC permitidos de diferentes VLAN. De manera breve se efectuaron los siguientes pasos para la programación de los dos switches.

1. Se hizo los pasos 1 y 2 del Capítulo 3.5.2.2.
2. Se escribió los siguientes comandos en el CLI, del switch HMSW10A:

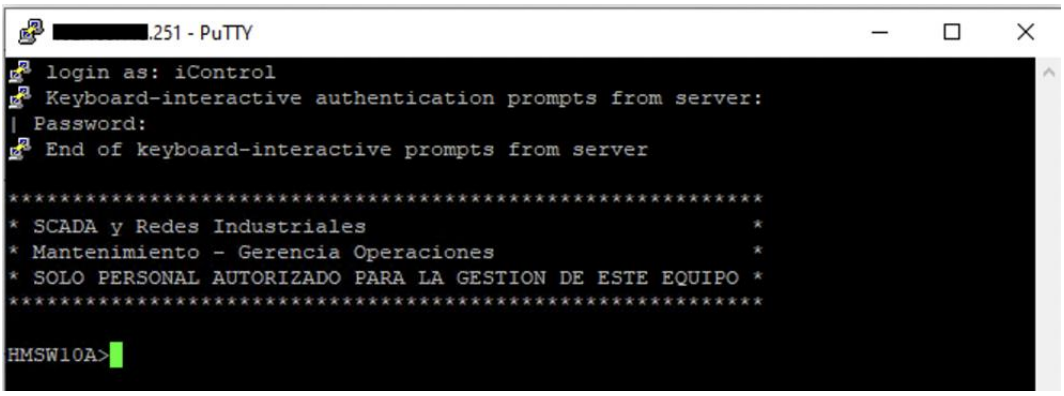
```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname HMSW10A

HMSW10A (config)# enable secret contraseñaPrivilegiada

HMSW10A (config)# line console 0
HMSW10A (config-line)# password contraseñaConsola
HMSW10A (config-line)# login
HMSW10A (config-line)# exit

HMSW10A (config)# ip domain name iacs.com
HMSW10A (config)# username user privilege 15 secret 0 contraseña
HMSW10A (config)# crypto key generate rsa
        1024 y enter
HMSW10A (config)# ip ssh version 2
HMSW10A (config)# line vty 0 15
HMSW10A (config-line)# login local
HMSW10A (config-line)# exit

HMSW10A (config)# service password-encryption

HMSW10A (config)# interface vlan 1
HMSW10A (config-if)# ip address C.C.A.251 mascara
HMSW10A (config-if)# no sh
HMSW10A (config-if)# exit

HMSW10A (config)# ip default-gateway C.C.A.1

HMSW10A (config)# vlan 103
HMSW10A (config-vlan)# name Medicion
HMSW10A (config)# vlan 260
HMSW10A (config-vlan)# name Terminal
HMSW10A (config)# vlan 261
HMSW10A (config-vlan)# name Planta
HMSW10A (config)# vlan 262
HMSW10A (config-vlan)# name IEC
HMSW10A (config)# vlan 263
HMSW10A (config-vlan)# name Proteccion
HMSW10A (config)# vlan 264
HMSW10A (config-vlan)# name Tiempo
```

```
HMSW10A (config)# vlan 265
HMSW10A (config-vlan)# name HMI
HMSW10A (config)# vlan 266
HMSW10A (config-vlan)# name Multifuncion
HMSW10A (config-vlan)# end

HMSW10A (config)# interface Fa1/1
HMSW10A (config-if)# switchport mode trunk
HMSW10A (config-if)# switchport trunk native vlan 1
HMSW10A (config-if)# switchport trunk allowed vlan all
HMSW10A (config)# interface Fa1/2
HMSW10A (config-if)# switchport mode access
HMSW10A (config-if)# switchport access vlan 113
HMSW10A (config)# interface Fa1/3
HMSW10A (config-if)# switchport mode access
HMSW10A (config-if)# switchport access vlan 113
HMSW10A (config)# interface Fa1/4
HMSW10A (config-if)# switchport mode access
HMSW10A (config-if)# switchport access vlan 113
HMSW10A (config)# interface Fa1/5
HMSW10A (config-if)# switchport mode trunk
HMSW10A (config-if)# switchport trunk native vlan 113
HMSW10A (config-if)# switchport trunk allowed vlan all
HMSW10A (config)# interface Fa1/6
HMSW10A (config-if)# switchport mode access
HMSW10A (config-if)# switchport access vlan 1

HMSW10A (config)# ntp server direcciónIPGPS
HMSW10A (config)# clock time LIM -5

HMSW10A (config)# logging direcciónIPdelSysLog
HMSW10A (config)# logging trap 4
HMSW10A (config)# source-interface Fa1/5
HMSW10A (config)# end

HMSW10A (config)# do wr
```

3. Se verificó la correcta configuración del switch HMSW01A:

Figura 54

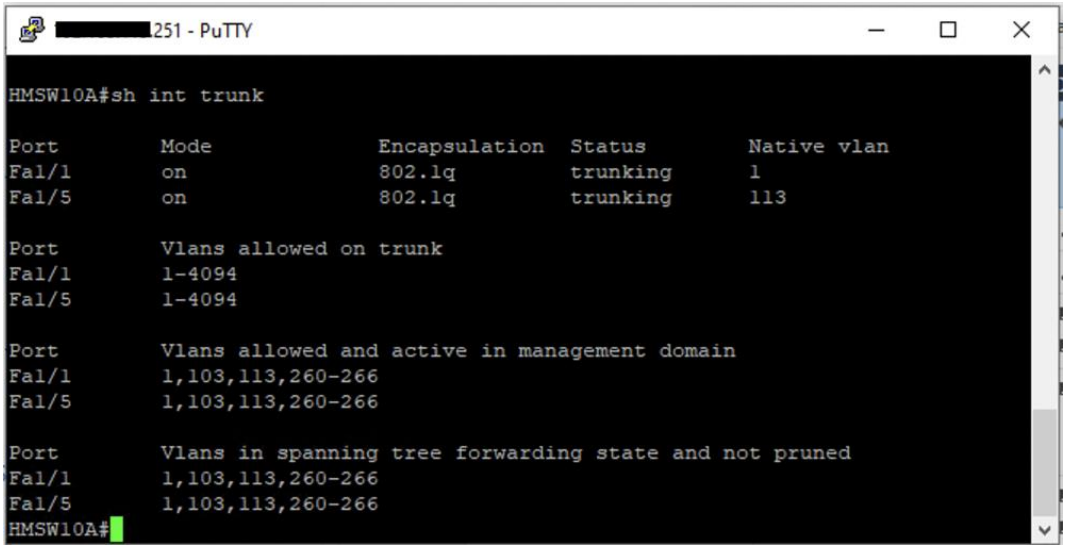
CLI que muestra el banner de bienvenida al switch HMSW10A.



Fuente: Propia

Figura 55

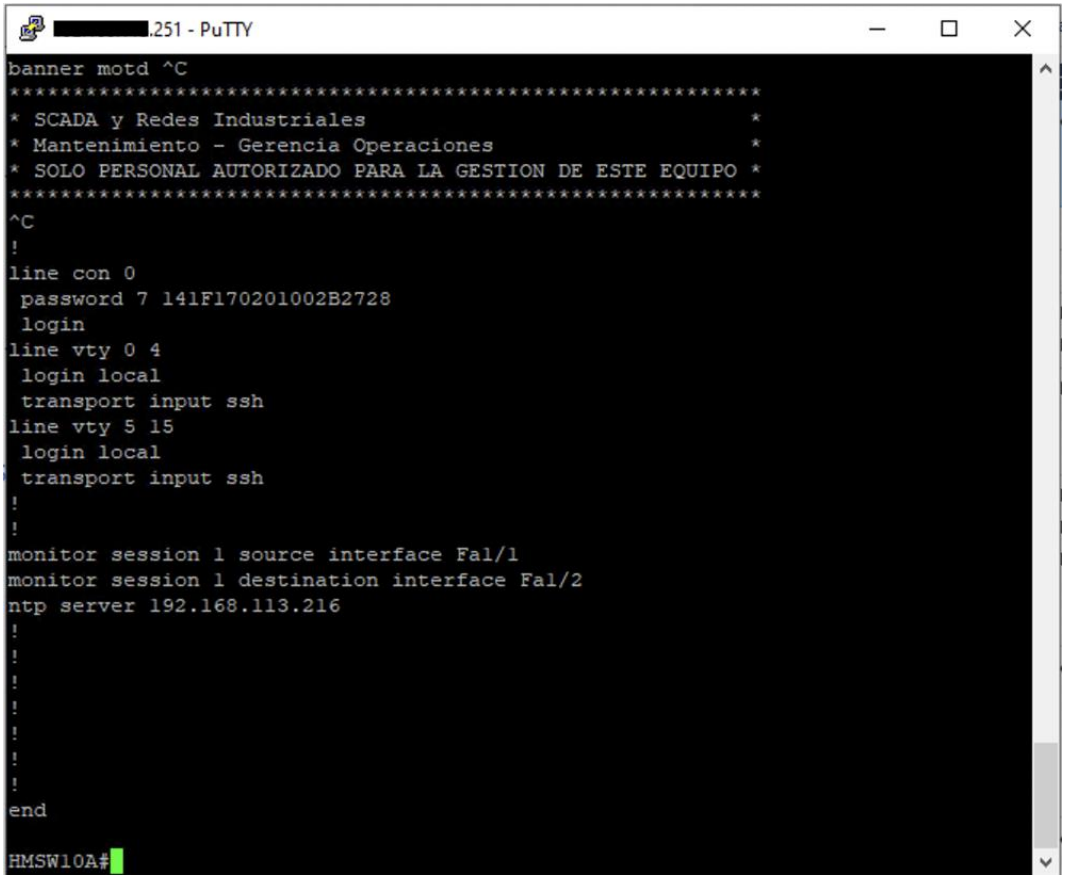
Interfaces troncales creadas en el switch HMSW10A.



Fuente: Propia

Figura 56

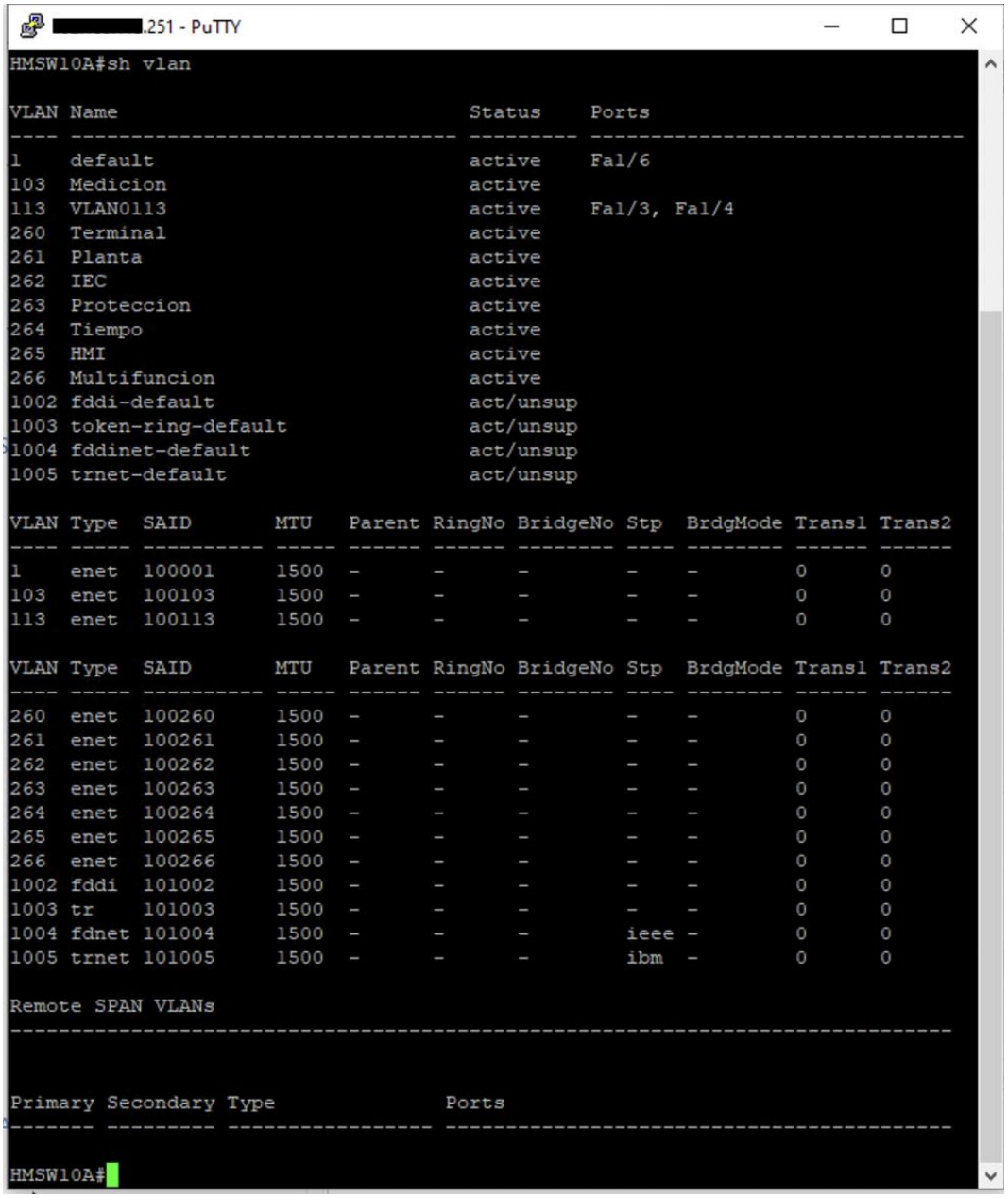
Encriptación de credenciales que fue creada en el switch HMSW10A



Fuente: Propia

Figura 57

CLI que muestra las VLAN creadas en el switch HMSW10A.



Fuente: Propia

4. Luego que se concluyó con la programación del switch HMSW01A, se escribió los siguientes comandos en el CLI, del switch HMSW01B:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname HMSW10B

HMSW10B (config)# enable secret contraseñaPrivilegiada

HMSW10B (config)# line console 0
HMSW10B (config-line)# password contraseñaConsola
```

```
HMSW10B (config-line)# login
HMSW10B (config-line)# exit

HMSW10B (config)# ip domain name iacs.com
HMSW10B (config)# username user privilege 15 secret 0 contraseña
HMSW10B (config)# crypto key generate rsa
       1024 y enter
HMSW10B (config)# ip ssh version 2
HMSW10B (config)# line vty 0 15
HMSW10B (config-line)# login local
HMSW10B (config-line)# exit

HMSW10B (config)# service password-encryption

HMSW10B (config)# interface vlan 1
HMSW10B (config-if)# ip address C.C.A.252 mascara
HMSW10B (config-if)# no sh
HMSW10B (config-if)# exit

HMSW10B (config)# ip default-gateway C.C.A.1

HMSW10B (config)# vlan 103
HMSW10B (config-vlan)# name Medicion
HMSW10B (config)# vlan 260
HMSW10B (config-vlan)# name Terminal
HMSW10B (config)# vlan 261
HMSW10B (config-vlan)# name Planta
HMSW10B (config)# vlan 262
HMSW10B (config-vlan)# name IEC
HMSW10B (config)# vlan 263
HMSW10B (config-vlan)# name Proteccion
HMSW10B (config)# vlan 264
HMSW10B (config-vlan)# name Tiempo
HMSW10B (config)# vlan 265
HMSW10B (config-vlan)# name HMI
HMSW10B (config)# vlan 266
HMSW10B (config-vlan)# name Multifuncion
HMSW10B (config-vlan)# end

HMSW10B (config)# interface Fa1/1
HMSW10B (config-if)# switchport mode trunk
HMSW10B (config-if)# switchport trunk native vlan 1
HMSW10B (config-if)# switchport trunk allowed vlan all
HMSW10B (config)# interface Fa1/2
HMSW10B (config-if)# switchport mode access
HMSW10B (config-if)# switchport access vlan 113
HMSW10B (config)# interface Fa1/3
HMSW10B (config-if)# switchport mode access
HMSW10B (config-if)# switchport access vlan 113
HMSW10B (config)# interface Fa1/4
HMSW10B (config-if)# switchport mode access
HMSW10B (config-if)# switchport access vlan 260
HMSW10B (config)# interface Fa1/5
HMSW10B (config-if)# switchport mode trunk
HMSW10B (config-if)# switchport trunk native vlan 113
HMSW10B (config-if)# switchport trunk allowed vlan all
HMSW10B (config)# interface Fa1/6
HMSW10B (config-if)# switchport mode access
HMSW10B (config-if)# switchport access vlan 1

HMSW10B (config)# ntp server direcciónIPGPS
```

```
HMSW10B (config)# clock time LIM -5

HMSW10B (config)# logging direcciónIPdelSysLog
HMSW10B (config)# logging trap 4
HMSW10B (config)# source-interface Fa1/6
HMSW10B (config)# end

HMSW10B (config)# do wr
```

3.6.3. POLITICAS DE CIBERSEGURIDAD

Después que se concluyó con la configuración a los firewalls y la programación a los switches que fueron indicados en el Capítulo 3.6.1, se ingresó las políticas de seguridad con el fin de ampliar la defensa en profundidad para la protección de la red IACS de HM. Si esta actividad no hubiera sido efectuada, implicaba tener la red abierta para una conexión abierta a cualquier host, esto quiere decir: todas las redes IACS se comunicarían contra todas las redes IACS del HM y posiblemente con la red TI

Tabla 28
Políticas de seguridad para la red IACS de HM.

No.	Source	Destination	Services & Applications
1	ES20 PG20	VLAN113 VLAN260 VLAN261 VLAN262 VLAN263 VLAN264 VLAN265 VLAN266	TightVNC S7 protocol ICMP Protocol snmp ION Schneider
2	ES20 PG20	VLAN103	ICMP Protocol ION Schneider
3	OS20	VLAN113 VLAN260 VLAN261 VLAN262 VLAN264	 S7 protocol ICMP Protocol
4	ES20	Lim_ES01 Lim_ES02 Lim_OSNPM Lim_ESP01	ICMP Protocol Remote_Desktop_Protocol ssh_version_2 smb http https

5	PG20	Lim_VLanAdm	ICMP Protocol Remote_Desktop_Protocol ssh_version_2 smb http https
6	ES20	Lim_PHS	https http smb
7	OS20	RTU	TCP_2404_5
8	Lim_ESP01	VLAN113	ICMP Protocol Remote_Desktop_Protocol ssh_version_2 smb http https
9	Lim_ESP01	VLAN260 VLAN261 VLAN262 VLAN263 VLAN264 VLAN265 VLAN266	TightVNC S7 protocol ICMP Protocol snmp ION Schneider
10	PMES	VLAN103	ICMP Protocol ION Schneider
11	OSS10	VLAN113 VLAN260 VLAN261 VLAN262 VLAN264	 S7 protocol ICMP Protocol
12	OSS10	RTU	TCP_2404_5

Fuente: Propia

.

CAPÍTULO IV. RESULTADOS

4.1. DEL PROYECTO

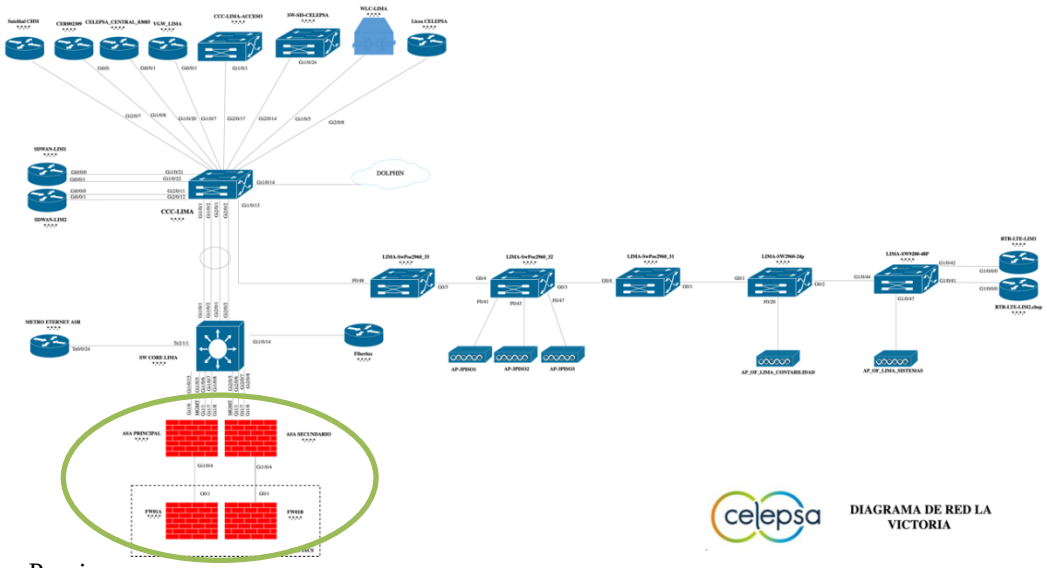
Luego de la implementación y la puesta en servicio de los firewall y switches, se validó el cumplimiento de los objetivos planteados en el Capítulo 3.1.2, en los siguientes puntos:

4.1.1. SEGREGACIÓN ENTRE LAS REDES DE IACS Y TI.

En la Figura 58, se muestra la topología lógica de la red de TI de Lima y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de TI.

Figura 58

Diagrama de Red la Victoria, gestionada por TI.

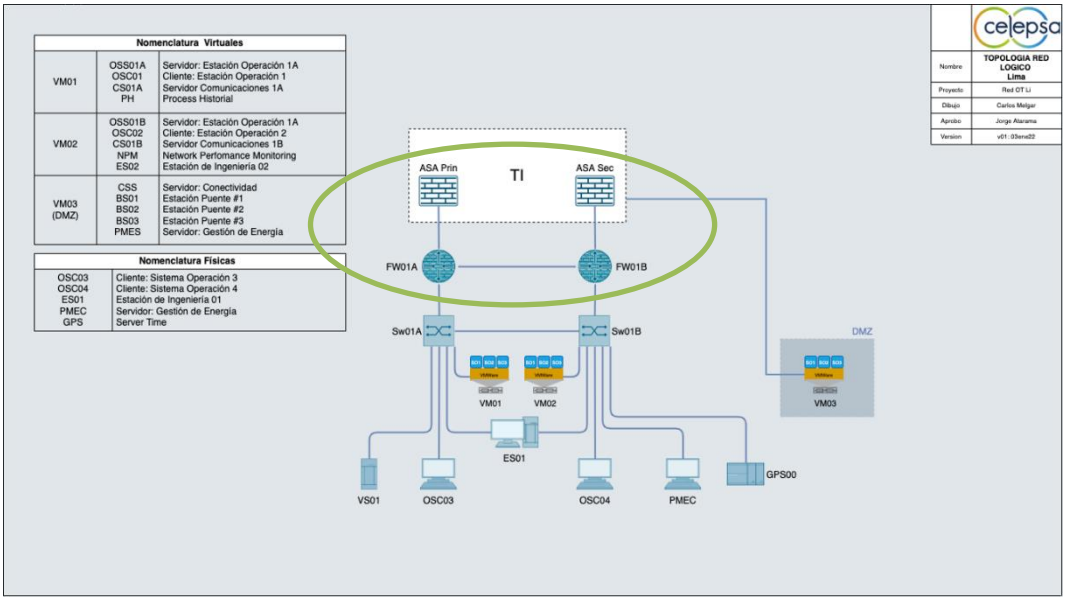


Fuente: Propia

En la Figura 59, se muestra la topología lógica de la red de IACS del CCC y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de Mantenimiento, además de mostrar que los firewalls están directamente conectados a los switch SW01A y SW01B.

Figura 59

Diagrama de Red IACS del CCC, gestionada por Mantenimiento.

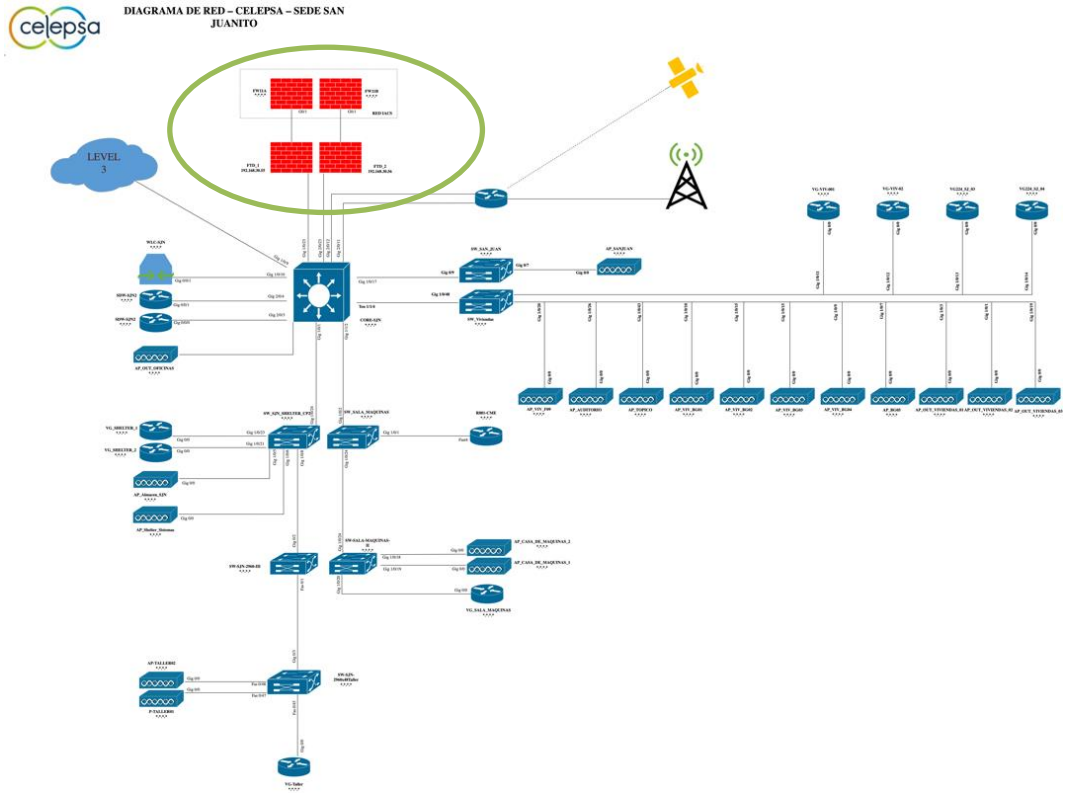


Fuente: Propia

En la Figura 60, se muestra la topología lógica de la red de TI de San Juanito y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de TI.

Figura 60

Diagrama de Red de San Juanito, gestionada por TI.

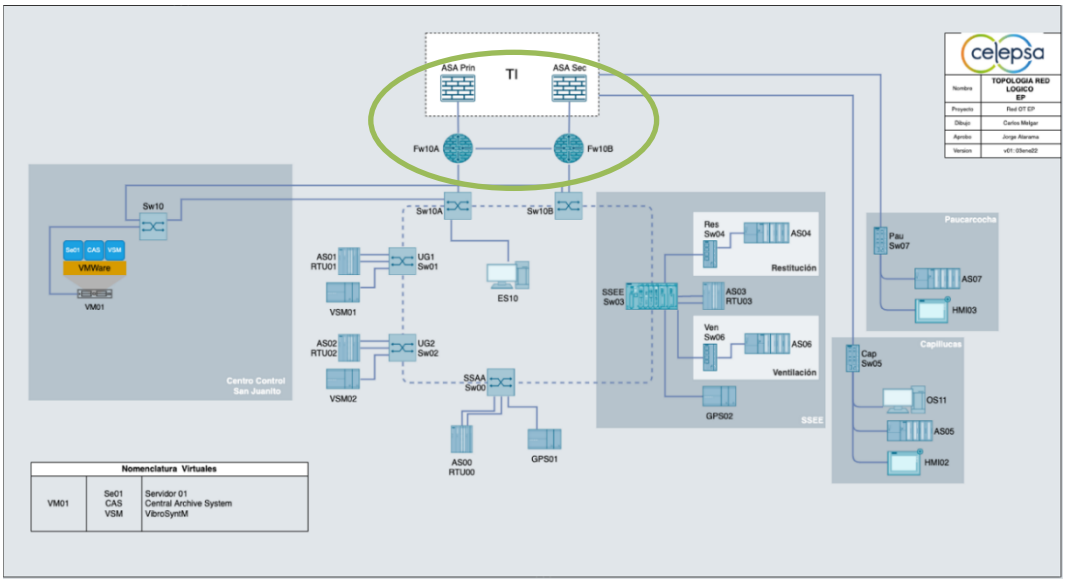


Fuente: Propia

En la Figura 61, se muestra la topología lógica de la red de IACS de EP y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de Mantenimiento, además de mostrar que los firewalls están directamente conectados a los switch SW10A y SW10B.

Figura 61

Diagrama de Red IACS de EP, gestionada por Mantenimiento.

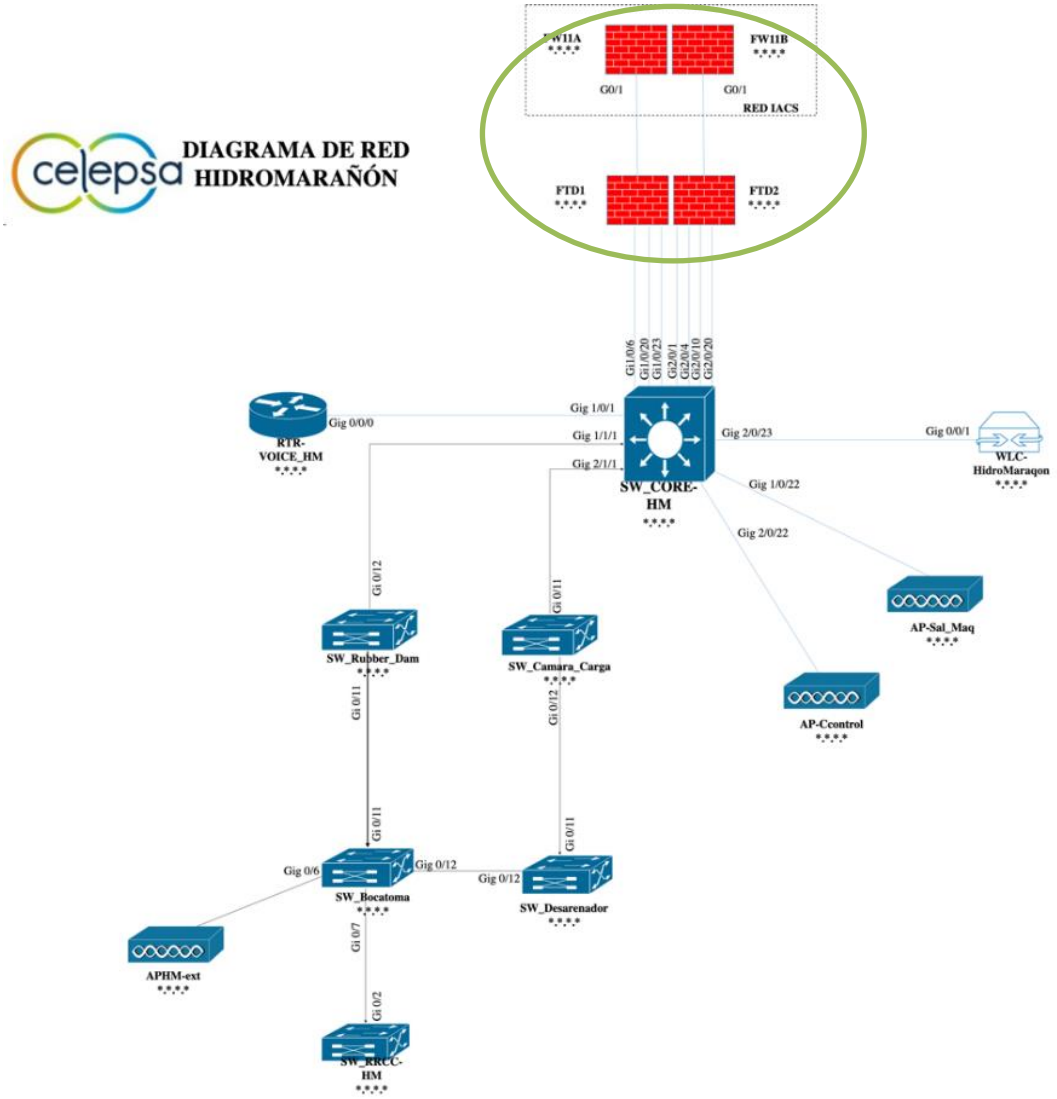


Fuente: Propia

En la Figura 62, se muestra la topología lógica de la red de TI de Marañón y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de TI.

Figura 62

Diagrama de Red de HM, gestionada por TI.

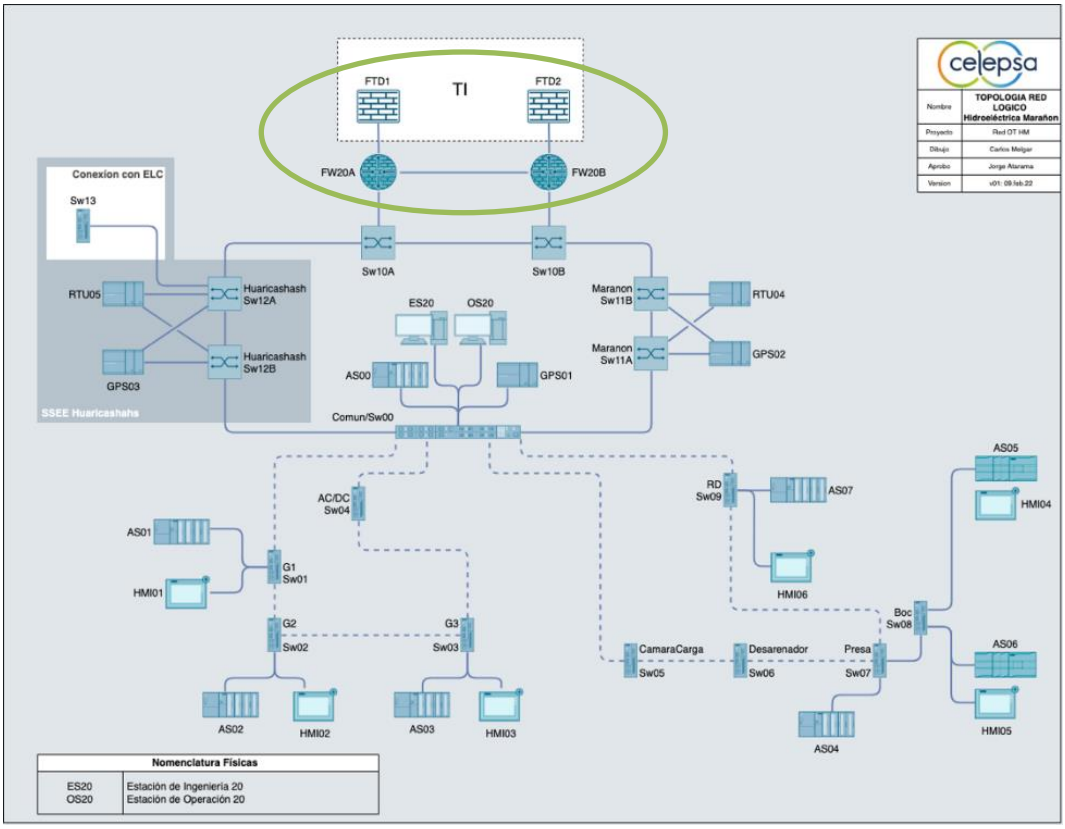


Fuente: Propia

En la Figura 63, se muestra la topología lógica de la red de IACS de HM y dentro del eclipse la “Segregación de redes TI e IACS” visto desde el lado de Mantenimiento, además de mostrar que los firewalls están directamente conectados a los switch SW10A y SW10B.

Figura 63

Diagrama de Red IACS de HM, gestionada por Mantenimiento.



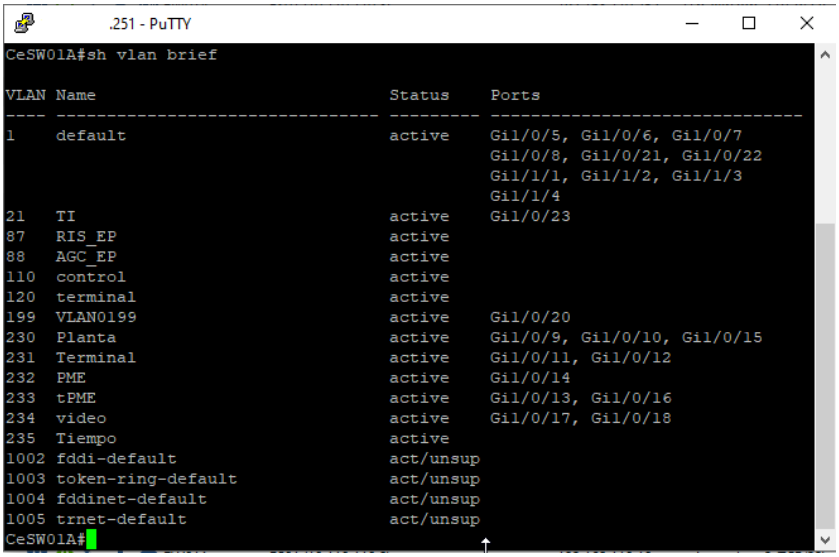
Fuente: Propia

4.1.2. SEGMENTACION DE LA RED IACS.

En la Figura 64, se muestra las VLans creadas en el switch SW01A para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS del CCC”

Figura 64

VLans que fueron creadas y son usadas en el switch SW10A de la Red IACS del CCC

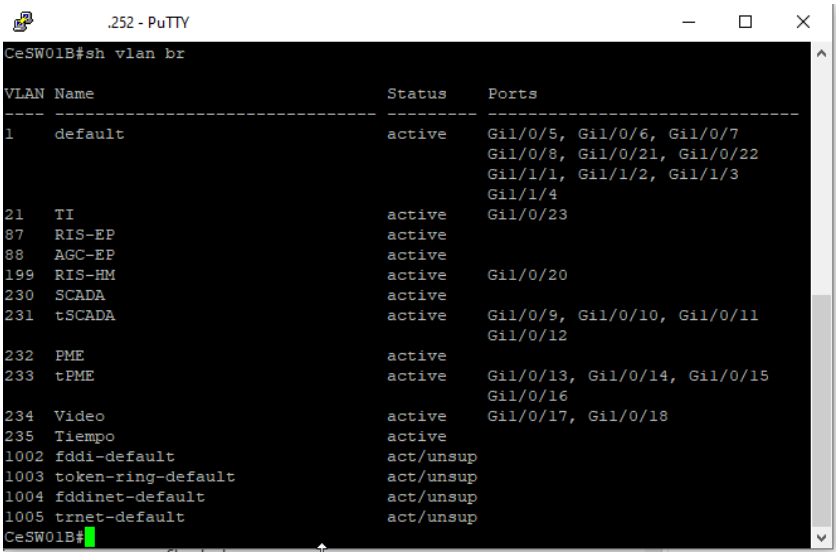


Fuente: Propia

En la Figura 65, se muestra las VLans creadas en el switch SW01B para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS del CCC”

Figura 65

Vlan que fueron creadas y son usadas en el switch CeSW10B de la Red IACS del CCC



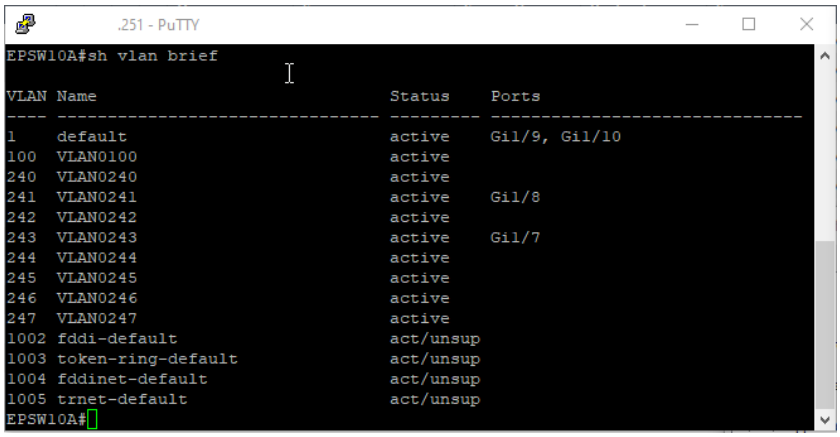
Fuente: Propia

En la Figura 66, se muestra las VLans creadas en el switch SW10A para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama

técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS de EP.

Figura 66

Vlan que fueron creadas y son usadas en el switch EPSW10A de la Red IACS de EP

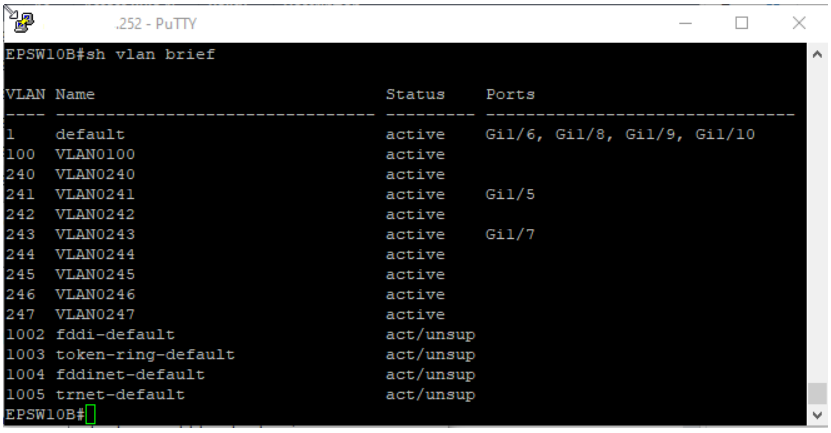


Fuente: Propia

En la Figura 67, se muestra las VLans creadas en el switch SW10B para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS de EP.

Figura 67

VLans que fueron creadas y son usadas en el switch EPSW10B de la Red IACS de EP



Fuente: Propia

En la Figura 68, se muestra las VLans creadas en el switch SW20A para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama

técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS de HM.

Figura 68

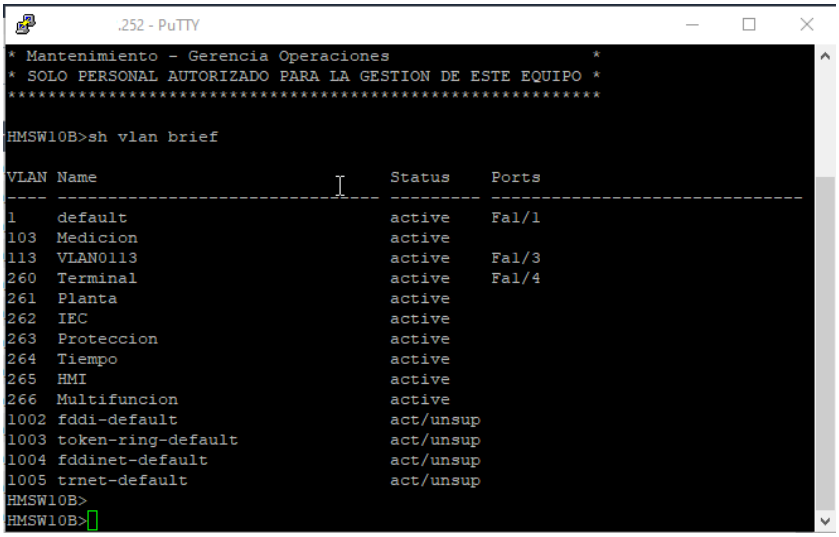
VLans que fueron creadas y son usadas en el switch HMSW10A de la Red IACS de HM

Fuente: Propia

En la Figura 69, se muestra las VLans creadas en el switch SW20B para la conexión entre los ciberactivos, además de visualiza el puerto a la Vlan que pertenece, esto se llama técnicamente “Segmentación de la red” y corresponde a la Segmentación de la red IACS de HM.

Figura 69

Vlan que fueron creadas y son usadas en el switch HMSW10B de la Red IACS de HM



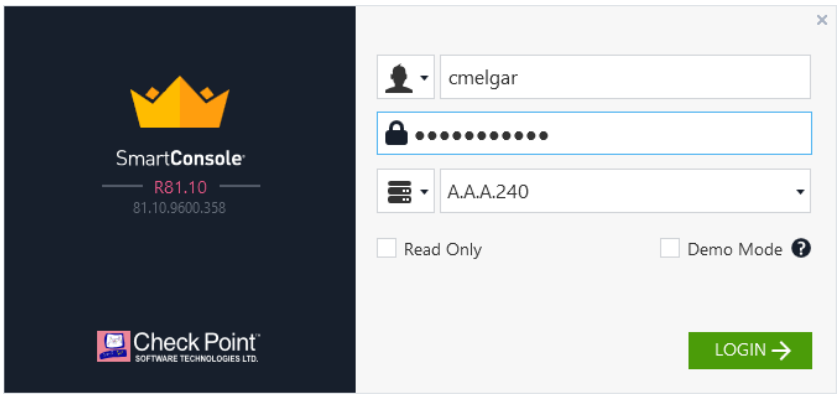
Fuente: Propia

4.1.3. GESTIÓN REMOTA DE LOS CIBERACTIVOS DE LOS IACS

En la Figura 70, se muestra la solicitud de credenciales para el acceso al software de configuración de los firewalls: CEFW01 del CCC, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 70

Gestión remota habilitada través de aplicativo para en NGFW CEFW01 de la Red IACS del CCC

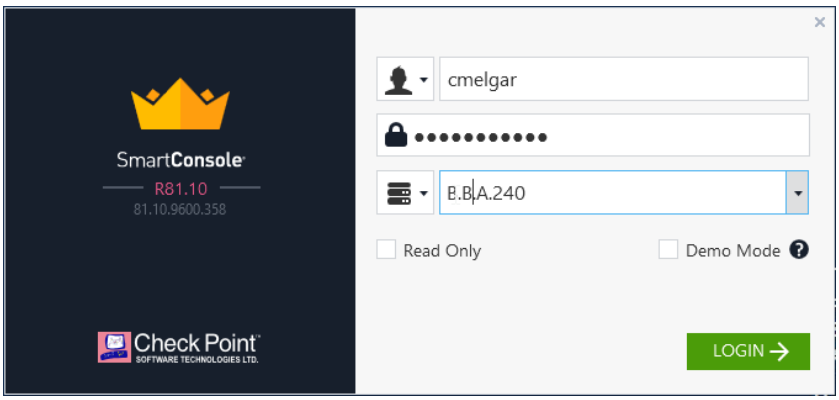


Fuente: Propia

En la Figura 71, se muestra la solicitud de credenciales para el acceso al software de configuración de los firewalls: EPFW10 de EP, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 71

Gestión remota habilitada través de aplicativo para en NGFW EPFW10 de la Red IACS de EP.



Fuente: Propia

En la Figura 72, se muestra la solicitud de credenciales para el acceso al software de configuración de los firewalls: EPFW20 de HM", cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 72

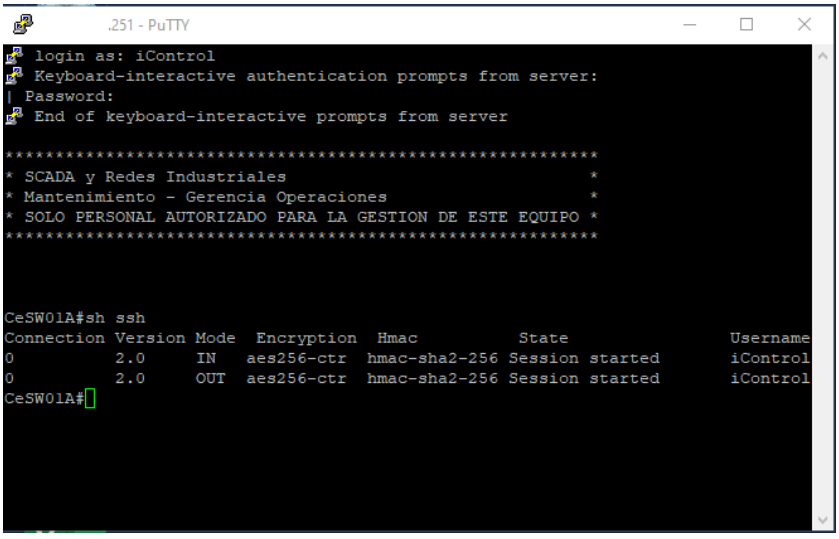
Gestión remota habilitada través de aplicativo para en NGFW HMFW20 de la Red IACS de HM.

Fuente: Propia

En la Figura 73, se muestra el CLI del switch CESW01A del CCC, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 73

Gestión remota habilitada través de SSH en el switch CESW10A de la Red IACS del CCC

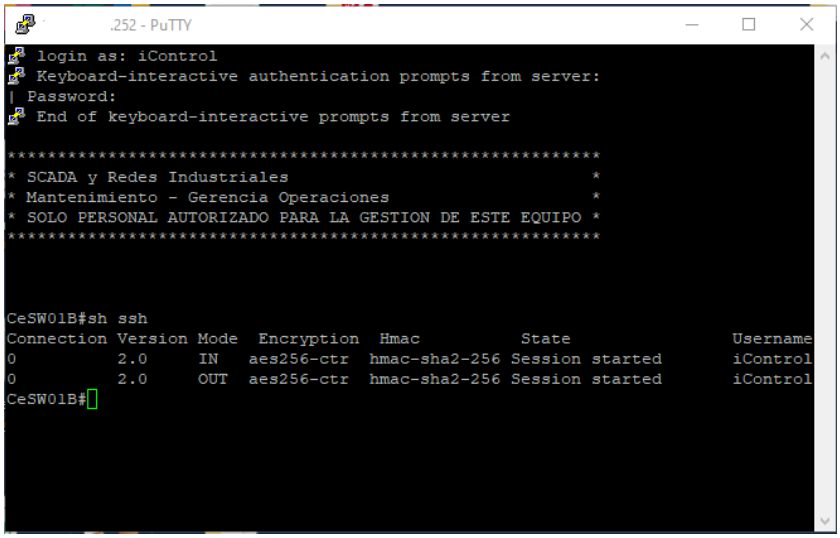


Fuente: Propia

En la Figura 74, se muestra el CLI del switch CESW01B del CCC, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 74

Gestión remota habilitada través de SSH en el switch CESW10B de la Red IACS del CCC

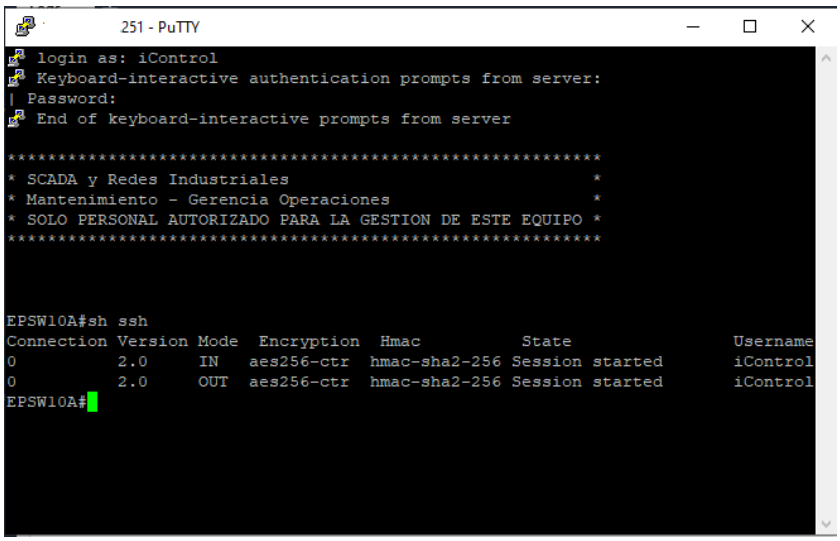


Fuente: Propia

En la Figura 75, se muestra el CLI del switch EPSW10A de EP, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 75

Gestión remota habilitada través de SSH en el switch EPSW10A de la Red IACS de EP

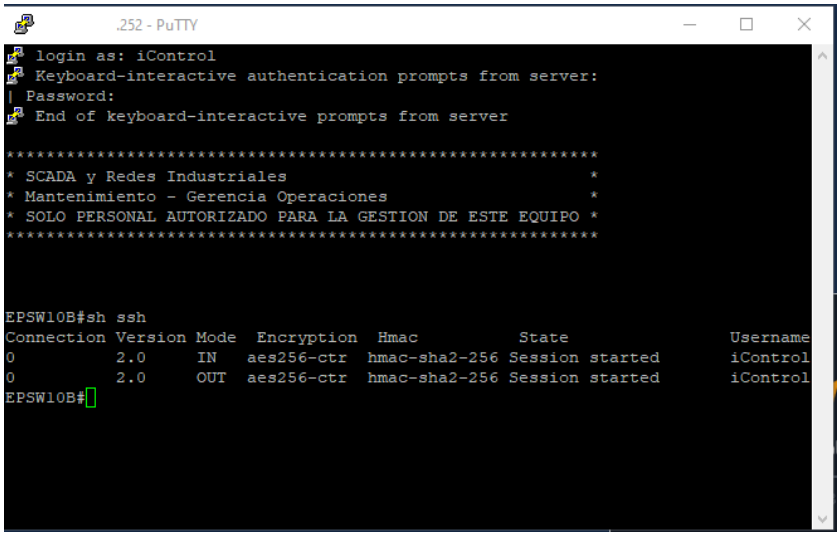


Fuente: Propia

En la Figura 76, se muestra el CLI del switch EPSW10B de EP, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 76

Gestión remota habilitada través de SSH en el switch EPSW10B de la Red IACS de EP

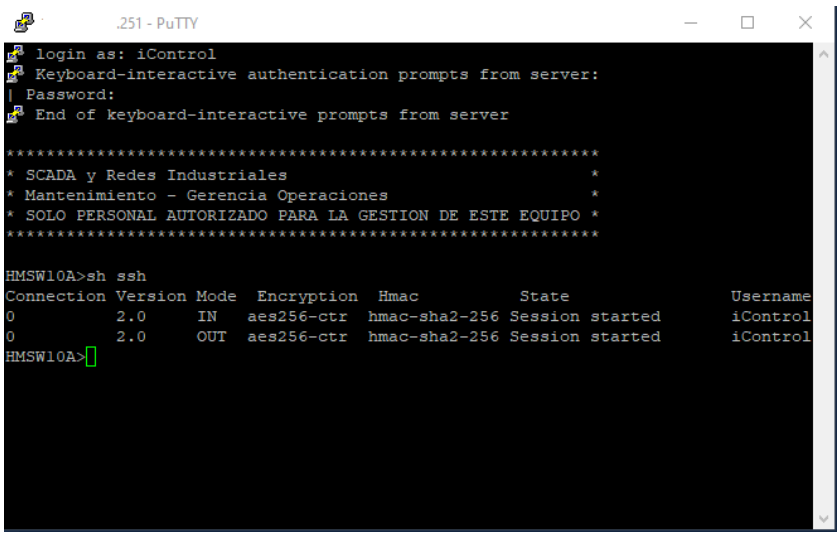


Fuente: Propia

En la Figura 77, se muestra el CLI del switch HMSW10A de HM, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 77

Gestión remota habilitada través de SSH en el switch HMSW10B de la Red IACS de HM

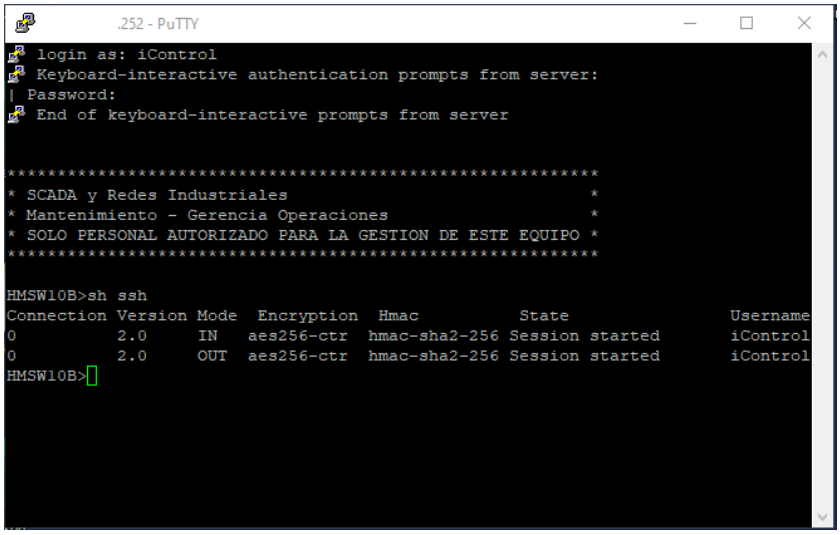


Fuente: Propia

En la Figura 78, se muestra el CLI del switch HMSW10B de HM, detallando el uso del servicio SSH para la gestión remota del switch, cabe resaltar que los accesos remotos son desde la ES01 en Lima.

Figura 78

Gestión remota habilitada través de SSH en el switch HMSW10B de la Red IACS de HM



Fuente: Propia

4.2. ANALISIS DE RESULTADO

De acuerdo con la evidencia presentada, en la Tabla 29 se realiza el análisis de estos para verificar si estos pueden demostrar el cumplimiento de los objetivos específicos establecidos en el punto 3.1.2.

Tabla 29

Resumen de los resultados obtenidos luego de la implementación.

Objetivo	Resultado
Segregación entre las redes IACS y TI.	Se muestra la segregación de las redes de TI e IACS en las Figuras 59,61,63 vistas desde el lado de Mantenimiento.
Segmentación de la red IACS.	Para la validación de la segmentación de las redes IACS, esto es a través de la habilitación de las VLans en cada uno de los switches y estos son validados con las Figuras 64 a 69 que corresponde

	a cada switch de todas las áreas operativas.
Gestión centralizada de los ciberactivos de IACS.	Para la validación de la gestión remota de los SUC de las redes IACS, mostramos las Figuras 70 al 78.

Fuente: Propia

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

El objetivo principal de este proyecto fue “Implementar Ciberseguridad en el Sistemas de Control y Automatización Industrial dentro de la Compañía Eléctrica El Platanal S.A.”, su término permite asegurar las operaciones de forma remota de las áreas operativas de El Platanal y Marañón desde el Centro de Control CELEPSA desde marzo del 2021.

Con la segregación de las redes de TI que pertenece a la Jefatura de Sistemas y las redes IACS dentro de Mantenimiento, se ha establecido una frontera de las responsabilidades para la gestión ambas redes en base a los conocimientos, experiencias y usos de los diferentes sistemas de uso en TI e IACS. Otro beneficio obtenido es que ha aumentado la ciberseguridad de cada red IACS.

Con la implementación de la segmentación de las redes IACS del Centro de Control, El Platanal y Marañón se ha redujo los dominios de difusión mejorando el tráfico de toda la red, algo que no teníamos antes del 2020, es decir todas las tramas de broadcast llegaban a cada uno de los ciberactivos de la única red. Además, se ha aumentado la ciberseguridad de cada red IACS.

Con la gestión centralizada de los ciberactivos de IACS se ha afianzado el uso de los diferentes softwares de gestión de los ciberactivos de manera remota y segura, además de las buenas prácticas como son: autenticación, autorización y administración de los ciberactivos de la red IACS. Algo indudablemente obtenido es que se redujo la cantidad de viaja a cada área operativa.

Luego de la implementación de este proyecto se ha endurecido las capas de seguridad tal y como menciona la defensa en profundidad.

Definitivamente existen buenas prácticas de uso para TI que no se puede usar en el mundo industrial porque perjudican la correcta operación de los ciberactivos de IACS.

5.2. RECOMENDACIONES

6. Mantener activa las conexiones con el servidor de actualizaciones de los NGFW de todas las áreas operativas, con el fin de mantener al IPS totalmente actualizado y operando correctamente.
7. Mantener un ancho de banda mínimo exclusivo para las IACS de 8 Mbyte/s entre las áreas operativas: Platanal y Marañón con el Centro de Control CELEPSA en Lima con el fin de mantener un adecuado tráfico de información en tiempo real entre los diferentes ciberactivos de todas las redes IACS.
8. Separar las comunicaciones de las redes IACS y TI con cada una de las plantas, es decir tener un enlace dedicado para las redes IACS y otro enlace para las redes TI, con el fin de tener una independencia total de las redes.
9. Mantener activamente las capacitaciones especializadas en ciberseguridad industrial a través de los diferentes niveles de Certificaciones de la IEC 62443.
10. Tener capacitado al personal en el uso, configuración y mantenimiento de los diferentes ciberactivos de comunicaciones y seguridad perimetral.
11. Implementación de una sonda de red por cada área operativa, las sondas son equipos electrónicos o virtuales pasivas y realizan el descubrimiento de los dispositivos, así como el alertamiento relacionado con cualquier incidente o anomalía de seguridad y su integración al actual Sistema SCADA del Centro de Control CELEPSA en Lima.
12. Establecer los límites y responsabilidades de las redes IACS y TI

REFERENCIAS

ACSC. (Octubre de 2021). *Austrilian Cyber Security Centre.* Obtenido de https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-network-segmentation-and-segregation

Ariganello, E. (2014). *Redes Cisco.* España: RA-MA.

CISA. (September de 2016). *Cybersecurity & Infraestructure Security Agency.* Obtenido de www.cisa.gov › uscert › sites › default › files › recommended_practices

Cisco. (2022). Obtenido de https://www.cisco.com

Clarke, G., Reyders, D., & Wright, D. (2004). *Pratical Modern SCADA Protocols: DNP3, 60870 and Reñated Systems.* ELSEVIER.

El Congreso de Colombia. (2009). *LEY 1341.* Bogota: El Congreso de Colombia. Obtenido de Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información

Gunter, D. G., Medoff, M. D., & O'Brien, P. C. (2018). *Implementing IEC 62443.* Sellersville: Exida.

IEC/TS 62443-1-1. (2009). *Security for Indistrial Automation and Control Systems.* ISA/IEC.

incibe-cert. (5 de 12 de 2018). *Mejorando la seguridad del IEC 104 con la ayuda del estándar IEC 62351*. Obtenido de https://www.incibe-cert.es/blog/mejorando-seguridad-del-iec-104-ayuda-del-estandar-iec-62351

ISA 62443-1-2. (2018). *Security for Industrial Automation and Control Systems: Master Glossary of Terms and Abbreviations.* ISA.

ISO 27001. (2018). *ISO IEC 27000.*

Knapp, E. D. (2015). *Industrial Network Security- Second Edition* .

NIST SP 800-53 Rev5. (2020). *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology.

NIST SP 800-82 Rev2. (2015). *Guide to indistrial Control Systems Security.* National Institute of Standards and Technology.

Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 1.* Cisco Press.

Odom, W. (2020). *CCNA 200-301 Official Cert Guide, Volume 2.* Cisco Press.

Putty. (s.f.). *https://putty.org/*. Obtenido de https://putty.org/

SIEMENS. (17 de 1 de 2021). *SiePortal* . Obtenido de 8970169 services ports: https://support.industry.siemens.com/cs/document/8970169/which-ports-are-used-by-the-various-services-for-data-transfer-via-tcp-and-udp-and-what-should-you-watch-out-for-when-using-routers-and-firewalls-?dti=0&lc=en-WW

SIEMENS. (9 de 2022). *CPU-CPU Communication with SIMATIC Controllers.* Obtenido de https://support.industry.siemens.com/cs/ww/en/view/78028908