UCUENCA

Universidad de Cuenca

Facultad de Ingeniería

Carrera de Electrónica y Telecomunicaciones

Construcción e implementación de un modelo para diagnosticar el nivel de la ciberseguridad en una micro-red. Caso de Estudio: micro-red de la Universidad de Cuenca.

Trabajo de titulación previo a la obtención del título de Ingeniero en Electrónica y telecomunicaciones.

Autor:

Daniela Dolores Jiménez Mendieta

Julio Andres Sumba Naula

Director:

Darwin Fabian Astudillo Salinas

ORCID: 0000-0001-7644-0270

Cuenca, Ecuador

2023-05-25

Resumen

Un ciberataque en una infraestructura crítica puede provocar un fallo o interrupción en su funcionamiento. Las consecuencias directas en el entorno donde se produce el impacto son muy elevadas, ocasionando graves pérdidas económicas, además de poner en peligro vidas humanas o afectar el medio ambiente. Una micro-red está dentro de este tipo de estructuras, por lo que es importante un modelo de madurez de ciberseguridad para estas. En el presente trabajo se realizó la construcción de un modelo de madurez de ciberseguridad, el cual permite medir el nivel de madurez de ciberseguridad en una micro-red, este modelo se basa en las series ISO 27000, NIST 800 y el modelo C2M2. El modelo se compone de diez dominios, los cuales tienen una serie de atributos con distintos puntajes asignados, y cuatro niveles indicadores de madurez NIM, los cuales tienen un rango de puntaje e indicadores de color para establecer el nivel de madurez en el que se encuentra una micro-red. Se desarrolló una aplicación web, la cual permite la evaluación de ciberseguridad usando el modelo creado mediante un cuestionario, permitiendo establecer y mostrar el nivel de madurez en el que se encuentra una micro-red según los resultados. Como caso de estudio, se realizó la evaluación a la micro-red de la Universidad de Cuenca. Los resultados obtenidos son detallados, y en base a los mismos se procedió a realizar las recomendaciones para aumentar el nivel de madurez de la misma.

Palabras clave: ciberseguridad, modelo de madurez, micro-red

Abstract

A cyberattack on a critical infrastructure can cause a crash or interruption in its operation. The direct consequences in the environment where the impact occurs are very high, causing serious economic losses, in addition to endangering human lives or affecting the environment. A micro-grid is within this type of structure, so a cybersecurity maturity model is important for them. In the present work, the construction of a cybersecurity maturity model was made, which allows measuring the level of cybersecurity maturity in a micro-grid, this model is based on the series ISO 27000, NIST 800 and the C2M2 model. The model is made up of ten domains, which have a series of attributes with different assigned scores, and four levels of maturity indicators NIM, which have a range of scores and color indicators to establish the level of maturity in which is a micro-grid. A web application was developed, which allows the evaluation of cybersecurity using the model created through a questionnaire, allowing to establish and show the level of maturity in which a micro-grid according to the results. As a case study, the evaluation of the microgrid of the University of Cuenca was carried out. The results obtained are detailed, and based on them, recommendations were made to increase the level of maturity of the same.

Keywords: cibersecurity, madurity model, micro-grid

Índice general

Índice de figuras

Índice de tablas

Dedicatoria y agradecimientos

Agradezco primeramente a Dios por permitirme alcanzar esta meta tan importante en mi vida, brindándome bendiciones y sabiduría necesaria para llevar este camino. A mi ángel Juan Antonio que desde el cielo me ha acompañado en los momentos que más he necesitado.

A mis padres Julia y Norman sin su apoyo no hubiera logrado alcanzar este objetivo, gracias por estar siempre para mi impulsándome en cada momento, dándome el aliento necesario para no rendirme por más difícil que se torne el camino. A mis hermanos Norman y Julio por ser mi ejemplo a seguir y mi apoyo incondicional. Este logro también es suyo.

Un agradecimiento especial a mi compañero de tesis Andrés y de igual manera a nuestro director de tesis Ing. Fabian Astudillo por brindarnos el apoyo y los conocimientos necesarios para lograr cumplir con este trabajo de titulación.

Daniela Dolores Jiménez Mendieta

Dedicatoria y agradecimientos

Gracias a Dios por la fortaleza y mentalidad que me ha dado a lo largo de este camino y de toda mi vida. A mis padres, Julio y Blanca, que día a día son un ejemplo para mí, y que siempre han estado aquí para apoyarme, aconsejarme y darme ánimos. A mi hermana Priscila, que ha sido un ejemplo de dedicación durante toda mi vida y siempre está para ayudarme. A mi tía Gladys, que en incontables veces ha brindado su apoyo y cariño a toda la familia.

En todo este camino nunca estuve solo, compañeros y amigos también hicieron parte del mismo, gracias a todos ellos. Un agradecimiento especial a mi compañera de tesis Daniela y de igual manera a mi tutor de tesis Ing. Fabián Astudillo por todo el conocimiento compartido en las aulas y en este trabajo.

Julio Andres Sumba Naula

Abreviaciones y acrónimos

AEAD Authenticated Encryption with Associated Data. 78

BMS Sistema de gestión de batería. 63

C2M2 *Cybersecurity Capability Maturity Model*. 2, 3, 18, 32, 33

CA Corriente alterna. 64

CEA Conciencia del estado actual. 7, 9, 42, 52, 67, 95, 100

CIA *Confidentiality, Integrity, Availability*. 17

CMFA *Cybesecurity Maturity Assessment Framework*. 32

CMMC *Cybersecurity Maturity Model Certification*. 60

COBIT Control Objectives for Information and Related Technology. 33

CP Capacitación del Personal. 7, 9, 42, 58, 67, 95, 104

CYSFAM *Cybesecurity Focus Area Maturity*. 32

DCS Sistemas de Control Distribuido. 29

DoE *Departament of Energy*. 33

DoS *Denegation of Service*. 23, 39, 84

DTIC Dirección de Tecnologías de la Información y Comunicación. 68

ES-C2M2 *Electricity Subsector Cybersecurity Capability Maturity Model*. 33

GA Gestión de activos. 7, 9, 42, 46, 47, 95, 97

GAV Gestión de amenazas y vulnerabilidades. 7, 9, 42, 50, 67, 95, 99

GDE Gestión de dependencias externas. 7, 9, 42, 56, 67, 95, 103

GIA Gestión de identidad y acceso. 7, 9, 42, 48, 67, 95, 98

GPC Gestión del programa de ciberseguridad. 7, 9, 42, 59, 60, 67, 95, 105

GR Gestión de riesgos. 7, 9, 41, 45, 67, 95, 96

ICMP Internet Control Message Protocol. 76

ICS Sistema de Control Industrial. 28, 29

IDPS Intrusion Detection Prevention System. 39

IDS Intrusion Detection System. 39

IIC Intercambio de información y comunicaciones. 7, 9, 42, 53, 67, 95, 101

IoT Internet of Things. 31

IPS Intrusion Prevention System. 39

ISO *International Organization for Standardization*. 2, 3, 18, 20, 23, 25–27, 32, 33, 35, 60, 66, 69, 73

NIM Nivel Indicador de Madurez. 2, 3, 34, 35, 43, 44, 67, 68, 87

NIST *National Institute of Standards and Technology*. 2, 3, 18, 20, 25, 28, 29, 31–33, 35, 60

OLE *Object Linking and Embedding*. 13, 30

OPC *OLE for Process Control*. 20, 30, 111

PCI DSS *Payment Card Industry Data Security Standard*. 33

PHVA Planificar-Hacer-Verificar-Actuar. 26, 27

PLC Control Lógico Programable. 8, 30, 31, 63, 82, 111–113

R-C2M2 *Railway Cybersecurity Capability Maturity Model*. 33

RFID *Radio Frequency Identification*. 69

RI Repuesta a incidentes. 7, 9, 42, 54, 67, 95, 102

RTU Unidad de terminal remoto. 8, 30, 31, 63, 111, 113

SCADA Sitema de Control y Adquisición de Datos. 8, 29, 30, 38, 69, 71, 79, 111, 112

SGSI Sistema de Gestión de la Seguridad de la Información. 26, 27

SNMP Simple Network Management Protocol. 76, 77

SSL Secure Sockets Layer. 76–79, 82

TI Tecnología de la Información. 2, 3, 32, 34, 35, 42, 46, 47, 50, 51, 55, 56, 60, 63, 68, 71, 79, 81

TLS Transport Layer Security. 76–79, 82

TO Tecnología de Operaciones. 2, 3, 9, 32, 34, 35, 42, 46, 47, 50, 51, 55, 56, 60, 63, 66, 68, 71, 79, 81

Glosario

firmware Software que tiene directa interacción con el hardware, siendo así el encargado de controlarlo para ejecutar correctamente las instrucciones externas. 47

framework Conjunto de herramientas y módulos que pueden ser reutilizados para varios proyectos. 34

pentesting Ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. 71, 72, 87, 114

1. Introducción

En la actualidad la digitalización de varios procesos y servicios, algunos de estos industriales, aportan de manera considerable al desarrollo de un país; sin embargo, también trae consigo muchos riesgos que pueden afectar gravemente la seguridad de los procesos industriales. Estos riesgos pueden ser actividades como espionaje, sabotaje, fraudes o ciberataques realizados por otros países, grupos delictivos o terroristas u otros particulares. Nuevas tecnologías traen consigo nuevas vulnerabilidades y riesgos. Por lo tanto, es necesario proponer un plan de protección y prevención para mitigar las nuevas amenazas.

Este capítulo se organiza de la siguiente manera. En la Sección 1.1 se presentan los antecedentes. En la Sección 1.2 se describe el proyecto y su alcance. Por último, la Sección 1.3 menciona los objetivos de este proyecto.

1.1. Antecedentes

La ciberseguridad en la actualidad es de gran importancia debido a que trata la protección de información digital, dispositivos y activos, los cuales forman parte de la mayoría de sistemas industriales. Según [2], estos sistemas podrán contar con protección ante ataques informáticos, hackeos o cualquier robo de datos o identidad, la cual se logra con nuevas herramientas que van apareciendo con el fin de evitar múltiples amenazas al utilizar nueva tecnología.

Hoy en día, la mayoría de procesos industriales como: distribución de gas, fabricación de productos de primera necesidad, transporte de petróleo, distribución de energía eléctrica, etc., están automatizados. El objetivo es disminuir los de costes de fabricación, mantener la calidad en los medios de producción, y redimir al ser humano de las tareas tediosas, peligrosas e insalubres [3].

El término de infraestructura crítica es empleado para describir activos esenciales para el funcionamiento de la sociedad y la economía. Estas infraestructuras ejecutan diversos procesos industriales los cuales son vulnerables a ataques cibernéticos. En consecuencia, para garantizar el funcionamiento de los diferentes servicios es necesaria la protección de sus infraestructuras. Uno de estas infraestructuras es la del sector eléctrico.

En el artículo [4] se abordan los principales riesgos de seguridad al que se exponen las empresas en el siglo XXI. Los autores mencionan que la seguridad de la información depende de la

triada *Confidentiality, Integrity, Availability* (CIA). La confidencialidad hace referencia al hecho de que la información de una organización solo puede ser conocida por personal otorgado a la misma. Mientras que la integridad se refiere a que la información solo se modifica dentro de un proceso corporativo legítimo desde un lugar autorizado. Finalmente, la disponibilidad hace referencia a la garantía de que la información será accesible por el personal autorizado cuando sea necesario.

De acuerdo con el reporte de la oficina del director de Inteligencia Nacional de los Estados Unidos [5], las amenazas a la infraestructura crítica en el sector eléctrico son múltiples como por ejemplo los ataques a las infraestructuras de generación y distribución de electricidad. Un ataque cibernético en un sistema de suministro de energía puede tener un impacto significativo en la disponibilidad de un sistema para realizar funciones críticas, así como en su integridad y la confidencialidad de la información. Esto, a su vez, podría afectar la seguridad nacional, la seguridad pública y la economía [6].

Como se menciona en [7] a menudo se considera la infraestructura del sector de energía eléctrica, tanto de generación como de transmisión eléctricas, como la más crítica de las infraestructuras: cuando esta deja de funcionar se paralizan otras infraestructuras como las del transporte, servicios de hospitales, redes de comunicación, etc.

Los sistemas eléctricos son una infraestructura crítica; con la creciente digitalización se vuelven particularmente vulnerables a los ciberataques. Por lo tanto, la ciberseguridad se vuelve cada vez más crucial para proveer el suministro [8]. Dado que se requiere un mecanismo de defensa frente a los ataques para intentar evitarlos antes de que ocurran, es necesario conocer las vulnerabilidades a las que se enfrentan las empresas de energía.

Un ataque comienza con la selección de un objetivo y la exploración de vulnerabilidades; conocer las vulnerabilidades es importante tanto para realizar un ataque hacia el objetivo como para realizar la protección del mismo [9]. Uno de los principales puntos de entrada a los objetivos es el factor humano, las personas pueden abrir accidentalmente correos infectados o conectar dispositivos con virus (por ejemplo USB) a dispositivos conectados a la red de una industria.

Un ejemplo de estos ciberataques es el ocurrido en la ciudad de Oldsmar en Florida, en donde se consiguió acceder al sistema de agua de la ciudad. Lo que buscaban los atacantes es envenenar el suministro de agua aumentando la cantidad de hidróxido de sodio. Otro ejemplo importante que ha surgido en la actualidad es el sucedido en Costa Rica en donde se realizaron una serie de ciberataques contra sus instituciones públicas como: Ministerio de tra-

bajo, Ministerio de Ciencia, tecnología y Telecomunicaciones, entre otras, con la finalidad de usurpar todo tipo de información [10, 11].

Ecuador tiene muchas deficiencias para identificar riesgos. Además, al país le faltan herramientas jurídicas institucionales para tener un nivel de ciberseguridad adecuado [12]. Por ende, es urgente que el país elabore una estrategia nacional de ciberseguridad para proteger su infraestructura informática, de comunicaciones y crítica. Para el desarrollo de estas políticas deben considerarse a varias instituciones tales como: Ministerio de Telecomunicaciones, Ministerio de Defensa Nacional, Fiscalía, Ministerio del Interior, la academia entre otros; tomando como referencia la experiencia y estrategias en ciberdefensa de los países de la región.

1.2. Descripción y alcance del proyecto

El presente proyecto define un modelo para medir el nivel de madurez de la ciberseguridad de las micro-redes. Este modelo permitirá plantear acciones y actividades de protección para mejorar el nivel de madurez; se utilizará como base los estándares y normativas dados por la ISO 27000, NIST 800 y el modelo C2M2. A partir de los estándares y modelos anteriormente mencionados, se formulará una serie de requisitos de ciberseguridad que debería cumplir cada nivel de madurez en las micro-redes, teniendo así un modelo que permita analizar la ciberseguridad en estas. Una vez conocidos los dominios que se ha planteado para el modelo, se establecen atributos dentro de cada dominio con un puntaje para permitir evaluar una micro-red y determinar en que nivel de madurez se encuentra la misma.

Este modelo será implementado en una aplicación que facilitará la evaluación periódica por parte de los encargados de la micro-red y permitirá visualizar la evolución del nivel de seguridad mediante un *Dashboard*.

Como caso de estudio se determinará el nivel de madurez actual de la micro-red de la Universidad de Cuenca. Para esto se aplicará el modelo de madurez establecido, con los resultados obtenidos se recomendarán las acciones para incrementar al menos un nivel del actual. El trabajo de titulación realizado se ha enfocado dentro de la formación académica recibida, para contribuir al empleo de materiales y medios que proporcionen seguridad, confidencialidad y máximo acceso a redes y servicios de telecomunicaciones.

1.3. Objetivos

1.3.1. Objetivo general

Construir e implementar un modelo de madurez para diagnosticar el nivel de ciberseguridad en las micro-redes.

1.3.2. Objetivos específicos

- Realizar el estado del arte referente al nivel de madurez de ciberseguridad.
- Definir el modelo más adecuado para medir la madurez de la ciberseguridad en las micro-redes eléctricas.
- Aplicar el modelo creado a la micro-red en la Universidad de Cuenca.
- Recomendar las acciones necesarias para subir en al menos un nivel, el estado actual de madurez de la micro-red de la Universidad de Cuenca.

2. Marco teórico y estado del arte

En este capítulo se indican los fundamentos teóricos y principios importantes relacionados con la temática del trabajo desarrollado. En la Sección 2.1 se presenta conceptos de micro-redes y los componentes que constan en las mismas. La Sección 2.2 enfoca conceptos sobre las diferentes amenazas a redes industriales. En la Sección 2.3 se analiza el concepto control de acceso físico. La Sección 2.4 presenta la ciberseguridad en micro-redes. En la Sección 2.5 se introduce el concepto de modelo de madurez. Las secciones 2.6 y 2.8 presentan las normativas ISO y NIST respectivamente. La Sección 2.9 aborda lo que es la pirámide de automatización y su importancia dentro de las industrias y las tecnologías que usan.La Sección 2.10 define sistema de control y adquisición de datos, en 2.11 se realiza la definición de OPC, en 2.12 puntualiza el control lógico programable. Por último, la Sección 2.14 describe el estado de arte del tema tratado en este trabajo.

2.1. Micro-redes

La micro-red es un sistema de generación eléctrica bidireccional que permite la distribución de electricidad desde los proveedores hasta los consumidores. La tecnología digital favorece la integración de las fuentes de generación de origen renovable con el objetivo de ahorrar energía, reducir costes e incrementar la fiabilidad. Los tamaños de una micro-red van desde los 3KW a los 10MW, inferiores a los de las grandes centrales generadoras actuales [13]. Estas micro-redes proveen a un número específico de usuarios, estas son alimentadas por generadores o fuentes de energía renovables como: paneles solares, energía eólica, energía hidráulica, etc.

2.1.1. Elementos que conforman una Micro-red

Los elementos que forman una micro-red son:

Sistemas de generación distribuida: Los elementos de generación pueden diferir mucho entre una micro-red y otra en función de los recursos del lugar de instalación. Además, existen numerosas clasificaciones según:

- Origen de la electricidad: Renovables o no renovables.
- Controlables o intermitentes: Según el modo de operación.

- Recurso energético primario.
- Interfaz basada en electrónica de potencia.

Los componentes de generación que son parte de una micro-red son: aerogeneradores, paneles solares, micro turbinas, sistemas electrógenos (generadores diésel) y pilas de combustible [14].

Sistemas de almacenamiento de energía: Uno de los componentes más importantes de una micro-red debido a sus principales usos y aplicaciones son los sistemas de almacenamiento de energía. Es una forma de garantizar la continuidad eléctrica y cubrir los picos de la misma, de esta manera solo se consume de ella en los momentos de menor demanda, y por tanto, de menor precio de la electricidad. También permite inyectar electricidad en la red en los momentos de mayores tarifas para sistemas de generación externos [13].

Cargas de una micro-red: Estas cargas pueden clasificarse en torno a muchos aspectos: cargas controlables o no controlables, cargas críticas o prioritarias, cargas no críticas, cargas inteligentes o cargas convencionales y cargas de corriente continua o corriente alterna.

Interruptor: Se cuenta con al menos un interruptor general que permita la conexión/desconexión de la red eléctrica. Esto puede tener un papel crucial en el caso de que ocurran fallas a tierra o entre fases.

Protecciones: Será necesaria la instalación de diversos mecanismos de protección para la micro-red que garanticen el correcto funcionamiento del conjunto generadores-cargas. Las protecciones fundamentales son: protecciones contra cortocircuitos o sobre-tensiones, que ayudan a detectar fallas en el sistema [13].

Sistemas de control: En una micro-red es fundamental y necesario un sistema de control robusto que permita la monitorización del estado de la red como la realización de cambios rápidos y eficaces en los elementos que la componen. La clasificación según los elementos controlados puede ser: control de la potencia activa (P) y la potencia reactiva (Q) o control de la frecuencia y tensión de la red [15].

2.2. Amenazas a redes industriales

Existen algunas formas de vulnerar un sistema hoy en día, por lo que es necesario mencionar las amenazas más usadas para infligir un daño a sistemas que se encuentran vulnerables.

2.2.1. Código malicioso

Dentro de este ámbito se incluyen algunas amenazas de seguridad que son programadas en la computadora, en donde se ve comprometido el *software* de los sistemas operativos y la seguridad para irradiar el código malicioso.

Según lo explicado en [16] existen programas desarrollados que son utilizados para lanzar ataques a sistemas remotos, pudiendo desencadenar innumerables problemas. Existen diferentes códigos maliciosos como *"Caballo de Troya"* en donde el usuario es engañado mediante la descarga de otro programa que ayuda a tomar control sobre la máquina afectada. Otro ejemplo es el *"Gusano"* en donde no se necesita intervención humana y se propaga causando incidentes graves de seguridad.

2.2.2. Ataque de contraseñas

Técnica utilizada por los intrusos para obtener acceso ilegal a un sistema. En donde se trata de conseguir el nombre del usuario y la contraseña del mismo. Un método utilizado para este ataque es el *ataque de diccionario*, en donde se realiza una lista con miles de posibles contraseña, luego son encriptados con el mismo *script* usado para encriptar las claves, se comparan, y si se encuentra coincidencia, se conoce rápidamente el usuario y la clave, con lo que se vulnera al sistema [16].

En ocasiones estos ataques son utilizados en entidades financieras, en donde se logra acceder a páginas de enlaces falsos y los clientes proporcionan la información como: número de cedula, número de tarjeta de crédito, código de tarjeta de crédito,logrando efectuar fraudes. Actualmente se emplean mecanismos de cifrado que ayudan a evitar estas intromisiones.

2.2.3. Ataque de denegación de servicios (DoS)

En este tipo de ataque los usuarios no autorizados tienen acceso a los recursos. Es usado por los intrusos cuando han fallado en el intento de ingresar al sistema. En ocasiones, el sistema

se sobrecarga por las numerosas peticiones provenientes del ataque, provocando que no atienda a peticiones legítimas.

Este tipo de ataque puede ser más crítico ya que podría direccionarse a elementos físicos, produciendo un daño agresivo o incluso destruyendo el disco duro, dejando a los servidores inutilizados o eliminando programas que detienen un proceso de producción.

El ataque de *Denegation of Service* (DoS) causa la interrupción de uno o varios servicios por el uso excesivo de los servidores o elementos de red intermedios. Como consecuencias se tiene el consumo excesivo de ancho de banda, alteración del CPU, limitación de memoria, alteración base de datos, etc.

2.3. Control de acceso físico

El control de acceso a las instalaciones y puntos críticos de una industria es de gran importancia para evitar las manipulaciones mal intencionadas de equipos y el robo de información. Las puertas de acceso deben soportar ingresos forzados y resistentes, además de contar con cerraduras magnéticas, llaves especiales o controles biométricos. El acceso físico puede administrarse usando los apartados sobre seguridad física y del entorno de la norma ISO 27002 [17]. Las políticas de control de acceso físico deben ser acatadas por todo el personal que solicite acceso a espacios críticos, tales como cuarto de servidores, cuarto de control, etc.

2.4. Ciberseguridad en micro-redes

Para hablar de la ciberseguridad en las micro-redes, deben estar claros los conceptos tanto de ciberseguridad como de micro-red. La ciberseguridad es definida por [18] como la aplicación y gestión de técnicas con la finalidad de proteger la confidencialidad, integridad y disponibilidad de la información.

Se denomina micro-red a los sistemas de energía de baja y media potencia, los cuales son de tamaño pequeño y funcionan con un grupo descentralizado de fuentes y cargas de electricidad, los cuales pueden operar conectados o desconectados a la red principal [19]. Estos sistemas deben tener una estructura de red fiable y flexible, esto se debe a que su principal objetivo es la disminución de combustibles fósiles y resolver problemas de energía [20].

Para un manejo óptimo de las micro-redes se usan tecnologías de la información y comunicación. El uso de distintos dispositivos y componentes a los que se pueden acceder de manera

física o remota hacen que una micro-red sea vulnerable a sufrir ataques cibernéticos y físicos.

En [20] se presentan tres pilares fundamentales de ciberseguridad, mismos que deben cumplirse en una micro-red:

Confidencialidad: La información del sistema no puede ser revelada ni llegar a terceros. Se debe asegurar la información de clientes y del mercado eléctrico.

Integridad: Es un requisito crítico en sistemas de energía, ya que se pueden tener casos en los cuales los datos son modificados sin autorización, la fuente y tiempo de los datos no son autenticados lo que provoca un desconocimiento de la calidad de los datos.

Disponibilidad: Es de suma importancia en contextos industriales. El bloquear el funcionamiento de una micro-red trae consigo pérdidas económicas y de reputación de una empresa, además de los problemas que causan el daño o interrupción de una infraestructura crítica.

En [21] se propone dos pilares importantes dentro de la ciberseguridad, los cuales aportan a la seguridad dentro de una red.

Autenticidad Capacidad o característica de una entidad o usuario que garantiza que es quien dice ser o la fuente de la que proviene la información.

Verificalidad Capacidad de verificar y comprobar la autenticidad e integridad de los datos o información.

El impacto de un ciberataque a una infraestructura crítica puede producir la interrupción de servicios básicos (agua potable, energía eléctrica, telecomunicaciones, etc), en caso de tratarse de energía eléctrica puede producirse un efecto cascada, afectando al funcionamiento de otras industrias o áreas de salud [22].

Para [23] es posible mejorar la resiliencia de la ciberseguridad del sector eléctrico si se siguen principios generales como: implementar estándares de ciberseguridad, realizar una evaluación continua de las medidas de ciberseguridad, usar un modelo de madurez para evaluar las capacidades de ciberseguridad y gestionar los riesgos.

2.5. Modelo de madurez

El modelo de madurez es un conjunto de características, atributos e indicadores que representan el logro y progreso en un dominio o disciplina. El modelo de madurez permite que una

industria evalúe sus prácticas y procesos en referencia de mejores prácticas, estándares u otros lineamientos importantes en una disciplina, permitiendo mejorar en la misma [24].

Para [24] y [25] los modelos de madurez están compuestos por:

Niveles: Representan el aspecto de medición de la madurez del modelo, cada nivel tiene atributos que lo definen.

Atributos: Son el contenido principal del modelo, se expresan como características, indicadores, prácticas o procesos. Si se demuestra que se cumplen los atributos se dice que se ha alcanzado un nivel y las capacidades que ese nivel representa.

Métodos de evaluación y puntuación: Garantizan la coherencia de la valoración.

Dominios: Definen el alcance del modelo de madurez, permiten agrupar atributos en un área de importancia.

Existen tres tipos de categorías de modelos de madurez.

Modelo de progresión: Es una escala simple de una característica, indicador o atributo, la progresión es marcada por el aumento del nivel. Proporciona una hoja de ruta de progresión de un atributo mejorado a medida que avanza la escala [24].

Modelo de capacidad: Este modelo mide la capacidad organizacional en torno a un conjunto de características, también la capacidad de la realización de alguna tarea, reflejando el grado en que las capacidades están integradas [24, 25].

Modelo híbrido: Reflejan transiciones entre niveles que son similares a un modelo de capacidad pero tienen una estructura de modelo de progresión [24].

Existen varios modelos de madurez para la ciberseguridad, cada uno de estos tiene diferentes enfoques para sus propósitos y objetivos basándose en distintos estándares. La mayoría de modelos de madurez se basan en normas, estándares y recomendaciones emitidas por organizaciones como ISO y NIST [26].

2.6. ISO 27000

La *International Organization for Standardization* (ISO) es una federación mundial de organismos nacionales de normalización. Es una organización no gubernamental que comprende organismos de normalización de más de 160 países, con un organismo de normalización que representa a cada país miembro. La norma ISO 27000, es la norma para la gestión segura

de la información se fundamenta en Planificar-Hacer-Verificar-Actuar (PHVA). En esta guía se presentan las siguientes etapas:

Arranque del proyecto: Se debe tomar en cuenta cuales son los objetivos que se desean alcanzar, para lo cual se debe tener el compromiso de los dirigentes de la organización con el fin de alcanzar el objetivo planteado, es necesario considerar que la propuesta va a minimizar los riesgos.

Planificación: Se determina el alcance del proyecto, se definen las políticas de seguridad basadas en la actividad de la empresa. Para este proceso es necesario conocer las vulnerabilidades y amenazas que podrían afectar el entorno de la red, considerando las consecuencias de la pérdida de confiabilidad o la disposición de la información.

Se debe asegurar que las actividades y los procesos operativos diarios estén diseñados, dirigidos y tengan recursos para gestionarse.

Implementación: Se debe definir en esta etapa un plan del tratamiento del riesgo para identificar las acciones a tomar y así poder implementarlas en base a los objetivos. Realizando la respectiva asignación del personal, asignación de actividades y recursos para garantizar las mismas.

Seguimiento: Se realizan las pruebas ejecutando los procedimientos para la revisión de la efectividad, en donde se analizan los resultados para comprobar si se ha cumplido con el objetivo. En esta etapa se puede detectar si es que existen falencias en los procedimientos. En esta etapa también se alerta sobre los cambios a nivel de la organización y verificando que se cumpla con la norma ISO 27001, para determinar mejoras en Sistema de Gestión de la Seguridad de la Información (SGSI).

Los beneficios más importantes del empleo de esta norma se los ha tomado de [27].

- Establece una metodología de gestión de seguridad.
- Reduce los riesgos de pérdida o robo de la información.
- Verifica los procesos de riesgos y controles.
- Ofrece garantía de calidad y confidencialidad comercial para los clientes.
- Identifica debilidades en el sistema y áreas de mejora.
- Garantiza continuidad de las operaciones necesarias, tras un incidente de gravedad.
- Genera reglas claras para las personas de la organización.

- Aumenta la seguridad en la gestión de procesos.

ISO 27001 La ISO 27001 se basa en el ciclo PHVA. Este ciclo puede aplicarse no solo al sistema de gestión sino también a cada elemento individual para proporcionar un enfoque en la mejora continua.

ISO 27002 La ISO 27002 está diseñada para que las organizaciones la usen como referencia para la selección controles dentro del proceso de implantación SGSI de la norma ISO 27001. Es posible usar esta norma en industrias y organizaciones para el desarrollo de directrices de gestión de la seguridad de la información, teniendo en cuenta su entorno específico de riesgo de seguridad de la información [28].

ISO 27006 Especifica los requisitos y brinda orientación para los organismos que brindan auditoría y certificación de un sistema de SGSI, además de los requisitos contenidos en ISO 17021-1 e ISO 27001. Su objetivo principal es para apoyar la acreditación de los organismos de certificación que brindan la certificación SGSI [29].

ISO 27019 Proporciona una guía basada en ISO 27002:2013 aplicada a los sistemas de control de procesos utilizados por la industria de servicios públicos de energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo, calor, y para el control de procesos de apoyo asociados [30].

2.7. ISO 31000

La ISO 31000 está destinada a ser una familia de normas relativas a la gestión de riesgos.El propósito de la norma es proporcionar principios y directrices genéricas sobre la gestión de riesgos. Por tanto, tiene por objeto proporcionar un paradigma universalmente reconocido por los profesionales y las organizaciones que emplean procesos de gestión de riesgos para sustituir a la miríada de las actuales normas, métodos y paradigmas que difieren entre industrias, temas y regiones.

El riesgo es definido por la norma,como el efecto de la incertidumbre sobre los objetivos. Trabajar con el estándar ayuda a tomar decisiones, establecer y lograr objetivos y mejorar el desempeño.Los riesgos comprenden varios niveles [31]:

Riesgos estratégicos están relacionados con los objetivos estratégicos de la organización. Por ejemplo, si la estrategia de una organización apunta a introducirse en nuevos merca-

dos, pero se desconocen las consecuencias de incumplir las expectativas de los clientes y usuarios, se incurriría en un riesgo estratégico.

Riesgos operacionales Tienen que ver con el propósito de los procesos que componen el negocio. Se presentan en la ejecución de tales procesos, y, si se materializan, pueden imposibilitar que la organización o parte de ella cumpla su función.

Riesgos tecnológicos Aluden a los equipos de tecnologías de información y comunicación y/o sus operaciones. Por ejemplo: sistemas operativos, aplicaciones, comunicaciones en las redes, entre otros. También abarcan ciberseguridad, privacidad y seguridad de la información.

Riesgos financieros Apuntan a las operaciones financieras, como pagos, deudas, ofertas, cobros y costos. Riesgos legales: Están ligados al cumplimiento de los requisitos legales y reglamentarios.

Riesgos de procesos Son riesgos relacionados con los resultados de un proceso y sus interacciones. Si se materializan, afectan la eficacia y la eficiencia de la organización.

2.8. NIST 800

El *National Institute of Standards and Technology* (NIST) es una agencia general no regulada que pertenece al departamento de comercio exterior de Estados Unidos, tiene como misión promover la innovación y la competitividad en base a normas y tecnologías para mejorar la estabilidad económica y la calidad de vida [32].

Esta serie comprende pautas, recomendaciones, especificaciones técnicas e informes anuales de las actividades de ciberseguridad de la NIST. Estas publicaciones abordan y respaldan la necesidad de seguridad y privacidad de la información y los sistemas de información del gobierno federal de Estados Unidos [33].

NIST 800-53 Establece controles para satisfacer un conjunto de requisitos de seguridad y privacidad que se han impuesto a los sistemas de información; estos son consistentes y complementarios con otros estándares nacionales e internacionales reconocidos de seguridad y privacidad de la información [34]. Se basa en fuentes que incluyen requisitos y controles de las comunidades de fabricación, defensa, finanzas, salud, transporte, energía, inteligencia y control industrial, además de otros estándares.

NIST 800-82 Esta publicación brinda una orientación para proteger los Sistema de Control In-

dustrial (ICS), incluyendo los sistemas Sitema de Control y Adquisición de Datos (SCADA), Sistemas de Control Distribuido (DCS) y otros sistemas que realizan control, presenta un control de seguridad adaptada a los ICS basada en NIST 800-53 [35].

2.9. Pirámide de automatización industrial

Una pirámide de automatización es una estructura estratégica orientada a la intercomunicación de cada uno de los niveles en el proceso de producción en una empresa. Esta estructura que integra personas, procesos, información y estructuras tecnológicas, proporciona un método más eficaz de gestión que ofrece muchas ventajas competitivas para la empresa [1].

Dentro de una industria es necesario un flujo efectivo y continuo de información a través de los distintos procesos y áreas de la misma, tanto procesos de fabricación, información de recursos y administración. La pirámide de automatización representa la manera en que los procesos de fabricación son integrados con los sistemas de gestión de la producción y la administración de los recursos [36]. Además, permite visualizar los elementos que intervienen en cada nivel en el proceso de producción [37].

Los niveles de la pirámide se relacionan entre sí, de manera jerárquica, mediante diferentes tipos de tecnologías (propias de cada fase de producción). Esto hace posible determinar la clase de instrumentos y herramientas tecnológicas que se utilizan en cada nivel de la pirámide [36, 37].

Los niveles que conforman esta pirámide son básicamente cinco, los mismos se presentan en la Figura 2.1:

- Nivel de instrumentación o de campo
- Nivel de control
- Nivel de supervisión
- Nivel de planificación
- Nivel de gestión

2.10. Sistema de control y adquisición de datos

El sistema SCADA incorporado en la micro-red sirve para supervisar, controlar y adquirir datos de los equipos que intervienen en la misma, en donde operan energías renovables como la

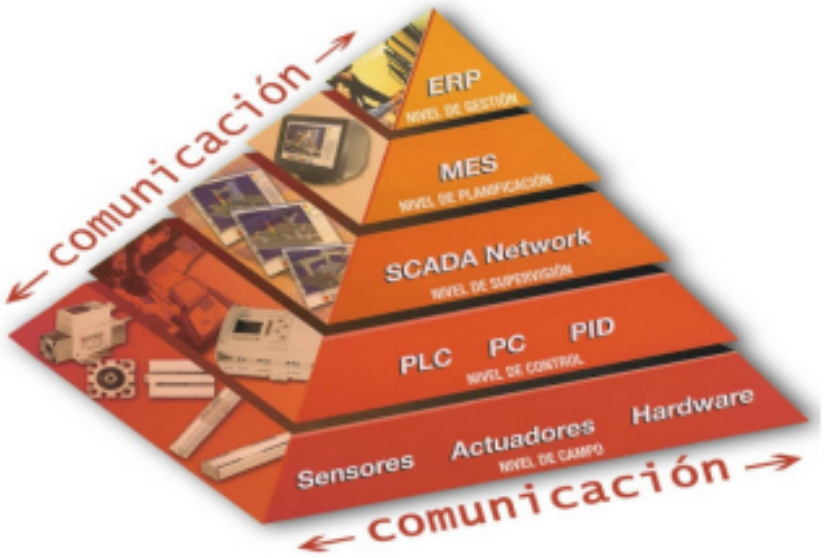

Figura 2.1: Pirámide de automatización industrial tomado de [1].

energía fotovoltaica, eólica y eléctrica [17].

Un sistema SCADA se emplea para controlar y monitorear los dispositivos que han sido instalados a lo largo del sistema eléctrico de potencia como: apertura y cierre de interruptores, seccionadores, reconectadores, etc.

2.11. Servidor OPC

OLE for Process Control (OPC) es una tecnología de comunicación con una arquitectura de cliente y servidor. Mediante una aplicación que actúa como servidor proporcionando datos y otra que como cliente leyéndolos o manipulándolos [38].

Con ello se permite el intercambio de información entre múltiples dispositivos y aplicaciones de control sin restricciones. Un servidor OPC puede estar comunicándose continuamente con los Control Lógico Programables (PLCs) de campo o Unidad de terminal remotos (RTUs). Aunque el *hardware* y el *software* provengan de diferentes marcas comerciales, el cumplimiento del estándar OPC posibilita la comunicación continua en tiempo real [39].

2.12. Control lógico programable

El PLC es utilizado para la automatización de los equipos y de los procesos industriales, los mismos poseen una programación compatible con sistemas de supervisión. Es una compu-

tadora industrial que usa la ingeniería para la automatización de procesos y tiene como finalidad, que las máquinas desarrollen efectivamente todos los sistemas que la componen. Gracias a estas bondades los PLC se han convertido en una herramienta fundamental para el desarrollo tecnológico de las industrias y todo el entorno social [40].

2.13. Unidades terminales remotas

Las RTUs son las encargadas de recopilar toda la información de campo como señales digitales, analógicas, mensajes de relés, para ser remitidas al PLC. Las mismas están conectadas a inversores que controlan los paneles solares, policristalinos, monocristalinos u otros inversores que están conectados a un sistema de gestión de baterías, banco de condensadores, rectificador, etc [41].

2.14. Trabajos relacionados

Las empresas industriales se enfrentan actualmente a desafíos importantes con respecto a la implementación de nuevas tecnologías como el Internet of Things (IoT), los sistemas físicos cibernéticos o la fabricación basada en la nube, también conocida como Industria 4.0. Como se menciona en [32], el NIST ha emitido un marco para proporcionar orientación a organizaciones dentro de sectores de infraestructura crítica para reducir el riesgo asociado con ciberseguridad. Por lo tanto, existe la necesidad de adoptar un modelo de madurez existente o crear uno para tener una forma común de medir el progreso de la implementación del mismo.

Un modelo de madurez tiene como función principal medir el estado actual de una organización en un ámbito en específico permitiendo el auto-análisis y la definición del estado de madurez a alcanzar. Dando así oportunidades de mejora y de optimización de los procesos relacionados [42]. Las características principales que debe cumplir un modelo es que sea fácil de implementar, completo, actualizado y que permita la evaluación en diferentes escalas.

Existen diversos estudios en los cuales se han analizado y se han propuesto modelos de madurez. Estos modelos se basan en distintas normas, estándares y recomendaciones, y cuentan con dominios y niveles. La principal diferencia entre los modelos es el área de enfoque o sector. Estos modelos se han diseñado para el área de salud, sistemas industriales, ferrocarriles, etc. A continuación se escriben los trabajos relacionados que presentan el análisis y creación de diversos modelos de madurez.

En la investigación realizada en [43] se presentan modelos de madurez de seguridad cibernética para organizaciones de atención médica que usan activamente la nube informática. Los modelos de madurez de la seguridad cibernética en el cuidado de la salud designan una colección de capacidades esperadas en una organización de atención médica; además, ayudan a facilitar su capacidad para identificar dónde sus prácticas son débiles o están ausentes, y dónde están realmente arraigadas. Este documento presenta una revisión de la literatura de los modelos de madurez para la nube, evaluación de la seguridad en el cuidado de la salud y argumenta la necesidad de un modelo de madurez de seguridad en la nube para las organizaciones.

Otro modelo de madurez es el planteado en [42], el cual es para brindar servicios a las organizaciones del sector financiero. Para el desarrollo se ha tomado en cuenta algunos *frameworks* y modelos existentes, expandiendo el alcance para la integración de las capacidades de seguridad en la nube y privacidad. Este modelo se ha realizado en base al cumplimiento de controles, los cuales son evaluados en una escala de cinco niveles de madurez: 1) Inicial, 2) En desarrollo, 3) Definido, 4) Gestionado y 5) Optimizado, los resultados han sido agrupados por dominios y funciones.

Existen diferentes modelos dependiendo del ámbito a tratar, en este caso se abarca las infraestructuras críticas en el modelo *Cybersecurity Capability Maturity Model* (C2M2). Definido en [44], es un modelo enfocado en la implementación y gestión de prácticas de ciberseguridad asociadas con la Tecnología de la Información (TI), Tecnología de Operaciones (TO) y los activos de información, además de los entornos en los que operan. Este modelo de madurez se basa en las recomendaciones NIST-800, consta de tres niveles:1) Funcional, 2) Intermedio y 3) Experto, y consta de diez dominios.

El modelo creado por [45], llamado *Cybesecurity Maturity Assessment Framework* (CMFA) puede usarse como herramienta de autoevaluación o herramienta de auditoría para operadores de servicios esenciales y de servicios digitales, centrándose en cuidados de salud y computación en la nube. Basándose en documentos emitidos por diversas organizaciones, entre las cuales destacan ISO y NIST, establece veinte requisitos de seguridad (agrupados en tres categorías principales: identificación, protección y reacción) y seis niveles de madurez (nivel cero como inexistente y nivel cinco como eficiente), este modelo es de escala cualitativa.

En [46] se crea el modelo de madurez *Cybesecurity Focus Area Maturity* (CYSFAM) para la evaluación de capacidades de seguridad cibernética. Este modelo se divide en enfoques de área técnica y de área organizacional con un total de once dominios. En este modelo, la mane-

ra de evaluar cada dominio es la de asignar un valor numérico a cada uno, dependiendo si este cumple o no con algunos requerimientos; este modelo se usó en una institución financiera.

En base al modelo C2M2, [26] crea el *Railway Cybersecurity Capability Maturity Model* (R-C2M2), tomando como base a [44]. El nuevo modelo consta de un nivel superior de madurez, el cual tiene prácticas más avanzadas o completas; este nivel propone el uso de herramientas de automatización y de inteligencia de amenazas.

De igual manera, el *Departament of Energy* (DoE) de los Estados Unidos, presentó en 2014 el modelo de autoevaluación *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2), el cual está formado por cuatro niveles y diez dominios [47]. Este modelo está basado en normas ISO y principalmente en las NIST, dado a que es un modelo propuesto por una entidad gubernamental de dicho país.

Los modelos mencionados se basan en estándares y recomendaciones relacionados con distintas entidades; en [48] se realizó una comparación de las emitidas por NIST, ISO, Control Objectives for Information and Related Technology (COBIT) y *Payment Card Industry Data Security Standard* (PCI DSS). El resultado de este proceso es una base de ventiún categorías que puede ser usada para medir el nivel de madurez de la ciberseguridad de una organización, este modelo es general, ya que se creó tomando en cuenta las áreas de enfoque de todas las entidades antes mencionadas.

Con la revisión de la literatura realizada, se observa que existen una serie de normativas y recomendaciones emitidas por muchas entidades, algunas gubernamentales, con las cuales se han creado modelos para distintas áreas de enfoque. Además, basándose en modelos existentes se establecieron modelos para sectores específicos, sin embargo, no existe un modelo destinado a las micro-redes.

3. Modelo para la medición de la madurez de la ciberseguridad en las micro-redes

En este capítulo se describe el modelo creado y sus componentes para la medición de la ciberseguridad en las micro-redes. En la Sección 3.1 se presenta la descripción del modelo y cómo está conformado, además de las bases utilizadas para la creación del mismo. En la sección 3.2 se presenta los mecanismos que debe cumplir un sistema de gestión y operación. En la Sección 3.3 se presentan los dominios que componen el modelo y los objetivos de cada uno de estos. Los niveles de madurez y sus características se detallan en la Sección 3.4. En la Sección 3.5 se describen los tributos de cada dominio para cada nivel. Por último, la Sección 3.6 presenta la aplicación creada para la evaluación de cualquier micro-red.

3.1. Modelo planteado para las micro-redes

El modelo planteado utiliza una escala de niveles, a cada nivel se lo denomina Nivel Indicador de Madurez (NIM). En cada NIM se define con un conjunto de atributos de tal manera que una micro-red cumpla con estos y así definir que ha logrado ese nivel, con las capacidades que representa el mismo. Tener los estados medibles entre los niveles permite a la micro-red utilizar la escala para:

- Definir su estado actual de madurez.
- Determinar un estado más maduro.
- Indicar los componentes que debe alcanzar para lograr ese estado futuro.

De manera general, la información que se va a cuestionar con un modelo de madurez para las micro-redes será:

- ¿Qué se está haciendo en la micro-red?
- Del conjunto de atributos: ¿cuáles se cumplen y cuáles no?
- ¿Cómo se está realizando los procesos? Verificando que atributos se cumplen.

Para la elaboración de este modelo se ha tomado como base el *framework* presentado en [44], el cual se centra en la implementación y gestión de prácticas de ciberseguridad asociadas a los activos de TI, TO y los entornos que operan dentro de las infraestructuras críticas.

El modelo propuesto en este trabajo está enfocado en las micro-redes, se compone de diez

dominios y cuatro NIMs. Cada dominio tiene objetivos y un conjunto de atributos de ciberseguridad, y cada NIM define la progresión del modelo de madurez en cada dominio. Esta estructura del modelo es representada por la Figura 3.1. Se aplican los siguientes principios para establecer los niveles de madurez:

- Los niveles de madurez son independientes a cada dominio.
- Los niveles son acumulativos en cada dominio, para estar en un determinado nivel la organización debe cumplir con todas los atributos de ese nivel y de los niveles anteriores.
- El modelo servirá como guía para mejorar la ciberseguridad y establecer un nivel de madurez en una micro-red.

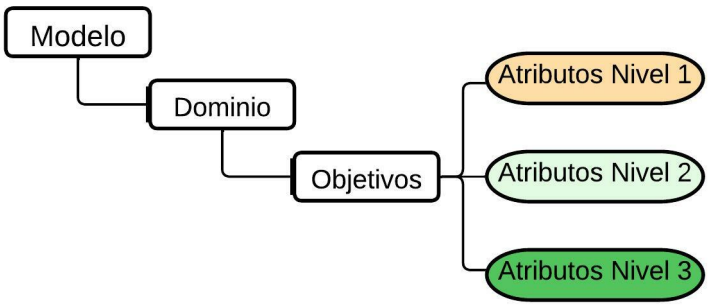

Figura 3.1: Estructura del modelo y sus elementos

El marco del modelo organiza los procesos y atributos para proporcionar una estructura y alinear el conjunto de capacidades dentro de cada dominio. Se ha tomado en cuenta para estructurar estos atributos la publicación del NIST 800 en donde se describe una guía para realizar las evaluaciones de riesgos dentro de los sistemas de información y organizaciones.

Otra base para establecer el modelo de este trabajo es la normativa ISO 27001, en donde el riesgo asociado a la seguridad de información se define como *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información"*. Por lo que se han considerado los riesgos y sus variables en cuanto a la seguridad de los procesos de las micro-redes. Todo activo de TI y TO podría tener al menos una vulnerabilidad por lo que tiene que ser evaluada para minimizar el riesgo. El modelo presentado basa sus dominios en los controles de la ISO 27002: gestión de activos, control de acceso, seguridad de las comunicaciones y gestión a incidentes.

Se toma como base diferentes normativas, estándares, pautas y recomendaciones de publicaciones oficiales, siendo una base sólida y justificada para la creación de un modelo de

madurez. Las guías e implementaciones prácticas, como la SP-1800-7(Conciencia situacional para servicios eléctricos) ofrece un enfoque técnico de un ejemplo realizado con productos de diferentes proveedores del sector eléctrico, son únicamente ejemplos y prácticas realizadas que se enfocan solo en la implementación o cambio de dispositivos, tomando en cuenta la ciberseguridad que debe existir en dicho proceso.

Todo esto se menciona en la misma publicación, en donde dice que *"Esta guía de prácticas de ciberseguridad del NIST describe nuestros esfuerzos de colaboración con los proveedores de tecnología y las partes interesadas del sector energético para abordar los desafíos de seguridad que enfrentan los proveedores de energía al implementar una capacidad integral de conocimiento de la situación. Ofrece un enfoque técnico para enfrentar el desafío y también incorpora una mentalidad de valor comercial al identificar las consideraciones estratégicas involucradas en la implementación de nuevas tecnologías. La guía proporciona una solución de ejemplo modular e integral que puede ser adaptada e implementada por proveedores de energía de diferentes tamaños y sofisticación."*[49]. Por este motivo no son tomadas como base para la creación de un modelo de madurez.

3.2. Sistema de gestión y operación

Una micro-red deberá cumplir con la implantación de diferentes mecanismos tales como:

Seguridad perimetral: Los cortafuegos también conocidos como *firewall* son dispositivos o sistemas que evitan el ingreso de paquetes no autorizados a una red, estableciendo enlaces controlados elevando una pared de seguridad al perímetro. Estos establecen un punto de resistencia en donde se mantiene a los usuarios no autorizados fuera de la red, dando protección ante ataques de suplantación de IP y enrutamiento. La seguridad perimetral que protege tus redes debe cumplir cuatro funciones básicas [50]:

- Resistir a los ataques externos.
- Identificar los ataques sufridos y alertar de ellos.
- Aislar y segmentar los distintos servicios y sistemas en función de su exposición a ataques.
- Filtrar y bloquear el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

Dentro de la seguridad de perímetro se encuentra la supervisión de accesos para lo cual

se puede implementar alarmas y controles. Se pueden implementar varias técnicas para control de acceso [51]:

- Control de Servicio: el cortafuegos puede filtrar el tráfico en base a direcciones IP y número de puertos TCP. Con la integración de funciones de proxy recibe e interpreta las solicitudes de acceso antes de proporcionar el ingreso.
- Control de Dirección: determina en qué dirección el cortafuegos puede iniciar las solicitudes de servicios particulares y en qué dirección se permite el ingreso a través del cortafuegos.
- Control de usuario: Controla el acceso al servicio en función del usuario que solicita el ingreso, puede emplearse para usuarios internos y externos.
- Control de comportamiento: Controla como se utilizan los servicios, por ejemplo, el cortafuegos puede filtrar correo basura.

Control de acceso a los recursos: El control de acceso es una forma de seguridad física que administra quién tiene acceso a un área en un momento dado. Los sistemas de control de acceso restringen el acceso a los usuarios autorizados y proporcionan un medio para realizar un seguimiento de quién entra y sale de las áreas seguras [52]. Tiene que ver con la determinación de las actividades permitidas de los usuarios legítimos, interviniendo cada intento de un usuario para acceder a un recurso en el sistema [53]. Al implementar un sistema de control de acceso, hay muchos factores a considerar como:

- Seguridad: el hardware debe ser a prueba de manipulaciones, el software debe actualizarse rutinariamente para protegerlo contra posibles vulnerabilidades, y las credenciales no deben estar sin cifrar, copiarse o compartirse fácilmente.
- Experiencia de usuario: el sistema de control de acceso debe ser fácil de configurar para los administradores, así como conveniente para los empleados y los inquilinos.
- Fiabilidad: junto con la experiencia del usuario, la fiabilidad es crucial. Los proveedores mejoran constantemente los métodos de acceso tradicionales a través de datos biométricos, códigos PIN y, más recientemente, credenciales de teléfonos inteligentes. Sin embargo, muchas de estas soluciones no son confiables o crean demasiada fricción. La mejor confiabilidad de su clase requiere múltiples formas de comunicación para autenticar una acción.
- Flexibilidad: los usuarios finales deben buscar un sistema que sea flexible, que

permita al usuario configurar la conveniencia y seguridad de cada puerta o entrada según los requisitos del mismo.

Existen diferentes tipos de control de acceso, los tres más comunes son [54]:

- Control de accesos basado en roles (RBAC): Este modelo otorga privilegios de acceso a los usuarios según el trabajo que realizan dentro de una organización. El modelo permite que un administrador asigne a un usuario uno o varios roles según sus asignaciones de trabajo. Cada rol permite acceso a recursos específicos.
- Control de accesos discrecional (DAC): Este modelo permite al propietario de un recurso decidir si permitir a una persona concreta acceder al recurso de pertenencia.
- Control de accesos obligatorio (MAC): Este modelo permite la agrupación o creación de recursos, según un modelo de sensibilidad. Un ejemplo de este modelo serían las clasificaciones de desclasificado, restringido, confidencial, secreto y alto secreto. Los privilegios que se otorgan a un usuario para ver determinados recursos dependen del nivel de acceso del usuario.

Autenticación de usuarios: Podemos definirla como un proceso de seguridad que evita que los usuarios no autorizados accedan a un dispositivo o red. Nos encontramos con un procedimiento de inicio de sesión donde una aplicación nos solicita nuestra contraseña para darnos acceso. En el caso de que un usuario no ponga su contraseña establecida la autenticación falla [55]. Los usuarios deben probar que son ellos los que están requiriendo acceder al sistema. Este proceso se realiza empleando métodos de combinación de: usuario y contraseña, preguntas de desafío y respuesta, y adicionalmente, se debe incluir cifrado [56].

Antivirus y antispyware: Los antivirus son programas que tienen como propósito detectar y evitar la activación de los virus. Los virus son programas que intervienen en el normal funcionamiento de los computadores causando problemas de *hardware* o del sistema operativo, suelen reproducirse fácilmente y son difíciles de detectar sin herramientas adecuadas [57]. En los sistemas SCADA también se ha reportado casos de ataques por gusanos, para combatir estos códigos maliciosos varias compañías desarrolladoras de antivirus han trabajado en conjunto con proveedores de sistemas SCADA para proporcionar protección sin comprometer su funcionamiento.

En cuanto a *antispyware* es una tecnología de seguridad que ayuda a proteger a un

equipo contra *spyware* que es un tipo de software que se instala en el ordenador sin que el usuario tenga constancia de ello. Suele venir oculto junto a otros programas que se instalan de manera consciente, lo que lo hace muy difícil de detectar, una vez en el ordenador, recopila información para enviarla a terceros. Este *software* ayuda a reducir los efectos causados por el *spyware* incluyendo el lento desempeño del equipo, ventanas de mensajes emergentes, cambios no deseados en configuraciones de Internet y uso no autorizado de la información privada [58], un ejemplo que se puede implementar es Avira Free Antivirus. Los síntomas que una computadora ha sido infectada por *spyware* son:

- Se abren continuamente ventanas emergentes mientras se navega en Internet.
- Se dirige a sitios web que no se han indicado.
- Aparecen barras de herramientas sin que se hayan especificado.

Detección y prevención de intrusiones: Un sistema de prevención de intrusos o Intrusion Prevention System (IPS), también conocido como Intrusion Detection Prevention System (IDPS), es una tecnología que vigila una red para detectar cualquier actividad maliciosa que intente aprovechar alguna vulnerabilidad conocida [59]. Se considera intrusión a toda actividad no autorizada o que no se espera que suceda en el normal funcionamiento de la red. Las tecnologías IPS pueden detectar o prevenir ataques de seguridad de red, como ataques de fuerza bruta, ataques DoS y vulnerabilidades de seguridad. Los Sistemas de Detección y Prevención de Intrusos (IPS/IDPS) ayudan a proteger las redes de comunicaciones y dispositivos. Configurados correctamente, contribuyen a descubrir y parar intrusiones, amenazas o comportamientos no deseados que ponen en riesgo la ciberseguridad de la empresa. Un Intrusion Detection System (IDS) es una tecnología de seguridad de red concebida inicialmente para detectar vulnerabilidades o *exploits* dirigidos contra una aplicación o sistema.

El método de detección basado en firmas utilizado por los IPS consiste en un diccionario de firmas identificables de manera única que se encuentran en el código de cada *exploit*. Hay dos tipos de métodos de detección basados en la firma para los sistemas de prevención de intrusos: los que se basan en la *exploit* y los que se basan en la vulnerabilidad. Los métodos orientados a *exploit* detectan la actividad maliciosa sobre la base de pautas de ataque comunes, mientras que los métodos orientados a la vulnerabilidad tratan de detectar la actividad maliciosa mediante la identificación de vulnerabilidades específicas [60].

Detección de comportamientos atípicos del tráfico: Asumiendo que todos los datos son generados por un conjunto de procesos, los valores atípicos son puntos con una baja probabilidad de ocurrencia dentro de un conjunto de datos determinado. Sin embargo, los valores atípicos no representan necesariamente un comportamiento anormal o un comportamiento que ocurrió debido a un proceso diferente [61]. Los valores atípicos son generados por el mismo proceso, pero ocurren con una menor probabilidad. Uno de los principales objetivos de los sistemas informáticos es ser capaces de detectar y controlar aquellos accesos no autorizados, o incluso prevenirlos antes de que se produzca una pérdida de valor en el sistema.

Las empresas generan volúmenes masivos de datos. Si se aprovechan correctamente, esos datos pueden ayudar a las empresas a tomar mejores decisiones, más rápido. Una forma es a través de la detección de anomalías, que puede evitar que un problema menor se convierta en un problema generalizado que consuma mucho tiempo. Mediante el uso de los últimos métodos de *Machine Learning*, las empresas pueden realizar un seguimiento de las tendencias, identificar oportunidades y amenazas, y obtener una ventaja competitiva con la detección de anomalías [62].

Auditoria de usuarios La auditoría es la recopilación de datos sobre el uso de los recursos del sistema. Los datos de auditoría proporcionan un registro de los eventos del sistema relacionados con la seguridad. Estos datos se pueden utilizar para asignar responsabilidad para acciones que ocurren en un *host*. La auditoría correcta comienza con dos funciones de seguridad: identificación y autenticación. En cada inicio de sesión, después de que un usuario proporciona un nombre de usuario y una contraseña, un único ID de sesión de auditoría se genera y se asocia con el proceso del usuario [63]. El ID de sesión de auditoría es heredado por cada proceso que se inicia durante la sesión de inicio de sesión. Incluso si un usuario cambia la identidad dentro de una única sesión, todas las acciones del usuario se rastrean con el mismo ID de sesión de auditoría.

Después de que los datos de auditoría se recopilan en el núcleo, los complementos distribuyen los datos a las ubicaciones adecuadas. A continuación, las herramientas de postselección permiten reducir y examinar partes interesantes de la pista de auditoría. Por ejemplo, puede elegir revisar registros de auditoría de usuarios individuales o grupos específicos [64]. Puede examinar todos los registros de un tipo determinado de evento en un día específico. O puede seleccionar registros que se han generado a una hora determinada del día. Con esto se puede hacer búsquedas relacionadas con eventos de

registro de usuarios y consultar qué acciones importantes han realizado los usuarios en sus propias cuentas. Entre estas acciones se incluyen cambios en contraseñas, en la información de recuperación de la cuenta (números de teléfono o direcciones de correo electrónico) y en el registro [65].

3.3. Dominios y objetivos

Cada uno de los diez dominios del modelo realizado contiene un conjunto estructurado de atributos de ciberseguridad, enfocado en el sector eléctrico, específicamente para las micro-redes. Cada conjunto de atributos representa las actividades que las micro-redes deben realizar para establecer y madurar en el dominio.

Cada dominio esta enfocado en el conjunto de atributos o prácticas que una micro-red puede realizar para establecer y madurar en cada ámbito de la misma. Para cada dominio, el modelo proporciona una declaración del objetivo, que es un resumen de la intención del dominio.

El modelo se puede utilizar para:

- Fortalecer las capacidades de ciberseguridad de la micro-red.
- Permitir que las micro-redes evalúen y comparen de manera efectiva y consistente las capacidades de ciberseguridad.
- Compartir conocimientos, mejorar prácticas y referencias relevantes entre las micro-redes como un medio para mejorar las capacidades de ciberseguridad.
- Permitir que las micro-redes prioricen acciones e inversiones para mejorar las capacidades de ciberseguridad.

Los dominios en los que se divide el modelo y sus objetivos son los listados y descritos en la Tabla 3.1.

Tabla 3.1: Dominios del modelo de madurez

Dominio	**Objetivos**
Gestión de riesgos (GR)	Establecer, operar y mantener un programa de gestión de riesgos de ciberseguridad para identificar, analizar y minimizar los riesgos de ciberseguridad para la micro-red, en donde se incluye su infraestructura interconectada relacionada y partes interesadas.

Gestión de activos (GA)	Gestionar los activos de TI y TO de la micro-red, incluidos el *hardware* y el *software*, de acuerdo con el riesgo de la infraestructura.
Gestión de identidad y acceso (GIA)	Gestionar las identidades para el personal al que se le puede conceder acceso lógico o físico a los activos de la micro-red. Controlar el acceso a los activos de la misma, al igual que el acceso a sus instalaciones.
Gestión de amenazas y vulnerabilidades (GAV)	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a las amenazas y vulnerabilidades de ciberseguridad, de acuerdo con el riesgo de la infraestructura de la micro-red.
Conciencia del estado actual (CEA)	Establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operativa y de ciberseguridad.
Intercambio de información y comunicaciones (IIC)	Establecer y mantener un marco para la interacción entre las microredes, con el objetivo de compartir información de ciberseguridad.
Repuesta a incidentes (RI)	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a incidentes de ciberseguridad y para mantener las operaciones durante dicho evento, de acuerdo al riesgo para la infraestructura.
Gestión de dependencias externas (GDE)	Establecer y mantener controles para gestionar los riesgos de ciberseguridad asociados con los servicios y activos que dependen de entidades externas.
Capacitación del Personal (CP)	Establecer y mantener planes, procedimientos, tecnologías y controles para crear ciberseguridad y garantizar la competencia continua del personal, de acuerdo con el riesgo para la infraestructura crítica y los objetivos organizacionales.
Gestión del programa de ciberseguridad (GPC)	Establecer y mantener un programa de ciberseguridad que proporcione planificación estratégica y amparo para las actividades de la micro-red de una manera que alinee los objetivos de ciberseguridad con los objetivos estratégicos de la micro-red.

3.4. Niveles de madurez

El modelo define cuatro NIMs, a los cuales se los clasifica desde cero a tres, que se aplican de forma independiente a cada dominio del modelo. A los indicadores de cada nivel se les asigna un valor, que al cumplirse se encuentran dentro de un rango de valores definido para cada nivel, los NIMs junto con sus nombres, valores y colores se presentan en la Tabla 3.2. Por otro lado, en la Tabla 3.3 se presenta un resumen de los indicadores del nivel de madurez.

Tabla 3.2: Niveles Indicadores de Madurez

Nivel	Nombre	Color	Puntos
NIM0	No Existente		[0-24]
NIM1	Inicial		[25-50]
NIM2	Satisfactorio		[51-75]
NIM3	Optimizado		[76-100]

Tabla 3.3: Características Niveles de Madurez

Nivel	Características
NIM0	No cumple con ningún atributo.
NIM1	Se realizan las prácticas iniciales. Por ejemplo: se inicia el proceso de identificar riesgos, se tiene un inventario de activos, etc. Si una micro-red inicia desde cero en la gestión y aplicación de ciberseguridad, debe centrarse en las prácticas de este nivel.
NIM2	Características de manejo: ▪ Los procesos están documentados. ▪ Se proporcionan recursos adecuados para realizar un proceso. ▪ El personal encargado de realizar las actividades tiene habilidades y conocimientos adecuados. Un enfoque característico: ▪ Los procesos son más avanzados y completos que en el NIM1.

NIM3	Características de manejo: ▪ Los procesos son guiados por políticas o directivas organizacionales. ▪ Los objetivos para desempeñar las actividades se establecen y monitorean para lograr la mejor ejecución. ▪ Las prácticas para las actividades de los dominios son documentadas y mejoradas en la micro-red. Un enfoque característico: ▪ Los procesos son más avanzados y completos que en el NIM2.

3.5. Atributos de los dominios

Los atributos de los dominios son basados en las prácticas que se cumplen dentro de cada nivel de madurez que ha sido establecido. En donde principalmente en un NIM0 no se han tomado medidas respecto a la ciberseguridad dado que la evolución de la micro-red no podría contar con ningún tipo de información referente a la importancia de la misma. Se ha considerado un nivel NIM1 en donde las prácticas empiezan a aparecer dentro de la micro-red. Y finalmente se procede analizar los NIM2 y NIM3, en donde cada nivel cumple con una serie de atributos referente a cada dominio. Siendo estos dos últimos los más avanzados en cuanto a la implementación de los atributos. La relación y plan de implementación de los atributos y NIMs de cada dominio se detallan en los esquemas de A para cada uno de estos.

El puntaje asignado a cada uno de los atributos es en base a la investigación realizada de cuáles de ellos son considerados más importantes y de mayor esfuerzo para su implementación, asignando a esos una puntuación mayor. Tal como se menciona en [66], para una evaluación se procede a la verificación de objetivos, actividades y tareas para comprobar en qué medida se alcanza el estado deseado del procedimiento, permitiendo evitar que este pase a la fase de implementación con un modelo erróneo. Asignando así puntajes que permitan establecer un diagnóstico.

3.5.1. Atributos del dominio de gestión de riesgos

El riesgo de ciberseguridad se define como el riesgo para las operaciones en la micro-red en donde se incluye las funciones y misión, los recursos y otras organizaciones debido al potencial de acceso, uso, divulgación, interrupción, modificación o destrucción de información

no autorizados.

El riesgo de ciberseguridad es un componente del entorno general de riesgo empresarial y se alimenta de la estrategia y el programa de gestión de riesgos empresariales de una organización. No se puede eliminar por completo, pero se puede gestionar a través de procesos informados para la toma de decisiones. Dentro de la micro-red sus principales objetivos son:

- Establecer la estrategia de gestión de riesgos de ciberseguridad en la micro-red.
- Gestionar los riesgos de ciberseguridad en la micro-red.
- Generar actividades de gestión en la micro-red.

Una estrategia de gestión de riesgos de ciberseguridad es importante ya que proporciona orientación para analizar y priorizar el mismo y define la tolerancia. Incluye una metodología de evaluación de riesgos, una estrategia de monitoreo de los mismos con un programa de ciberseguridad. El dominio GR toma en cuenta los objetivos descritos y presenta en la Tabla 3.4 los atributos relacionados con estos, formando así este dominio.

Tabla 3.4: Atributos necesarios para el dominio de GR.

Nivel	**Atributos**	**Puntos**
NIM1	Se identifican los riesgos de ciberseguridad en la micro-red.	25
	Los riesgos identificados son tratados, aceptados y tolerados.	50
NIM2	Existe una estrategia documentada de gestión de riesgos de ciberseguridad. Los riesgos son documentados.	54
	La estrategia proporciona un enfoque para la priorización de riesgos, incluido el impacto del riesgo.	60
	Se realizan evaluaciones de riesgos para identificar y monitorizar los mismos de acuerdo con la estrategia de gestión de riesgos.	64
	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas, para respaldar las actividades de gestión de riesgos.	70
	Se usan directrices para informar las actividades de gestión de riesgos.	75
NIM3	Los criterios de riesgo de la micro-red para evaluar, categorizar y priorizar los riesgos operativos son en función del impacto, la tolerancia al riesgo y los enfoques de respuesta al mismo están definidos y disponibles.	79

	La estrategia de gestión de riesgos se actualiza periódicamente para actualizar las amenazas.	82
	Se utiliza un registro estructurado de riesgos identificados para respaldar las actividades de gestión de riesgos.	85
	Las actividades de gestión de riesgos están guiadas por políticas documentadas u otras directivas organizacionales.	88
	Las políticas de gestión de riesgos incluyen requisitos de cumplimiento de normas y/o directrices específicas.	91
	Las actividades de gestión de riesgos se revisan periódicamente para garantizar el cumplimiento de la política.	94
	El personal que realiza actividades de gestión de riesgos tiene las habilidades y los conocimientos necesarios para desempeñar sus responsabilidades asignadas.	100

3.5.2. Atributos del dominio de gestión de activos

Un activo es un instrumento de valor para una organización. En este modelo, los activos a considerar son los activos de *hardware y software* de TI y TO, así como la información esencial para operar cada función. Dentro de la micro-red sus principales objetivos son:

- Administrar el inventario de activos de la micro-red.
- Administrar la configuración de activos de la micro-red.
- Gestionar las actividades de administración en la micro-red.

Un inventario de activos es importante para la ejecución de la micro-red, es un recurso dentro de la gestión del riesgo de ciberseguridad. Es importante tener un inventario sólido de activos ya que se puede identificar la ubicación de implementación del *software* que requiere ajustes. Administrar la configuración de activos implica definir una línea base de configuración para los activos de TI y TO, y garantizar que estén configurados de acuerdo a la misma. El dominio GA toma en cuenta los objetivos descritos; la Tabla 3.5 presenta los atributos relacionados con estos, formando así este dominio.

Tabla 3.5: Atributos necesarios para el dominio GA

Nivel	Atributos	Puntos
NIM1	Hay y un inventario de activos de TI y TO que son importantes para la ejecución de funciones en la micro-red.	25
	Se establecen líneas base de configuración de los activos.	35
	Los cambios en los activos inventariados se evalúan y aprueban antes de implementarse.	50
NIM2	Los cambios en los activos inventariados son registrados.	53
	El inventario de TI y TO incluye atributos que respaldan las actividades de ciberseguridad (por ejemplo, ubicación, sistema operativo y versiones de *firmware*, fecha de adquisición).	57
	Las líneas base de configuración se utilizan para configurar activos en la implementación y restauración de los mismos.	65
	Se establecen, siguen y mantienen procedimientos documentados para las actividades en el dominio gestión de activos .	68
	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas, para apoyar las actividades en el dominio gestión de activos.	75
NIM3	El inventario de activos de TI y TO está completo, además es actualizado periódicamente o cuando se ingresa o retira un activo.	77
	Los datos se destruyen o eliminan de forma segura de los activos de TI y TO antes de la redistribución y al final de la vida útil.	80
	El inventario de activos de información se utiliza para identificar los riesgos cibernéticos, como el riesgo de divulgación, el riesgo de destrucción y el riesgo de manipulación.	83
	Los activos de información se resetean o destruyen al final de su vida útil utilizando técnicas adecuadas a sus requisitos de ciberseguridad.	87
	Las configuraciones de activos se supervisan para garantizar la coherencia con las líneas de base a lo largo de los ciclos de vida de los activos.	90
	Los cambios en los activos se prueban y registran para determinar el impacto en la ciberseguridad antes de su implementación.	95

	El personal que realiza actividades en el dominio gestión de activos tiene las habilidades y los conocimientos necesarios para desempeñar sus responsabilidades asignadas.	100

3.5.3. Atributos del dominio de gestión de identidad y acceso

En este dominio, el control de acceso se aplica al acceso lógico a los activos utilizados en la micro-red, el acceso físico a los activos cibernéticos relevantes para cada función y los sistemas de control de acceso automatizado. Las prácticas inadecuadas de gestión de acceso pueden dar lugar a un uso, divulgación, destrucción o modificación no autorizados, así como a una exposición a riesgos de ciberseguridad. Dentro de la micro-red sus principales objetivos son:

- Establecer y mantener identidades para la micro-red.
- Controlar el acceso en la micro-red.
- Gestionar actividades para la micro-red.

El establecimiento y mantenimiento de identidades comienza con la aprobación y la eliminación de identidades disponibles cuando ya no son necesarias. Las entidades pueden incluir personas, así como dispositivos, sistemas o procesos que requieren acceso a los activos de la micro-red. El dominio GIA toma en cuenta los objetivos descritos; la Tabla 3.6 presenta los atributos relacionados con estos que forman este dominio.

Tabla 3.6: Atributos necesarios para el dominio GIA

Nivel	**Atributos**	**Puntos**
NIM1	Las identidades se proporcionan para el personal que requiere acceso a los activos de la micro-red.	32
	Se determinan los requisitos de acceso, incluidos los de acceso remoto. Tomando en cuenta qué personal puede acceder al activo y los parámetros de autenticación.	38
	El acceso se otorga al personal según los requisitos de la micro-red.	44
	Las identidades se dan de baja cuando ya no son necesarias.	50

NIM2	Los repositorios de identidad se revisan y actualizan periódicamente para garantizar que el personal aún necesita acceso.	54
	Las identidades se dan de baja dentro de los umbrales de tiempo definidos por la micro-red, es decir cuando ya no se necesitan.	58
	Los requisitos de acceso incorporan los principios de privilegio mínimo y separación de funciones.	62
	Se siguen prácticas documentadas para establecer y mantener identidades y controlar el acceso.	66
	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas para respaldar las actividades de gestión de identidad y acceso .	70
	Se han identificado estándares y/o directrices para informar las actividades de gestión de identidad y acceso.	75
NIM3	Los requisitos para las credenciales están informados por los criterios de riesgo de la micro-red.	79
	Los intentos de acceso extraños se monitorean como indicadores de eventos de ciberseguridad.	82
	Las actividades de administración de acceso e identidad están guiadas por políticas documentadas.	85
	Las políticas de gestión de identidad y acceso incluyen requisitos de cumplimiento para normas y/o directrices específicas.	88
	Las actividades de gestión de identidad y acceso se revisan periódicamente para garantizar el cumplimiento de la política.	91
	La responsabilidad y la autoridad para el desempeño de las actividades de gestión de identidad y acceso se asignan al personal.	94
	El personal que realiza las actividades de administración de acceso e identidad tiene las habilidades y el conocimiento necesario para desempeñar sus responsabilidades asignadas.	100

3.5.4. Atributos del dominio de gestión de amenazas y vulnerabilidades

Podrían existir vulnerabilidades dentro de la micro-red cuando se pueda afectar el cumplimiento de las operaciones, a través del acceso no autorizado lo que conlleva a la destrucción, modificación de la información o negación de un servicio. Las amenazas a los activos de in-

fraestructura de TI, TO y comunicación varían y pueden incluir actores maliciosos, como por ejemplo *malware*. Dentro de la micro-red sus principales objetivos son:

- Identificar y responder a las amenazas que puede afectar la micro-red.
- Reducir las vulnerabilidades de ciberseguridad en la micro-red.
- Realizar actividades de gestión de acceso para cada función en la micro-red.

La reducción de las vulnerabilidades de ciberseguridad comienza con la recopilación y el análisis de la información de vulnerabilidad. Al tomar en cuenta las vulnerabilidades debe considerarse el efecto de un activo expuesto y la importancia del mismo para cumplir con una función. El dominio GAV toma en cuenta los objetivos descritos; la Tabla 3.7 presenta los atributos relacionados con estos y que forman este dominio.

Tabla 3.7: Atributos necesarios para el dominio GAV

Nivel	**Atributos**	**Puntos**
NIM1	Se identifican fuentes de información para respaldar las actividades de gestión de amenazas.	25
	Se abordan las amenazas que se consideran importantes para el funcionamiento de la micro-red.	50
NIM2	Se establece un perfil de amenazas para cada función que incluye la probabilidad, la capacidad y el objetivo de las amenazas a las funciones.	54
	Se priorizan y monitorean las fuentes de información sobre amenazas que abordan todos los componentes de las mismas.	57
	Las amenazas se abordan de acuerdo con la prioridad asignada.	60
	Se realizan evaluaciones de vulnerabilidad de ciberseguridad como: revisiones de la arquitectura, pruebas de penetración, herramientas de identificación de vulnerabilidades.	63
	El impacto operativo se evalúa antes de implementar parches de ciberseguridad.	65
	Se proporcionan los recursos adecuados: personas, herramientas y financiamiento para respaldar las actividades de gestión de amenazas y vulnerabilidades.	70

	Se han identificado estándares y/o directrices para informar las actividades de gestión de amenazas y vulnerabilidades.	75
NIM3	El perfil de amenazas para cada función se valida con una frecuencia definida por la micro-red.	79
	El análisis y la priorización de las amenazas se basan en los criterios de función de riesgos.	82
	Las evaluaciones de vulnerabilidad de ciberseguridad se realizan para todos los activos, con una frecuencia definida por la micro-red.	85
	Se agrega información de vulnerabilidad de ciberseguridad al registro de riesgos.	88
	Las actividades de amenazas y vulnerabilidades están guiadas por políticas documentadas.	91
	Las políticas de gestión de amenazas y vulnerabilidades incluyen requisitos de cumplimiento para normas y/o directrices específicas.	94
	El personal que realiza actividades de gestión de amenazas y vulnerabilidades tiene las habilidades y el conocimiento necesario para desempeñar sus responsabilidades asignadas.	100

3.5.5. Atributos del dominio de Conciencia del estado actual

La conciencia del estado actual implica desarrollar un conocimiento casi en tiempo real de un entorno operativo. Esto se logra a través de un registro y supervisión de los activos de la infraestructura TI y TO y comunicaciones esenciales para la ejecución de la micro-red. Los cambios rápidos entre las operaciones de emergencia predeterminadas pueden permitir una respuesta más rápida y eficaz a los eventos de ciberseguridad. Dentro de la micro-red los objetivos principales son:

- Realizar registro del estado actual de la micro-red.
- Realizar monitoreo de los activos de la micro-red.
- Realizar actividades de gestión en la micro-red.

La condición de los activos es importante dado que se describe a través del monitoreo como se constituye a una micro-red. Comunicar efectivamente el panorama operativo al personal habilitado ayudará a disminuir los riesgos de amenazas que se puedan presentar dentro de

la misma. El dominio CEA toma en cuenta los objetivos descritos; la Tabla 3.8 presenta los atributos relacionados con estos, formando así este dominio.

Tabla 3.8: Atributos necesarios para el dominio CEA

Nivel	Atributos	Puntos
NIM1	El registro de los activos importantes se está produciendo para cada función de la micro-red.	25
	Se realizan actividades de monitoreo de ciberseguridad con revisiones periódicas de registro de datos y comportamientos anómalos.	50
NIM2	Se han definido requisitos de registro para todos los activos importantes.	56
	Los requisitos de monitoreo y análisis que se han definido abordan una revisión oportuna de los datos de cada evento.	61
	Las alarmas y alertas están configuradas para ayudar en la identificación de eventos de ciberseguridad.	66
	Las actividades de monitoreo están alineadas con el perfil de amenazas de las funciones de la micro-red.	70
	Se establecen y mantienen métodos para comunicar el estado actual de ciberseguridad en la micro-red.	75
NIM3	Los requisitos de registro se basan en el riesgo de cada función de la micro-red.	80
	Los datos de registro respaldan otros procesos comerciales y de seguridad.	85
	Se realiza un monitoreo continuo en todo el entorno operativo para identificar actividades anómalas.	90
	Los datos de monitoreo se agregan para proporcionar una comprensión casi en tiempo real del estado de ciberseguridad.	95
	Se recopila información externa a la micro-red para mejorar la imagen operativa común.	100

3.5.6. Atributos del dominio de intercambio de información y comunicaciones

El objetivo de compartir información es fortalecer la ciberseguridad al establecer y mantener una interacción entre las micro-redes. Los objetivos que se deben cumplir para las mismas

son:

- Compartir información de ciberseguridad.
- Realizar actividades de gestión en la micro-red.

El intercambio de información de ciberseguridad comienza con la recopilación de información de ciberseguridad relevante para cada función de la micro-red. El intercambio seguro de diferentes tipos de información relacionada con el riesgo, es esencial para el bienestar de las micro-redes. El dominio IIC toma en cuenta los objetivos descritos; la Tabla 3.9 presenta los atributos relacionados con estos, formando así este dominio.

Tabla 3.9: Atributos necesarios para el dominio IIC

Nivel	**Atributos**	**Puntos**
NIM1	La información se recopila y se proporciona a personas u organizaciones seleccionadas.	35
	La responsabilidad de las obligaciones de informar sobre ciberseguridad se asigna al personal.	50
NIM2	Las partes interesadas que comparten información se identifican en función de su relevancia para la operación continua de las funciones (proveedores, reguladores).	55
	Se identifican fuentes técnicas que pueden ser consultadas en el ámbito de ciberseguridad.	60
	Se establecen y mantienen disposiciones para permitir el intercambio seguro de información confidencial o clasificada.	65
	Se siguen prácticas documentadas para las actividades de intercambio de información.	70
	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas, para apoyar las actividades de intercambio de información.	75
NIM3	La micro-red participa con centros de análisis e intercambio de información.	78
	Los requisitos de intercambio de información se han definido para la difusión oportuna de información de ciberseguridad.	83
	Existen procedimientos para analizar y eliminar conflictos de la información recibida.	87

	Las actividades de intercambio de información están guiadas por políticas documentadas u otras directivas organizacionales.	90
	El personal que realiza actividades de intercambio de información tiene las habilidades y los conocimientos necesarios para desempeñar sus responsabilidades asignadas.	95
	Las políticas de intercambio de información abordan el uso ético de información y el intercambio de la misma, incluida la información confidencial y clasificada.	100

3.5.7. Atributos del dominio de respuesta a incidentes

Dado que se podría afectar significativamente la infraestructura crítica o los activos y servicios de la micro-red que requieren de la organización para prevenir o limitar los impactos adversos es importante tomar en cuenta el dominio de respuesta a incidentes. Los objetivos que deben cumplir dentro de la micro-red son:

- Detectar eventos de ciberseguridad en la micro-red.
- Responder a incidentes y eventos de ciberseguridad en la micro-red.
- Planificar para la continuidad para las actividades de la micro-red.

La detección de eventos de ciberseguridad incluye la designación de un foro para informar eventos y establecer criterios para la priorización de los mismos. Estos criterios deben alinearse con la estrategia de gestión de riesgos de ciberseguridad discutida en el dominio gestión de riesgos para garantizar una valoración coherente de los eventos y proporcionar una estructura para diferenciar los mismos. El dominio RI toma en cuenta los objetivos descritos; la Tabla 3.10 presenta los atributos relacionados que forman este dominio.

Tabla 3.10: Atributos necesarios para el dominio RI

Nivel	**Atributos**	**Puntos**
NIM1	Existe una persona a quien se le puede informar los eventos de ciberseguridad.	30
	Se reportan los eventos de ciberseguridad detectados.	35
	Los eventos de ciberseguridad se registran y rastrean.	40

	Se establecen criterios para el escalamiento de eventos de ciberseguridad, incluidos los criterios de declaración de incidentes	45
	Se identifica el personal de respuesta a incidentes y eventos de seguridad cibernética y se asignan roles.	50
NIM2	Existe un repositorio donde se registran los eventos de ciberseguridad en base a los criterios establecidos.	56
	Los criterios para los eventos de ciberseguridad, incluidos los de incidentes se establecen en función del impacto en la micro-red.	61
	Existe un repositorio donde los eventos y los incidentes de ciberseguridad se rastrean.	66
	Los planes de respuesta a incidentes y eventos de ciberseguridad abordan los activos de TO y TI.	70
	Se capacita a los equipos de respuesta a incidentes y eventos de ciberseguridad.	75
NIM3	Se realizan análisis de la raíz de eventos e incidentes de ciberseguridad y actividades de lecciones aprendidas, se toman como acciones correctivas.	82
	El personal de respuesta a incidentes y eventos de ciberseguridad participa en ejercicios conjuntos con otras organizaciones.	85
	Los planes de respuesta a eventos e incidentes de ciberseguridad se revisan y actualizan con una frecuencia definida por la micro-red.	88
	La política y los procedimientos para informar sobre eventos e incidentes de ciberseguridad a las autoridades designadas cumplen con las leyes y regulaciones.	91
	Los planes de los incidentes son revisados y actualizados periódicamente.	95
	Los activos restaurados se configuran adecuadamente y la información del inventario se actualiza luego de la ejecución de los planes.	100

3.5.8. Atributos del dominio de gestión de dependencias externas

A medida que aumentan las dependencias entre las infraestructuras, los socios operativos, los proveedores de servicios y los clientes, es necesario establecer y mantener una comprensión integral de las relaciones clave. Administrar sus riesgos de ciberseguridad asociados para la

ejecución segura, confiable y resistente. Dentro de la micro-red los objetivos principales son:

- Identificar las dependencias dentro de la micro-red.
- Gestionar el riesgo de la dependencia.
- Realizar actividades de gestión en la micro-red.

La identificación de dependencias implica establecer y mantener una comprensión integral de las relaciones externas claves requeridas para la ejecución de cada función en la micro-red. La gestión del riesgo de dependencia incluye enfoques, como pruebas independientes, revisión de código, exploración de vulnerabilidades y revisión de evidencia del proveedor de que se ha seguido un proceso de desarrollo de *software* seguro. El dominio GDE toma en cuenta los objetivos descritos; además de los atributos relacionados presentados en la Tabla 3.11.

Tabla 3.11: Atributos necesarios para el dominio GDE

Niveles	**Atributos**	**Puntos**
NIM1	Se identifican dependencias importantes de proveedores de TI y TO, es decir, partes externas de las que depende la entrega de una función, incluidos los socios operativos.	34
	Se identifican y abordan los riesgos significativos de ciberseguridad debido a los proveedores y otras dependencias.	42
	Los requisitos de ciberseguridad se consideran al establecer relaciones con proveedores.	50
NIM2	Las dependencias de los proveedores se identifican de acuerdo con los criterios establecidos.	57
	Las dependencias de los clientes se identifican de acuerdo con los criterios establecidos.	59
	Los riesgos de dependencia de ciberseguridad identificados se ingresan en el registro de riesgos.	60
	Los contratos y acuerdos con terceros incorporan el intercambio de información sobre amenazas a la ciberseguridad.	63
	Los acuerdos con proveedores requieren la notificación de incidentes de ciberseguridad relacionados con la entrega del producto o servicio.	66
	Los proveedores y otras entidades externas son revisados periódicamente por su capacidad para cumplir continuamente con los requisitos de ciberseguridad.	69

	Se siguen prácticas documentadas para gestionar el riesgo de dependencia.	72
	Se han identificado estándares y/o directrices para informar sobre la gestión de los riesgos de dependencia.	75
NIM3	La priorización e identificación de dependencias se basan en los criterios de riesgo de la micro-red.	82
	Se establecen requisitos de ciberseguridad para dependencias de proveedores con base en los criterios de riesgo de la micro-red.	85
	Los acuerdos con los proveedores exigen la notificación de los defectos de los productos que provocan vulnerabilidades a lo largo del ciclo de vida de los productos entregados.	88
	Las fuentes de información se monitorean para identificar y evitar amenazas.	91
	La responsabilidad y autoridad para la realización de la gestión del riesgo de dependencia se asigna al personal.	95
	El personal que realiza la gestión del riesgo de dependencia tiene las habilidades y conocimientos necesarios para llevar a cabo las responsabilidades asignadas.	100

3.5.9. Atributos del dominio de Capacitación del personal

A medida que las empresas de servicios públicos adoptan cada vez más tecnología digital avanzada, es un desafío mejorar los conjuntos de habilidades de su fuerza laboral existente y contratar personal con el nivel adecuado de experiencia, educación y capacitación en ciberseguridad. La dependencia de las empresas de servicios públicos de la tecnología avanzada para las comunicaciones y el control digital continúa creciendo y los problemas de la fuerza laboral son un aspecto crucial. Por lo que las micro-redes pueden necesitar implementar prácticas que cumplan con la capacitación del personal. Los objetivos que se deben cumplir para las mismas son:

- Asignar responsabilidades de ciberseguridad en la micro-red.
- Controlar el ciclo de vida laboral en la micro-red.
- Desarrollar seguridad laboral en la micro-red.

- Aumentar conciencia de la importancia de la ciberseguridad.

Un aspecto importante de la asignación de responsabilidades es garantizar la idoneidad, los roles específicos en el ámbito laboral son importantes responsabilidades a menudo fáciles de determinar, pero pueden ser difíciles de mantener. El dominio CP toma en cuenta los objetivos descritos y los atributos relacionados con estos (ver Tabla 3.12), formando así este dominio.

Tabla 3.12: Atributos necesarios para el dominio CP

Niveles	Atributos	Puntos
NIM1	Se identifican las responsabilidades de ciberseguridad para cada función.	31
	Las responsabilidades de ciberseguridad se asignan a personas específicas.	35
	Se realiza una investigación de antecedentes al momento de la contratación del personal para los puestos que tienen acceso a los activos de la micro-red.	40
	La capacitación en ciberseguridad está disponible para el personal con responsabilidades asignadas en la misma.	45
	Se realizan actividades de concientización sobre ciberseguridad.	50
NIM2	Las responsabilidades de ciberseguridad están documentadas.	57
	La investigación de antecedentes del personal se realiza con una frecuencia definida por la micro-red para los puestos que tienen acceso a los activos.	59
	Se identifican las brechas de conocimientos, habilidades y capacidades en ciberseguridad.	60
	Las brechas identificadas se abordan mediante el reclutamiento o la capacitación.	63
	La capacitación en seguridad cibernética se proporciona como un requisito previo para otorgar acceso a los activos.	66
	El contenido de concientización sobre ciberseguridad se basa en el perfil de amenazas de la micro-red.	69
	Se siguen prácticas documentadas para las actividades de gestión laboral de ciberseguridad.	72

	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas, para respaldar las actividades de gestión laboral de ciberseguridad.	75
NIM3	Las responsabilidades de ciberseguridad y los requisitos laborales se revisan y actualizan según corresponda.	82
	Las responsabilidades de ciberseguridad están incluidas en los criterios de evaluación del desempeño laboral.	85
	Las designaciones de riesgo se asignan a todos los puestos que tienen acceso a los activos necesarios para el desempeño de la micro-red.	88
	Se implementa un proceso formal de rendición de cuentas que incluye acciones disciplinarias para el personal que no cumple con las políticas y procedimientos de seguridad establecidos.	91
	Los programas de capacitación están alineados para respaldar los objetivos de gestión laboral de ciberseguridad.	95
	Los programas de capacitación incluyen educación continua y oportunidades de desarrollo profesional para el personal con importantes responsabilidades en ciberseguridad.	100

3.5.10. Atributos del dominio de gestión del programa de ciberseguridad

Un programa de ciberseguridad es un grupo integrado de actividades diseñadas y gestionadas para cumplir con los objetivos de ciberseguridad para la micro-red. Un programa de ciberseguridad puede implementarse a nivel de organización o de función, pero una implementación de nivel superior y un punto de vista empresarial pueden beneficiar a la micro-red al integrar actividades y aprovechar las inversiones de recursos en toda la empresa. Sus objetivos son:

- Establecer la estrategia del programa de ciberseguridad en la micro-red.
- Establecer y mantener la arquitectura de ciberseguridad en la micro-red.
- Desarrollo de *software* seguro para la micro-red.
- Realizar actividades de gestión en la micro-red.

La estrategia del programa debe incluir una lista de objetivos de seguridad cibernética y un plan para cumplirlos. En niveles más altos de madurez, la estrategia del programa será más completa e incluirá prioridad, estructura y organización para el programa. El dominio GPC

toma en cuenta los objetivos descritos; y además, los atributos relacionados con estos (ver Tabla 3.13), formando así este dominio.

Tabla 3.13: Atributos necesarios para el dominio GPC

Nivel	Atributos	Puntos
NIM1	Existe una estrategia de programa de ciberseguridad.	25
	Se proporcionan recursos como: personas, herramientas y financiamiento para apoyar el programa de ciberseguridad.	40
	Se implementa una estrategia para aislar la arquitectura de los sistemas TI de los TO.	50
NIM2	El programa de ciberseguridad define los objetivos para las actividades de la micro-red.	55
	La estrategia y las prioridades del programa de ciberseguridad están documentadas y alineadas con los objetivos estratégicos de la micro-red y el riesgo para la infraestructura crítica.	57
	La estrategia del programa de ciberseguridad identifica estándares y lineamientos que se pretende que siga el programa.	62
	La estrategia del programa de ciberseguridad identifica cualquier requisito de cumplimiento aplicable que debe cumplir el programa (NIST, ISO, CMMC, etc).	65
	Se proporcionan los recursos adecuados: personas, financiamiento y herramientas, para operar un programa de ciberseguridad alineado con la estrategia del programa.	68
	Si la organización desarrolla o adquiere software, se imparten prácticas seguras de desarrollo de software como un elemento del programa de seguridad cibernética.	71
	El software que se implementará en los activos se desarrolla utilizando prácticas seguras de desarrollo de software.	75
NIM3	La estrategia del programa de ciberseguridad se actualiza según los cambios en el entorno operativo y los cambios de amenazas.	80
	Las actividades del programa de ciberseguridad se revisan periódicamente para garantizar que se alineen con la estrategia del programa de ciberseguridad.	83

	El programa de ciberseguridad aborda y permite lograr el cumplimiento normativo.	87
	La micro-red colabora con entidades externas para contribuir al desarrollo e implementación de estándares, pautas, prácticas y tecnologías emergentes de ciberseguridad.	91
	El personal que realiza actividades en este dominio tiene las habilidades y el conocimiento necesarios para realizar sus responsabilidades asignadas.	96
	La efectividad de las actividades en este dominio es evaluada y rastreada.	100

3.6. Aplicación para la evaluación periódica de una micro-red

La aplicación creada para la evaluación periódica de ciberseguridad de una micro-red se basa en el modelo mencionado en este capítulo. Esta aplicación consta de dos partes, la primera parte presenta un cuestionario que evaluará el nivel de madurez, y la segunda parte consta de una serie de *dashboards* e indicadores de cumplimiento de dominios y niveles por parte de la micro-red.

Para la aplicación se ha utilizado *Django* que es un *framework* web escrito en *Python*, se ha implementado de esta manera la aplicación dado que facilita la creación de una página web, es gratuito y de código abierto.

El diagrama de flujo de estos procesos y cómo están relacionados se muestra en la Figura 3.2, la cual describe el funcionamiento de toda la aplicación creada. Las indicaciones para el uso de la aplicación, tanto como para la evaluación y visualización de resultados, se describen en B.

El puntaje final que emite la aplicación está relacionado con la Tabla 3.14, en donde se muestra el nivel de madurez correspondiente al valor total alcanzado sumando el puntaje que obtiene la micro-red evaluada de cada dominio; este valor está relacionado con un color dependiendo el nivel en el que se encuentre, similar al de la Tabla 3.2.

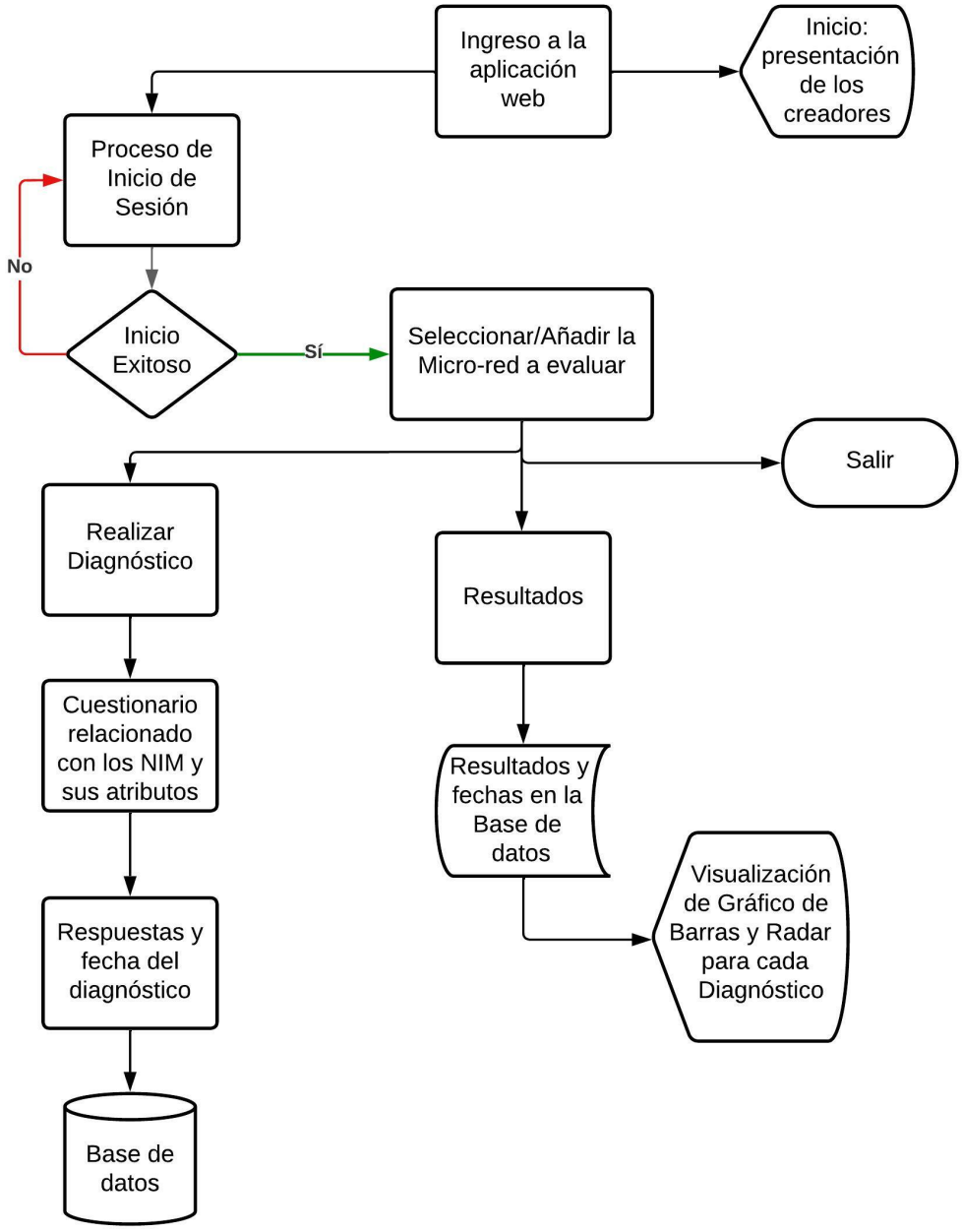

Figura 3.2: Diagrama de la aplicación web creada para la evaluación periódica de una micro-red

Tabla 3.14: Puntaje Total del Nivel de Madurez

Nivel	Nombre	Color	Puntos
NIM0	No Existente		[0-240]
NIM1	Inicial		[250-500]
NIM2	Satisfactorio		[510-750]
NIM3	Optimizado		[760-1000]

4. Medición de la madurez de la micro-red de la Universidad de Cuenca

En este capítulo se presenta la evaluación de ciberseguridad a la micro-red de la Universidad de Cuenca. En la Sección 4.1 se describe la arquitectura de la misma junto con los activos que posee. Los resultados de la evaluación realizada a dicha infraestructura se detallan en la Sección 4.2, mientras que las recomendaciones para mejorar el nivel de madurez se presentan en la Sección 4.3.

Profundizando el caso de estudio, en la sección 4.4 se presenta las vulnerabilidades, riesgos y amenazas de la micro-red. La sección 4.5 describe los mecanismo de protección necesarios para el sistema de seguridad, mientras que en la sección 4.6 se menciona los cumplimientos que debe cumplir una micro-red real (como la micro-red de la Universidad de Cuenca tiene un enfoque didáctico educativo). La sección 4.7 trata de la importancia del criterio de energía entregada y los servicios que dependen de la micro-red de la Universidad de Cuenca para hallar su criticidad.

4.1. Arquitectura de la micro-red de la Universidad de Cuenca

Para realizar el análisis de la madurez de la ciberseguridad dentro de la micro-red de la Universidad de Cuenca, es necesario conocer su topología e infraestructura. Por lo que, en esta sección se detallará la misma; esto sirve para conocer los activos de la micro-red y cuáles son las TI y TO utilizadas en la misma. El esquema de la infraestructura de la micro-red se observa en la Figura 4.1. La micro-red está conformada por los siguientes dispositivos:

- Servidor.
- PLC.
- RTU.
- Switch.
- Inversor.
- Batería.
- Sistema de gestión de batería (BMS).
- Analizador de red.

- Banco de condensadores.
- Pila de combustible.
- Electrolizador.
- Rectificador.
- Carga CA.

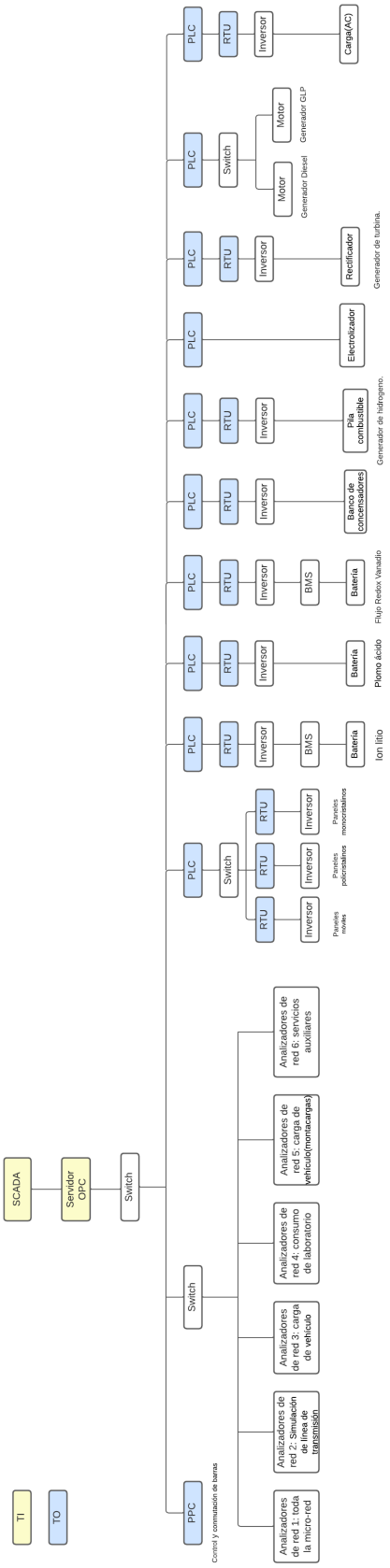

Figura 4.1: Topología de la micro-red

La clasificación de activos tiene como propósito, garantizar que se establecen las capas de protección adecuadas y que por sus características necesitan un tratamiento especial. El sistema, donde se clasifica la información de los activos que podría precisar la entidad, está basado en las características propias de la información; tiene en cuenta el funcionamiento interno de la entidad, siempre procurando dar cumplimiento a los lineamientos y requisitos estipulados en el ítem relacionado con la gestión de activos de los estándares ISO 27001:2013, ISO 27002, e ISO 27005.

Una organización puede establecer más niveles de clasificación a medida que la misma sea de mayor tamaño y presente una mayor complejidad. Para esta metodología se clasificarán los activos de información según su *nombre, modelo, tipo de activo, software, firmware y fecha de adquisición*.

Para emplear el análisis de la micro-red es necesario reconocer los activos de la misma; estos son detallados en la Tabla 4.1. Las imágenes respectivas de estos activos se presentan en el Apéndice C.

Tabla 4.1: Activos TO de la micro-red

Nombre	**Modelo**	**Número**	**Tipo**	**Software**	**Firmware**	**Fecha de Adquisición**
SCADA	s/m	1	TI	Windows 7	s/f	20/10/16
Servidor OPC	SIMATIC S7-1500	1	TI	STEP 7	V 3.0.1	20/10/16
PLC	Schneider M251	8	TO	SoMachine	SoMachine	20//10/16
RTU	Schneider TM3DQ8R	6	TO	SoMachine	V28	20/10/16

4.2. Diagnóstico del nivel de madurez de la micro-red de la Universidad de Cuenca

Para evaluar a la micro-red de la Universidad de Cuenca, se solicitó al encargado de la misma que llene la información necesaria mediante la aplicación anteriormente descrita. Los resultados de la evaluación se presentan en la Tabla 4.2 y la Figura 4.2.

La micro-red alcanzó un total de **178 puntos** en la evaluación realizada, lo que implica que

Tabla 4.2: Puntaje alcanzado en cada dominio de la micro-red.

Dominio	**Puntaje**
Gestión de riesgos	50
Gestión de identidad y acceso	25
Gestión de amenazas y vulnerabilidades	0
Gestión de identidad y acceso	0
Conciencia del estado actual	0
Intercambio de información y comunicaciones	35
Repuesta a incidentes	34
Gestión de dependencias externas	34
Capacitación del Personal	0
Gestión del programa de ciberseguridad	0
Total	**178**

Figura 4.2: Gráfico radar de la evaluación de la micro-red, resultado por cada dominio.

se encuentra en un **NIM0 No Existente**. Los resultados muestran que cinco de los diez dominios se encuentran en un puntaje de cero, es decir que no tienen implementación alguna de atributos ni prácticas. Con los resultados obtenidos, en la Sección 4.3 se presentan las recomendaciones para aumentar el nivel de madurez de ciberseguridad.

4.3. Recomendaciones para aumentar el nivel de madurez de la micro-red de la Universidad de Cuenca

Es importante tomar en cuenta las recomendaciones para aumentar el nivel de madurez de la micro-red, dado que su ciberseguridad en general es no existente. Lo principal es llegar al NIM1 dado que debe existir una progresión uniforme en todos los dominios dentro de la micro-red. A continuación se describen las recomendaciones a aplicarse en los dominios para que estos lleguen al nivel previamente mencionado. En esta sección, cada recomendación está basada en los controles.

4.3.1. Gestión de activos

En este dominio se puede dar un seguimiento a los activos TI y TO mediante el uso de un *software* libre para gestión de activos de TI llamado *Snipe-IT* (https://github.com/snipe/snipe-it) que permite gestionar y hacer seguimiento a todos los activos, establece funciones sencillas de automatización en su herramienta de gestión de activos de Tecnología de la Información por Internet. La otra opción es usar la misma herramienta que utiliza la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la universidad. Esto es usar el plugin en *fusion inventory* (https://fusioninventory.org/) sobre el *glpi* (https://glpi-project.org/). Por último, se propone *NetBox* (https://github.com/netbox-community/netbox), esta herramienta es de código abierto y permite la gestión de la infraestructura de la red como los activos, direcciones IP y documentación de la misma.

Una vez establecido el inventario de los activos, se tiene que evaluar y aprobar cualquier cambio dentro de la micro-red antes de implementarse (puede ser incorporar o eliminar cualquier activo), por lo que se recomienda que el encargado de la micro-red analice los cambios antes de realizarlos tal como lo menciona el control 8.1.3. En cuanto a la línea base de configuración de los activos, se recomienda que la micro-red tenga una asesoría con los proveedores de los equipos de tal manera que el personal de la misma tenga conocimiento de como se encuentran configurados los equipos.

4.3.2. Gestión de identidad de acceso

En este dominio, tal como [67] describe, se recomienda proporcionar identidades para el personal que esté capacitado y que requiera acceso así como se menciona en el control 9.1.2 en

la ISO 27002; en este caso para el cuarto de control en donde se encuentra el SCADA. Una vez que una persona no necesite más el acceso se debe dar de baja dicha identidad según lo indicado en el control 9.2.1 del mismo estándar. Para esto se deberá realizar la instalación de un sistema de control de acceso, ya que el cuarto no cuenta con ninguno, tal como una cerradura magnética con activación mediante tarjeta RFID.

Dado que la micro-red tiene un enfoque educativo y de investigación se tiene que gestionar el acceso a los equipos o activos mediante un listado de personas que han tenido acceso a los mismos, en donde se detalla: nombre, número de cédula de la persona que utilizó el equipo, equipo utilizado, descripción del uso del equipo y la firma.

4.3.3. Gestión amenazas y vulnerabilidades

En este dominio se recomienda identificar las fuentes de amenazas dentro de la micro-red como lo menciona el control 14.1.1. Se puede realizar un *pentesting*, con la finalidad de conocer las amenazas a las que podría estar expuesta la micro-red. Una vez que se han identificado las vulnerabilidades que se consideran importantes para el funcionamiento de la micro-red deben ser tratadas por especialistas en ciberseguridad.

La micro-red tiene un enfoque educativo e investigativo, por lo que la identificación de vulnerabilidades podría ser realizada por los estudiantes como proyecto de grado. La respuesta a estas vulnerabilidades también podría ser objeto de estudio por parte de docentes y estudiantes.

Según [68], una vez identificadas las amenazas, es necesario priorizarlas y establecer un perfil de amenazas, por ejemplo: objetivo, capacidad o impacto. A esta información se la puede dar seguimiento usando el software https://glpi-project.org/.

4.3.4. Conciencia del estado actual

En este dominio se recomienda llevar un registro de los activos de la micro-red en donde se detallen los procesos que se han realizado en los mismos según lo mencionado en el control 8.1.1; este control puede ser llevado a cabo usando https://glpi-project.org/. Teniendo así definido los activos y elementos que se usan para los diversos procesos (generación con paneles, control de baterías) que desempeña la micro-red. Se debe realizar actividades de monitoreo de ciberseguridad con revisiones en tiempos establecidos por la micro-red.

4.3.5. Intercambio de información y comunicaciones

Dado que la micro-red cuenta con diferentes instituciones que brindan soporte a los equipos, es necesario recopilar información y proporcionarla a las organizaciones con las cuales la micro-red tiene vínculo como se lo menciona en los controles 6.1.3 y 6.1.4. Según lo recomendado en [69], se debe asignar personal calificado para informarle sobre la ciberseguridad, para que en caso de existir alguna anomalía que implique riesgos, se tenga una persona encargada para receptar esta información según el control 16.1.1 del mismo estándar.

4.3.6. Respuesta a incidentes

Una vez que los eventos de ciberseguridad son detectados, se recomienda registrar y rastrear dichos eventos según lo indicado en el control 16.1.2. De tal manera que la micro-red cuente con un inventario de los mismos. A los eventos de ciberseguridad se les debe asignar un peso de importancia, para tener en cuenta el orden de priorización de los mismos. Se recomienda también identificar el personal que dé respuesta a dichos incidentes. Es importante seguir un proceso de respuesta a incidentes como los que se muestran en:

`https://learn.microsoft.com/es-es/security/compass/incident-response-process`

`https://www.atlassian.com/es/incident-management/incident-response`

`https://cloud.google.com/docs/security/incident-response?hl=es-419`

Tal como se menciona el control 6.1.1 del mismo estándar se debe asignar roles y responsabilidades para la seguridad de la información.

4.3.7. Gestión de dependencias externas

Dado que existe la identificación de dependencias por parte de los proveedores, se debe también identificar los riesgos de ciberseguridad que se dan debido a los mismos según el control 8.1.3. En este caso se puede solicitar una capacitación en donde se exponga las vulnerabilidades a las que se encuentran expuestas los equipos. Esto ayuda a establecer con los proveedores los requisitos de ciberseguridad necesarios. Estas dependencias están relacionadas con la parte de mantenimiento y actualización de *software*, además de la configuración de los equipos. Estas recomendaciones se basan en lo mencionado en [26].

4.3.8. Capacitación del personal

En este dominio se recomienda identificar las responsabilidades de ciberseguridad para cada función de la micro-red tal como se menciona en el control 6.1.1. Las mismas tienen que asignarse a personas específicas con capacidades para realizarlas según se describe en el control 6.1.2 del mismo estándar.

Antes de realizar el contrato del personal se recomienda que la micro-red analice los antecedentes de los mismos, en especial para puestos que requieren ingreso al centro de control del SCADA. El personal que ingrese debe realizar capacitación de ciberseguridad realizando cursos gratuitos disponibles en https://ciberseguridadenlinea.com/; además, todo el personal que tiene acceso a la micro-red tiene que realizar actividades de concienciación para esto es importante mantener contactos con grupos especilizados en ciberseguridad como lo menciona el control 6.1.4; de esta manera podrán informar a los estudiantes sobre la importancia de la ciberseguridad.

4.3.9. Gestión del programa de ciberseguridad

Como primer punto se recomienda realizar una estrategia para un programa de ciberseguridad, el cuál debe ir guiado por profesionales en este ámbito. Lo que se busca con esta estrategia es proporcionar el personal y las herramientas adecuadas para apoyar al programa. Es importante considerar una estrategia para aislar la arquitectura de los sistemas TI de los TO tal como lo menciona el control 12.1.4, dado que se debe analizar dicha arquitectura al momento de realizar un programa que se encuentre bien estructurado.

La implementación del programa se lo podría realizar de manera sencilla en https://fusioninventory.org/ ya que ayuda a inventariar los activos TI y desarrollar software de manera sencilla de acuerdo a las necesidades de la micro-red.

4.4. Determinación de vulnerabilidades, amenazas y riesgos

4.4.1. Pentesting

El *pentesting* realizado a la micro-red de la Universidad de Cuenca se desarrolló con herramientas de escaneo de red, tales como *Nmap* (usado en una máquina virtual *Kali Linux*) y *Nexpose*. Estas herramientas son usadas para el descubrimiento de hosts, puertos, servicios,

direcciones MAC, sistemas operativos, además de detectar vulnerabilidades existentes en la red (en el caso de *Nexpose*) [70–73].

El uso de estas herramientas se describe en el Apéndice D junto con la descripción de los 38 activos de la micro-red de la Universidad de Cuenca a los que se les realizó el *pentesting*.

Los resultados del *pentesting* mostraron los puertos a los que un atacante podría acceder, y con esto atacar los servicios que estos puertos ofrecen. La Figura 4.3 presenta los servicios más comunes y el número de activos en los que está presente cada servicio.

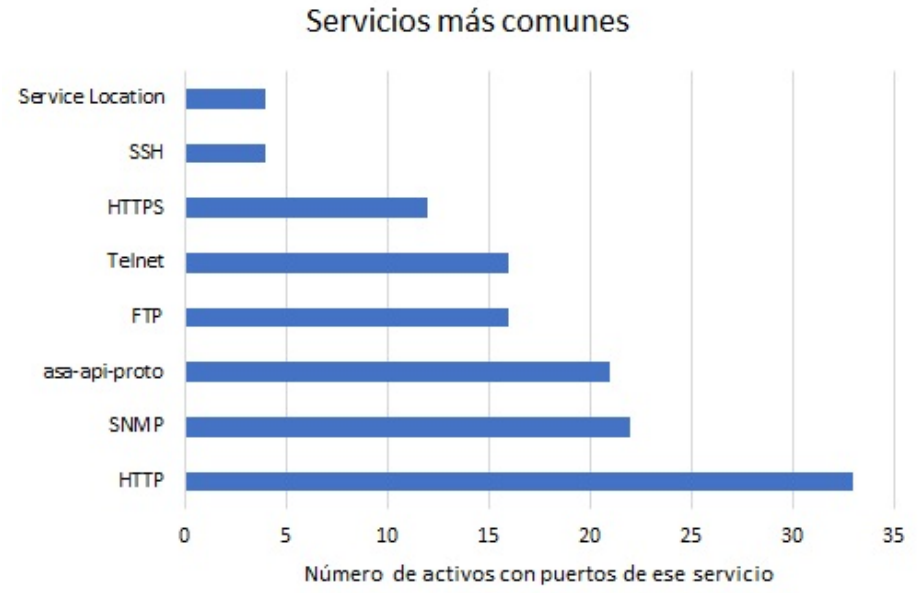

Figura 4.3: Servicios que corren en los puertos de los activos de la micro-red

A estos servicios encontrados, se les encuentra vulnerabilidades que se clasifican en tres tipos:

Crítica: Fáciles de explotar para los atacantes y pueden proporcionarles un control total de los sistemas afectados.

Severa: Son más difíciles de explotar y no brinden el mismo acceso a los sistemas afectados.

Moderada: Brindan información a los atacantes que pueden ayudarlos a montar ataques posteriores en su red

El total de vulnerabilidades encontradas en los activos de la micro-red de la Universidad de Cuenca es de 417. El número de cada una de estas se muestra en la Figura 4.4, mientras que el número de activos con cada tipo de vulnerabilidad se representa en la Figura 4.5. Los resultados muestran que más de la mitad de los activos tiene vulnerabilidades críticas y que

ningún activo presenta cero vulnerabilidades.

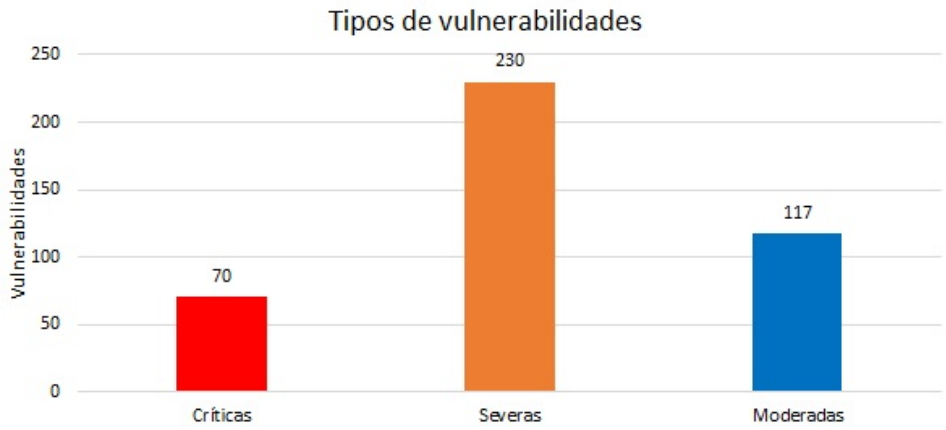

Figura 4.4: Tipos de vulnerabilidades en la micro-red

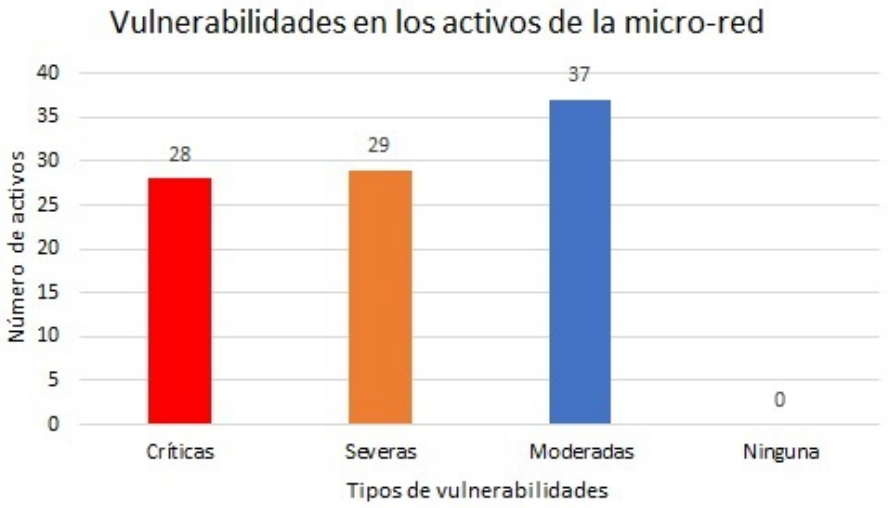

Figura 4.5: Número y tipo de vulnerabilidades en los activos de la micro-red

Todos los servicios presentan vulnerabilidades; los servicios que presentan más vulnerabilidades son mostrados en la Figura 4.6. Las vulnerabilidades más comunes son las que se muestran en la Figura 4.7; estas están relacionadas con cifrados y contraseñas de autenticación débiles, versiones de protocolos antiguas o que admiten ciertos ataques y problemas de cómo se transmite la información, cada una de estas representa un riesgo al sistema.

4.4.2. Riesgos del sistema y probabilidad de ocurrencia

Como se menciona en 2.7 en la norma ISO 31000 existen diferentes niveles de riesgos. En este caso nos enfocaremos en los riesgos tecnológicos, operacionales y de procesos dado que en ellos se abarca la ciberseguridad, eficacia y eficiencia de la organización.

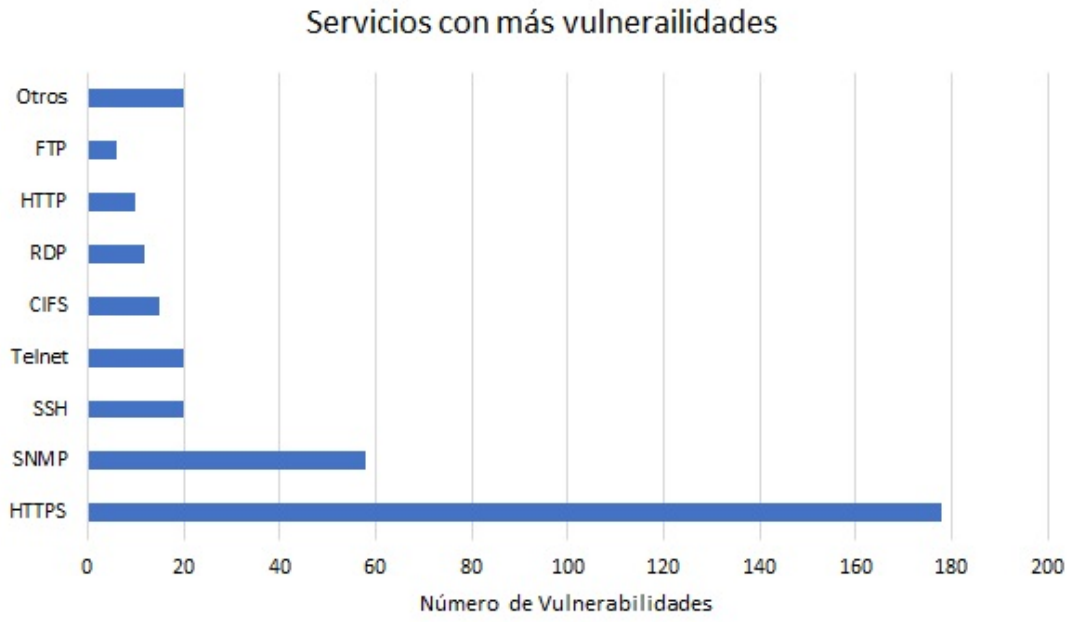

Figura 4.6: Número de vulnerabilidades por servicio en la micro-red

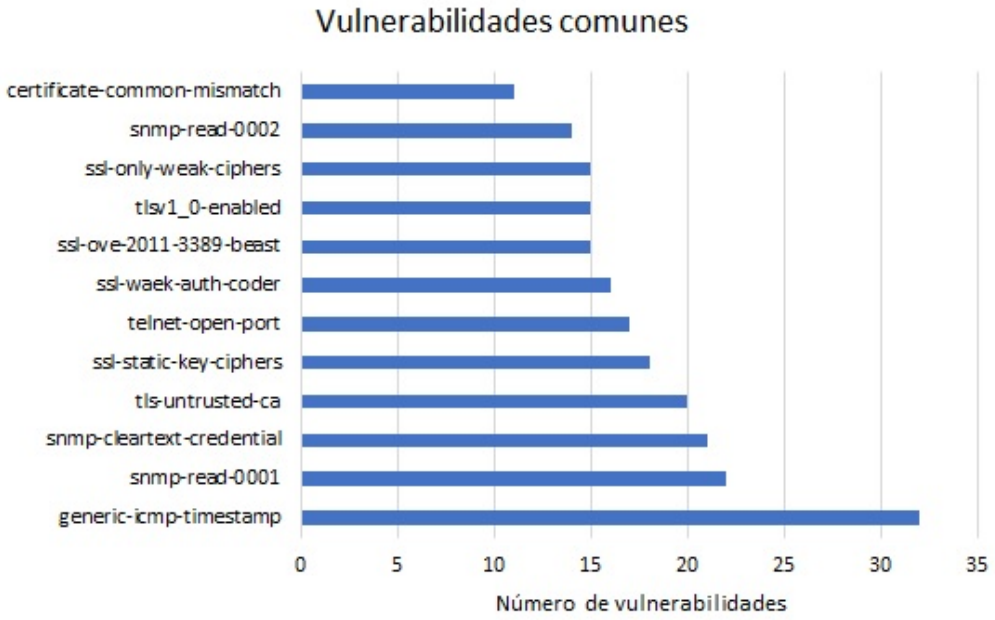

Figura 4.7: Vulnerabilidades más comunes en la micro-red

Para determinar los riesgos del sistema se usa la probabilidad de ocurrencia de las vulnerabilidades encontradas, basándose en el número de vulnerabilidades de cada tipo y el número total de vulnerabilidades. En la Figura 4.8 se presentan las vulnerabilidades con mayor probabilidad. A todas estas vulnerabilidades se les asigna un peso dependiendo de la clasificación de la vulnerabilidad (crítica, severa o moderada), los pesos asignados son los siguientes: crítica (3), severa (2) y moderada (1).

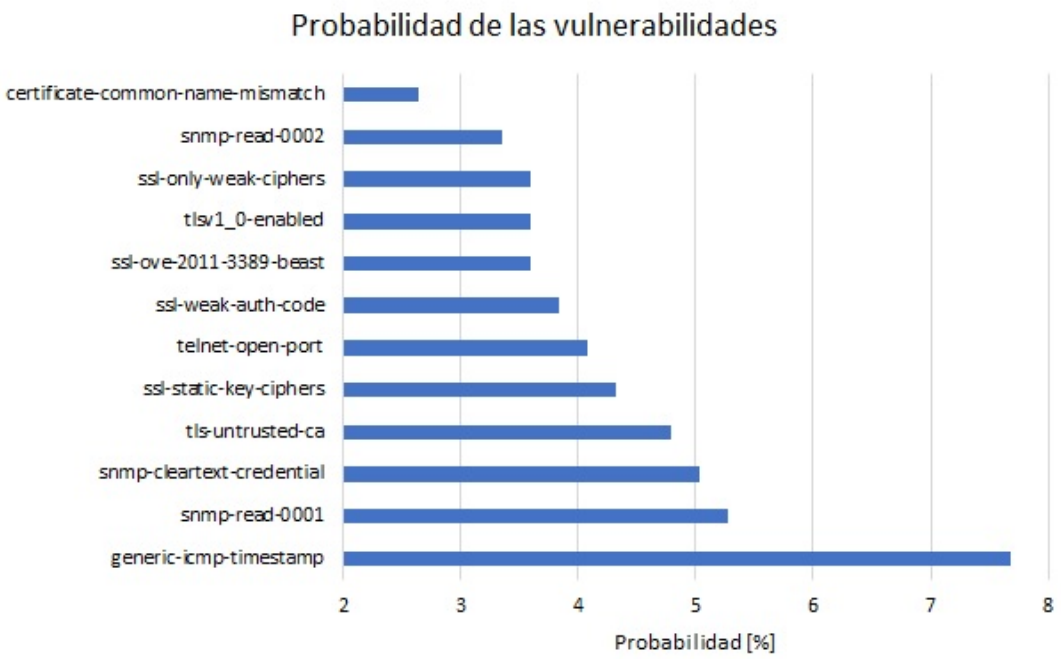

Figura 4.8: Probabilidades de las vulnerabilidades más comunes

A partir de que tan recurrente es la vulnerabilidad y el peso de la misma, se procede a calcular el valor de riesgo que tiene cada vulnerabilidad, obteniendo así los datos de la Figura 4.9, la cual muestra las vulnerabilidades con mayor riesgo en la micro-red.

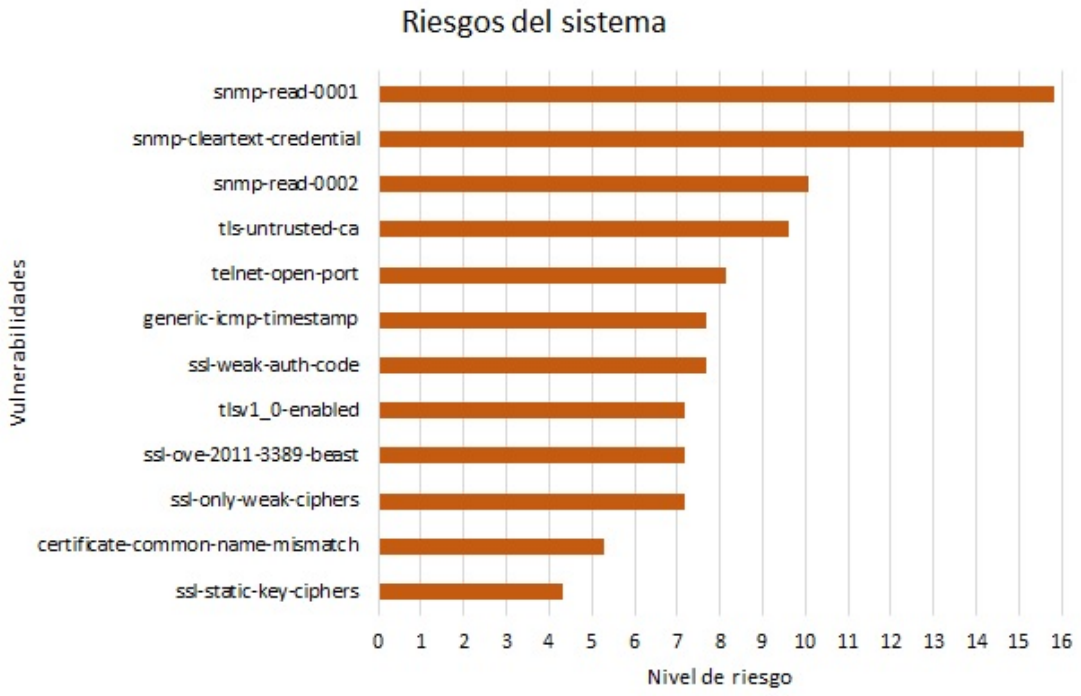

Figura 4.9: Riesgos del sistema en base a las vulnerabilidades

Las vulnerabilidades con mayor riesgos están relacionadas con el protocolo Simple Network Management Protocol (SNMP), el cual proporciona un marco estandarizado para un lenguaje común que se usa para monitorear y administrar dispositivos en una red. Esta vulnerabilidad podría permitir que un tercero no autorizado obtenga acceso a un dispositivo de red y a la información de la misma como claves y credenciales de autenticación; los atacantes pueden incluso reconfigurar o apagar dispositivos de forma remota.

El protocolo Transport Layer Security (TLS) presenta más vulnerabilidades con un alto riesgo, esta vulnerabilidad es de capa de transporte, puede permitir que un atacante use un certificado de autoridad de certificación (CA) no confiable para interceptar y manipular el tráfico de red. Además, algunos activos usan la versión antigua de este protocolo la cual es vulnerable a interceptar tráfico y a inyección de datos.

Existe riesgo con el Telnet, ya que un servidor tiene este puerto abierto y permite a un usuario remoto y toda la información enviada va sin cifrado.

La vulnerabilidad más común se relaciona con el protocolo Internet Control Message Protocol (ICMP), la respuesta del *timestamp* no tiene control y permite que un atacante inunde a un host con mensajes de solicitud ocasionando una sobrecarga que puede provocar una disminución en el rendimiento del host o incluso una denegación de servicio. También se puede aproximar el tiempo de actividad del host, lo que sería útil para futuros ataques.

El protocolo Secure Sockets Layer (SSL) se relaciona con algunas vulnerabilidades de alto riesgo. Las versiones usadas dentro de la micro-red cuentan con mecanismos de cifrado estático y algoritmos de autenticación poco robustos. Esto permitiría a un atacante interceptar y descifrar la información, además de obtener acceso no autorizado amenazando a la integridad y confidencialidad de la comunicación.

Por último, se tiene a la vulnerabilidad de certificados digitales en la comunicación SSL/TLS; esto debido a que no se hace una validación de los certificados permitiendo el robo de información.

4.4.3. Amenazas al sistema y su mitigación

Una amenaza es la posibilidad de que un sistema vulnerable sea atacado y sufra daños, en un sistema informático provienen principalmente de ataques externos (malware, denegación de servicio o inyecciones SQL, entre otros). Se observa en la Tabla 4.3 las amenazas encontradas en la micro-red de la Universidad de Cuenca y su mitigación.

Tabla 4.3: Amenazas y su mitigación

Riesgo	Amenaza	Mitigación
TLS timestamp	Denegación de servicio	Se recomienda deshabilitar el envío de respuestas de timestamp en los sistemas que no lo necesitan. Limitar la cantidad de solicitudes que se pueden enviar.
SNMP-READ-0001 y SNMP-READ-0002	Denegación de servicio y problemas de confidencialidad	Es importante mantener todas las implementaciones de SNMP actualizadas y aplicar los parches de seguridad necesarios para corregir la vulnerabilidad. Limitar el acceso a los dispositivos y sistemas de red a través de SNMP. Implementar la autenticación SNMP versión 3.
SNMP-Cleartext-Credentials	Autenticación débil	Se recomienda que los administradores de red eviten enviar credenciales de autenticación en texto plano a través de la red y en su lugar utilicen protocolos de seguridad más fuertes, como SNMP versión 3.
TLS-Untrusted-CA	Problemas de confidencialidad, phishing y malware	Utilizar certificados emitidos por CA confiables y realizar una verificación adecuada de la certificación. Mantener actualizadas las implementaciones de TLS.
SSL-Static-Key-Ciphers	Problemas de confidencialidad	Se recomienda utilizar siempre cifrados SSL/TLS con claves dinámicas y aleatorias en lugar de cifrados estáticos de clave. También es importante mantener actualizadas las implementaciones de SSL/TLS y otros protocolos de seguridad de red.

Telnet-Open-Port	Problemas de confidencialidad	Utilizar protocolos de comunicación seguros, como SSH, en lugar de Telnet, ya que SSH cifra todas las comunicaciones entre el cliente y el servidor. Limitar el acceso al servidor a usuarios autorizados solamente.
SSL-Weak-Message-Authentication-Code-Algorithms	Problemas de confidencialidad	Asegurarse de que los algoritmos de autenticación utilizados en SSL/TLS sean lo suficientemente fuertes y estén actualizados. También es importante mantener los sistemas y aplicaciones actualizados con las últimas correcciones de seguridad y configurar los servidores SSL/TLS.
SSL-CVE-2011-3389-Beast	Problemas de confidencialidad	Aplicar los parches de seguridad para los navegadores y servidores web que contienen las correcciones para esta vulnerabilidad. También se recomienda utilizar versiones más recientes del protocolo TLS. Usar TLSv1.2 con la configuración Authenticated Encryption with Associated Data (AEAD).
TLSV1-0-Enabled	Problemas de confidencialidad	Usar TLSv1.2 con la configuración AEAD
SSL-Only-Weak-Ciphers	Problemas de confidencialidad	Configurar los servidores web para que permitan el uso de algoritmos fuertes y seguros.

Certificate-Common-Name-Mismatch	Problemas de confidencialidad	Los sitios web deben asegurarse de que los certificados digitales que presentan en la comunicación SSL/TLS coincidan con el nombre de dominio que se está utilizando en la conexión. Esto se puede hacer a través de la emisión y validación adecuada del certificado digital y la configuración adecuada del servidor web.

4.5. Mecanismos de protección de seguridad

El diagnóstico realizado en la micro-red de la Universidad de Cuenca revela los siguientes detalles en los tópicos explicados en la sección 2.4.

Confidencialidad: No existe separación de las redes (TI, TO y red de la universidad son una sola red), no se usa ningún tipo de cortafuegos ni analizador de tráfico, no hay sistemas de autenticación.

Integridad: No existe mecanismos contra amenazas. Las vulnerabilidades no son tratadas ni analizadas, no hay métodos que aseguren la integridad de los datos.

Autenticidad: No existe ningún control de acceso a los activos. No hay políticas de gestión de identidad y acceso al sistema SCADA.

Disponibilidad: No existe mecanismos de control que eviten la pérdida de un proceso o de algún servicio, no se garantiza que los activos estén disponibles en todo momento.

Verificabilidad: No existe sistemas de verificación de sistemas en cuanto a funcionalidad, seguridad y acceso.

Acatando la recomendación de este trabajo, enfocada a dividir la red TI y la red TO de la micro-red evaluada; se da mecanismos de protección y un sistema de seguridad para cada una de las redes.

4.5.1. Recomendación de los mecanismos de protección y sistema de seguridad para la red

Para una red, según [74] y [75] los mecanismos de protección que pueden implementarse son los siguientes:

Confidencialidad: Establecer esquemas de autenticación fuerte y autorización granular para controlar el acceso de usuarios y dispositivos a los sistemas. La capacitación al personal, garantiza que tanto operarios como administradores de sistemas estén familiarizados con los sistemas y puedan detectar posibles fallos y vulnerabilidades en ellos. También se debe tomar en cuenta la encriptación de los datos, separación de redes, uso de cortafuegos y analizadores de tráfico de red.

Integridad: Protección de los equipos y sistemas de dispositivos físicos mediante sistemas de monitoreo y alarmas. Restringir el acceso a los sistemas y dispositivos a usuarios autorizados mediante la autenticación y autorización de usuarios y sistemas. Utilización de sistemas de detección de intrusiones que identifican actividades maliciosas y las detienen antes de que causen daño. Mantener actualizado el software y firmware de los sistemas y dispositivos para protegerlos de vulnerabilidades conocidas.

Disponibilidad: Implementación de sistemas redundantes y de *backup*, monitorización y alerta de fallos. Limitar la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la micro-red. Establecer un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones. Ingreso a las personas que cuenten con las credenciales requeridas para acceder a información y operación de los sistemas.

Autenticidad: Para evitar accesos no autorizados, se deben implementar medidas de seguridad avanzadas, como autenticación de usuario y contraseña. Para proteger la autenticidad, es crucial contar con software de seguridad actualizado. Es necesario asegurarse de que todos los programas instalados en los sistemas de tecnología operacional se actualicen con regularidad y se realice un seguimiento meticuloso de los parches de seguridad. Es importante utilizar protocolos de encriptación para proteger la autenticidad de los datos que se transmiten entre los sistemas de tecnología operacional. Un *firewall* es una herramienta de seguridad fundamental para los sistemas.

Verificabilidad: La certificación de los sistemas y equipos, así como las auditorías periódicas, garantizan la conformidad de los mismos con los estándares y normativas aplicables, y

aseguran que el sistema funciona según lo previsto. Contar con políticas de seguridad claras y bien definidas permite a los usuarios conocer las expectativas de la organización en cuanto a la protección de la información y los sistemas. La protección de los equipos y sistemas mediante sistemas de protección física como cámaras de seguridad, cerraduras, garantiza la integridad y protección de los sistemas.

Es importante mencionar que el orden de importancia para TI es: confidencialidad, integridad, disponibilidad, autenticidad y verificabilidad. Mientras que para TO es: disponibilidad, integridad, confidencialidad, autenticidad y verificabilidad. Esto debido a que para los sistemas de operaciones lo más importante es mantener el proceso industrial en funcionamiento. La carencia de disponibilidad podría derivar en una pérdida de control sobre el proceso o que se detuvieran las operaciones, con los consiguientes riesgos que ello implicaría tanto para la seguridad del sistema como para la seguridad física de las personas o los efectos en el medio ambiente. Se ha realizado un esbozo del sistema de seguridad que se tiene que tomar en cuenta para los activos TI y TO de la micro-red de la Universidad de Cuenca, tomando en cuenta los mecanismos anteriormente descritos, en la Figura 4.10.

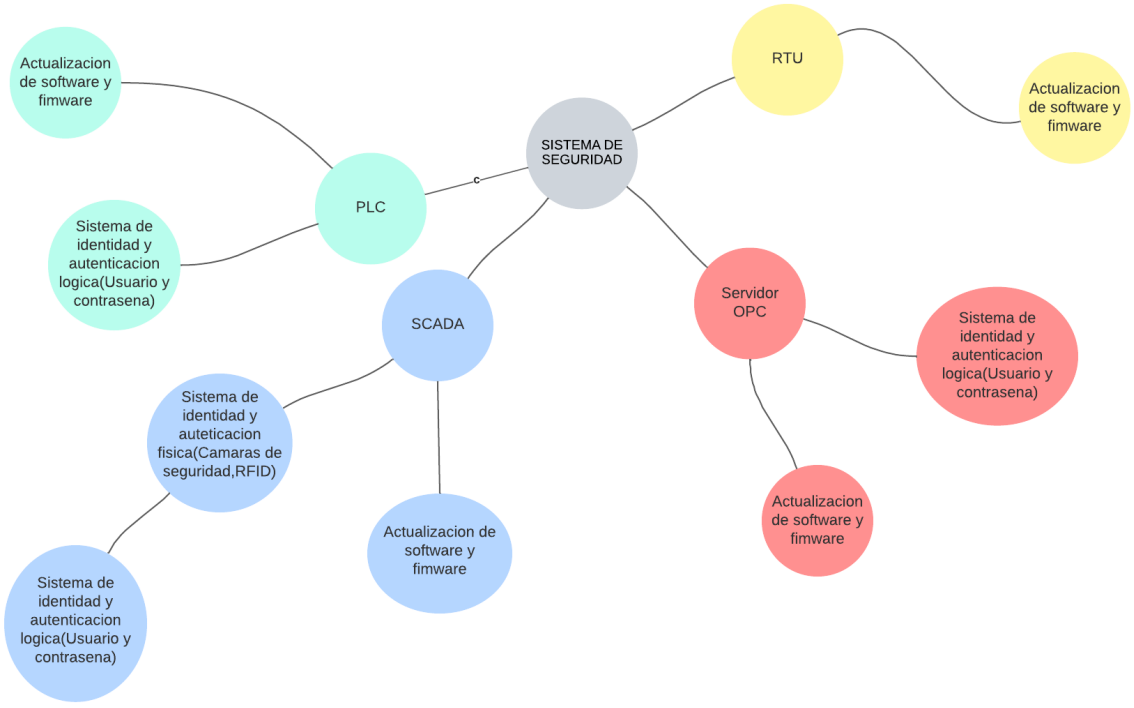

Figura 4.10: Sistema de seguridad para los activos de la micro-red de la Universidad de Cuenca

4.6. Cumplimientos necesarios de una micro-red en temas de ciberseguridad

En una micro-red se deben cumplir con los atributos mencionados en este modelo de ciberseguridad creado, sin embargo, es necesario el cumplimiento de otros temas de gran importancia por parte de una micro-red que no sea de enfoque académico.

Mecanismos: Para garantizar la protección de los datos, información y dispositivos eléctricos, se tienen algunos mecanismos que debe cumplir una micro-red según lo mencionado en [27, 44, 76].

Autenticación: Solo los usuarios autorizados deben acceder al sistema.

Para los puntos de red, los cuales se encuentren en las oficinas de los encargados de la micro-red, se deberá realizar una verificación de usuario cada vez que el equipo se conecte a la red. Estos usuarios tienen acceso a los otros dispositivos de la red. Para esto es necesario la implementación del servidor de autenticación *Radius*.

Encriptación: La comunicación entre los distintos dispositivos de la micro-red y los datos que se transfieren entre estos deben estar encriptados para proteger la información en caso de un acceso no autorizado.

Los PLCs usados en la micro-red permiten el uso del protocolo SSL/TLS. El uso de estos protocolos permite la encriptación en la comunicación.

Control de acceso: Además de los datos, se debe proteger la gestión de autenticación de usuarios y privilegios.

En base a las credenciales de autenticación se debe dar los permisos para cada tipo de usuarios dentro e la red, solo los que posean las credenciales de trabajadores de la micro-red podrán tener los permisos necesarios para acceder a los demás dispositivos de red y los servicios de cada uno de estos. Se puede configurar en el servidor *Radius*.

Detección de intrusos Es importatnte detectar y prevenir el acceso no autorizado a los dispositivos.

Existe software libre como *Suricata*, que permite la detección de intrusos y detecta patrones de tráfico malicioso en la red. Otra opción es *FortiClient*, que cuenta con un módulo de detección de intrusiones.

Monitoreo y registro de eventos: Con el fin de detectar y dar una respuesta oportuna a los incidentes de ciberseguridad.

Los dispositivos TI y TO (o sus respectivas redes) deben ser monitoreadas. Una opción es usar la herramienta *Zabbix*, la cual debe ser configurada para detectar y registrar eventos de interés, tales como falla en dispositivos, tráfico inusual o accesos no autorizados.

Políticas: Además de las políticas internas de cada micro-red, se debe cumplir con algunas políticas básicas tal como se ha mencionado en el modelo creado. Las políticas que se mencionan se basan en normas y estándares como ISO 27001, ISO 31000, NIST SP 800-53, NIST SP 800-61.

Seguridad de la información: Enfocada en la confidencialidad, integridad y disponibilidad de la información de la micro-red.

Algunas de estas políticas son la clasificación de información (sensibilidad y confidencialidad), control de acceso (gestión y revocación de credenciales), gestión de contraseñas (creación y cambio) y seguridad de red (cifrado de la información, detección de intrusos).

Gestión de identidad y acceso: Enfocada en la autenticación y gestión de privilegios.

Es necesario una política de contraseñas (longitud mínima, caducidad), control de acceso basado en roles (privilegios y permisos de los usuarios), accesos externos (gestión de acceso remoto de usuarios, VPN).

Gestión de respuesta a incidentes: Enfocada en la detección y respuesta a incidentes de ciberseguridad.

Se debe tratar acerca de la definición de incidentes, responsabilidades, procedimientos de respuesta y comunicación (procedimientos a realizar y forma en la que se manejan los incidentes).

Gestión de riesgos: Enfocada en identificar, evaluar y mitigar riesgos de ciberseguridad dentro de la micro-red.

Es importante la identificación de activos críticos, evaluación de riesgos (probabilidad e impacto), gestión de vulnerabilidades (identificación y mitigación).

Auditorías: Dependiendo de cada país, se debe cumplir con determinadas auditorías y certificaciones, las más comunes son:

Vulnerabilidades: Esta auditoría evalúa vulnerabilidades dentro de la micro-red, por ejemplo configuraciones, puertos usados, software no actualizado [77].

Seguridad de la red: Es importante la evaluación de la seguridad de la red y la protección que esta tiene ante diferentes ataques, como DoS, falsificación de identidad o intrusiones [77].

Cumplimiento de normativas: La micro-red debe cumplir con requisitos legales y normativos, se evalúan controles y políticas de seguridad, capacitación del personal, etc [78].

Certificaciones: Estas dependerán de la regulación interna de cada país, a continuación se mencionan las certificaciones más importantes en ciberseguridad dentro de entornos industriales según [79].

ISO 27001 Relacionada con estándares para la seguridad de la información.

NIST SP 800-82 Enfocada en estándares de ciberseguridad sistemas de control dentro de industrias.

IEC 62443 Enfocada en la protección cibernética en entornos con automatización industrial.

4.7. Criticidad de la micro-red de la Universidad de Cuenca

La micro-red de la Universidad de Cuenca entrega alrededor de 3272.4 kWh de energía al mes, el servicio que depende de la misma es el *data center* de la Universidad de Cuenca. Según [80] los incidentes de ciberseguridad se pueden clasificar por su criticidad, entendiendo esta como el impacto que tienen en la información, los sistemas y redes a los que afectan. Los niveles de criticidad o prioridad en los incidentes de ciberseguridad pueden clasificarse en tres, tanto para las infraestructuras críticas, como para otros agentes, empresas y en los ciudadanos:

Nivel de criticidad alta: agrupan a los incidentes que afectan a sistemas o información crítica para la entidad y con potencial impacto en el negocio.

Nivel de criticidad media: engloban a los incidentes que afectan a sistemas o información no críticos para la entidad o cuyo impacto no repercute directamente en el desarrollo del negocio.

Nivel de criticidad baja: hacen referencia a los incidentes en sistemas con bajo nivel de importancia, investigaciones que impliquen análisis forenses que se alarguen en el tiempo o consultas genéricas sobre seguridad.

Dado que se afectan sistemas de información crítica como lo es el centro de proceso de datos en donde se almacenan todos los datos y operaciones sobre las cuentas de la Universidad se podría considerar que se encuentra en un nivel de criticidad alto.

5. Conclusiones y recomendaciones

La ciberseguridad en las infraestructuras críticas es de suma importancia dado que en la actualidad existen múltiples maneras de vulnerar las mismas. Una de estas infraestructuras es el sector eléctrico en donde existen diferentes tipos de ataques a los que puede ser expuesta como: en la distribución de la electricidad, confiabilidad en las redes de comunicación. Debido al uso de energía eléctrica en casi todos los ámbitos de la vida, una afección a su generación y distribución puede traer consigo graves consecuencias más allá de las económicas.

Existe un déficit de información en cuanto a la ciberseguridad para los sectores eléctricos, dado que las normativas son amplias y poco focalizadas en los dispositivos que abarcan tecnología de la información y tecnología de operación. En el Ecuador existen muchas deficiencias para localizar los riesgos en el sector eléctrico, conciencia de ciberseguridad y su importancia. Por lo que se ha visto la necesidad de contribuir con estrategias de ciberdefensa dentro del país, en este caso con una infraestructura crítica específica.

Para iniciar con la creación de un modelo adecuado para medir el nivel de madurez en las micro-redes eléctricas se ha realizado un estado de arte referente al nivel de madurez de ciberseguridad, en donde se ha encontrado la información de diferentes modelos que se han ido diseñando en áreas industriales o infraestructuras críticas. Permitiendo así utilizar diferentes normas y estándares para definir un estado de madurez, sin embargo no ha existido ninguno que se enfoque en las micro-redes eléctricas.

Dada la falta de información en el sector eléctrico, es evidente la necesidad de encontrar un modelo que permita medir el nivel de madurez dentro de una micro-red; en donde en base a los dominios y atributos establecidos en cada nivel se permite observar la serie de requisitos y buenas prácticas que se necesitan cumplir para incrementar la protección y seguridad de las mismas. Se establecen cuatro niveles de madurez que permiten definir el estado actual de la micro-red mediante el establecimiento de dominios enfocados a identificación, detección, protección, respuesta y reparación de activos, procesos, amenazas, vulnerabilidades y dependencias dentro de una micro-red.

Con este proyecto se logra establecer en que nivel de madurez se encuentra una micro-red en base a los atributos que cumple la misma y establecer los pasos a seguir para aumentar el nivel. Logrando así tener un punto de partida para las prácticas a seguir con el fin de tener un mayor nivel de madurez.

El modelo creado se aplica a la micro-red de la Universidad de Cuenca como caso de estudio. en donde se ha podido observar que se encuentra en un nivel de madurez no existente (NIM0) por lo que es de suma importancia proceder con la implementación de la ciberseguridad dentro de esta. Las recomendaciones que se han propuesto son acciones necesarias para lograr subir un nivel del que se encuentra en la actualidad la micro-red.

En el presente trabajo se ha implementado un modelo de madurez que permite medir el nivel en el que se encuentra una micro-red. Se proporciona una aplicación que facilita la evaluación periódica de la misma, con estos resultados es posible brindar las recomendaciones necesarias para alcanzar un nivel de madurez superior al obtenido. Logrando así facilitar el proceso de acciones de ciberseguridad que debe tomar en cuenta una micro-red.

Como recomendaciones se propone la implementación de acciones mencionadas en la Sección 4.3 en la micro-red de la Universidad de Cuenca para incrementar el nivel de madurez dentro de la infraestructura evaluada, además de implementar las mitigaciones de las amenazas presentadas en la sección 4.4. El sistema de seguridad diseñado junto con el sistema de gestión y operación pueden ser implementados en trabajos futuros dentro de la micro-red tomada como caso de estudio.

El *pentesting* realizado a la micro-red de la Universidad de Cuenca dejó en evidencia las falencias que tiene la red, varios puertos de los activos presentan vulnerabilidades. Encontrando 417 vulnerabilidades clasificándolas en críticas, severas y moderadas, con esta información se ha encontrado los riesgos del sistema y la probabilidad de ocurrencia de los mismos. Una vez encontrados los riesgos se los ha clasificado en los diferentes tipos de amenazas y se ha procedido a detallar la mitigación de los mismos, siendo esto un punto importante a tomar en cuenta por parte de la micro-red.

Se da conocimiento también los mecanismos de protección de seguridad para la micro-red de la Universidad de Cuenca y los mecanismos de protección de seguridad para la red, además de que se mencionan las normativas y políticas con las que debe cumplir infraestructuras de este tipo.

Bibliografía

[1] M. d. C. Lozano Lozano y R. A. Zamora Muñoz, “Tecnologías y herramientas de ingeniería asociadas a los niveles superiores de la pirámide de la automatización,” 2008.

[2] W. A. ROSAS, F. A. MEDINA, y J. A. MESA, “Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas,” *Revista ESPACIOS*, vol. 41, num. 07, mar 2020.

[3] L. Milagros, Q. Carbajal, J. Sanchez, y W. Oña, “AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES Related papers Aut omat izacion Procesos Indust riales-Alfa Omega,” 1999. [En línea]. Disponible: www.lalibreria.upv.es

[4] E. J. S. Chinchilla y J. S. Allende, “Riesgos de ciberseguridad en las Empresas,” *Tecnología y desarrollo*, vol. 15, num. 0, dec 2017. [En línea]. Disponible: https://revistas.uax.es/index.php/tec_des/article/view/1174

[5] “2017 Public-Private Analytic Exchange Program (AEP) Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions PUBLIC-PRIVATE Analytic Exchange Program Supply Chain Risks of SCADA/Industrial Control Systems in the Electricity Sector: Recognizing Risks and Recommended Mitigation Actions.”

[6] “Cybersecurity technologies: Utilities to invest $3.2bn in security by 2026.” [En línea]. Disponible: https://www.smart-energy.com/industry-sectors/smart-grid/cybersecurity-technologies-navigant-research/

[7] L. A. Anchino, A. Torti, M. Miretti, E. Bernardi, G. Peretti, y R. Podadera, “Ciberseguridad en los sistemas de control industrial: clave para la ciberdefensa de las infraestructuras críticas,” *XXI Workshop de Investigadores en Ciencias de la Computación*, pp. 971–974, 2019. [En línea]. Disponible: http://sedici.unlp.edu.ar/handle/10915/77258

[8] F. Heymann, S. Henry, y M. Galus, “Cybersecurity and resilience in the swiss electricity sector: Status and policy options,” *Utilities Policy*, vol. 79, p. 101432, dec 2022.

[9] “La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial - Centro de Ciberseguridad Industrial.” [En línea]. Disponible: https://www.cci-es.org/activities/documento-la-proteccion-de-infraestructuras-criticas-y-la-ciberseguridad-industrial/

[10] “Florida: Detectan el ataque de un hacker que intentó envenenar con lejía el suministro de agua de Oldsmar.” [En línea]. Disponible: https://www.antena3.com/noticias/mundo/detectan-ataque-hacker-que-intento-envenenar-lejia-suministro-agua-oldsmar-florida_2021020960227e0411b1180001d505f2.html

[11] “” estamos en guerra¨: 5 claves para entender el ciberataque que tiene a costa rica en estado de emergencia - bbc news mundo.” [En línea]. Disponible: https://www.bbc.com/mundo/noticias-america-latina-61516874

[12] M. Mónica y D. R. Carlos, “La protección de infraestructuras críticas.” [En línea]. Disponible: http://www.aeiseguridad.es/descargas/categoria6/4508139.pdf.

[13] S. Pascual de Vega, “Micro redes y redes inteligentes,” 2018. [En línea]. Disponible: https://uvadoc.uva.es/handle/10324/31400

[14] B. P. Guzmán-Escoto, J. M. Lozano García, A. Pizano-Martínez, E. A. Zamora-Cárdenas, y H. J. Estrada-García, “Control de Generación de una Micro-Red Eléctrica Conformada por Fuentes Renovables de Energía.”

[15] D. Arbeláez Trejos y Á. D. Paredes Cortés, “Coordinación óptima de elementos de protección en microredes,” 2019. [En línea]. Disponible: https://hdl.handle.net/11059/10403

[16] “Vista de Gestión de seguridad en redes corporativas.” [En línea]. Disponible: https://revistas.ulima.edu.pe/index.php/Interfases/article/view/162/110

[17] G. Tandazo y N. Etelbida, “Evaluar las vulnerabilidades de seguridad existentes en la red del sistema scada de la eerssa,” 2016.

[18] G. Grispos, “Cybersecurity: Practice,” *Encyclopedia of Security and Emergency Management*, pp. 1–6, 2019.

[19] G. B. Gaggero, P. Girdinio, y M. Marchese, “Advancements and research trends in microgrids cybersecurity,” *Applied Sciences*, vol. 11, num. 16, p. 7363, 2021.

[20] P. J. Hueros Barrios *y otros*, “Ciberseguridad en smart grids: Estudio y aplicación real sobre una microrred inteligente,” 2021.

[21] A. M. Roy, “La ciberseguridad, el auditor externo y los ocex,” *Auditoría pública: revista de los Organos Autónomos de Control Externo*, vol. 70, pp. 27–38, 2017.

[22] A. Ayerbe, “La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio,” *Economía industrial*, num. 410, pp. 37–46, 2018.

[23] F. Heymann, S. Henry, y M. Galus, “Cybersecurity and resilience in the swiss electricity sector: Status and policy options,” *Utilities Policy*, vol. 79, p. 101432, 2022. [En línea]. Disponible: https://www.sciencedirect.com/science/article/pii/S0957178722000960

[24] R. Caralli, M. Knight, y A. Montgomery, “Maturity models 101: A primer for applying maturity models to smart grid security, resilience, and interoperability,” Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, Tech. Rep., 2012.

[25] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, y H. Janicke, “A holistic cybersecurity maturity assessment framework for higher education institutions in the united kingdom,” *Applied Sciences*, vol. 10, num. 10, p. 3660, 2020.

[26] R. Kour, R. Karim, y A. Thaduri, “Cybersecurity for railways–a maturity model,” *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 234, num. 10, pp. 1129–1148, 2020.

[27] “ISO - ISO/IEC 27000:2018 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.” [En línea]. Disponible: https://www.iso.org/standard/73906.html

[28] “Recursos.” [En línea]. Disponible: https://www.iso27000.es/iso27002.html

[29] “ISO - ISO/IEC 27006:2015 - Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.” [En línea]. Disponible: https://www.iso.org/standard/62313.html

[30] “ISO - ISO/IEC 27019:2017 - Information technology — Security techniques — Information security controls for the energy utility industry.” [En línea]. Disponible: https://www.iso.org/standard/68091.html

[31] “Tipos de riesgo según la norma ISO 31000 2018.” [En línea]. Disponible: https://www.isotools.us/2021/08/13/tipos-de-riesgo-segun-la-norma-iso-31000-2018/

[32] “NIST General Information — NIST.” [En línea]. Disponible: https://www.nist.gov/director/pao/nist-general-information

[33] [En línea]. Disponible: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

[34] [En línea]. Disponible: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[35] [En línea]. Disponible: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[36] G. B. López y L. E. Velasteguí, "Automatización de procesos industriales mediante industria 4.0," *AlfaPublicaciones*, vol. 3, num. 3.1, pp. 98–115, 2021.

[37] M. d. J. Ramírez Cadena, I. Macías Hidalgo, y K. I. Ibáñez Viruega, "La pirámide de la automatización," 2019.

[38] J. D. Lemos, D. M. Guerrero, y A. Arias, "Opc como alternativa a las tecnologías propietarias de comunicación industrial," *Revista Avances en Sistemas e Informática*, vol. 3, num. 1, pp. 7–12, 2006.

[39] W. Mahnke y S. Leitner, "Arquitectura opc unificada," *Revista ABB*, vol. 3, pp. 56–61, 2009.

[40] E. M. Pérez, J. M. Acevedo, y C. F. Silva, *Automatas programables y sistemas de automatizacion/PLC and Automation Systems*. Marcombo, 2009.

[41] W. W. Jusoh, M. M. Hanafiah, M. A. Ghani, y S. Raman, "Remote terminal unit (rtu) hardware design and implementation efficient in different application," in *2013 IEEE 7th International Power Engineering and Optimization Conference (PEOCO)*. IEEE, 2013, pp. 570–573.

[42] G. Alayo, J. Enrique, N. Mendoza, y P. Alejandro, "Modelo de madurez de ciberseguridad cloud para el sector financiero," *Universidad Peruana de Ciencias Aplicadas (UPC)*, jul 2020. [En línea]. Disponible: https://repositorioacademico.upc.edu.pe/handle/10757/660408

[43] O. O. Akinsanya, M. Papadaki, y L. Sun, "Smart Healthcare and Safety Systems Current Cybersecurity Maturity Models: How Effective in Healthcare Cloud?"

[44] S. Bilak y K. Brennan, "Cybersecurity capability maturity model (c2m2)-cybersecurity maturity model certification (cmmc) supplemental guidance (draft)," CARNEGIE-MELLON UNIV PITTSBURGH PA, Tech. Rep., 2022.

[45] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, y H. Janicke, "A nis directive compliant cybersecurity maturity assessment framework," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2020, pp. 1641–1646.

[46] B. Yigit Ozkan, S. van Lingen, y M. Spruit, “The cybersecurity focus area maturity (cysfam) model,” *Journal of Cybersecurity and Privacy*, vol. 1, num. 1, pp. 119–139, 2021.

[47] J. Stevens, “Electricity subsector cybersecurity capability maturity model (es-c2m2)(case study),” Carnegie-mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 2014.

[48] D. Sulistyowati, F. Handayani, y Y. Suryanto, “Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss,” *JOIV: International Journal on Informatics Visualization*, vol. 4, num. 4, pp. 225–230, 2020.

[49] J. McCarthy, O. Alexander, S. Edwards, D. Faatz, C. Peloquin, S. Symington, A. Thibault, J. Wiltberger, y K. Viani, “Nist special publication 1800-7a-situational awareness-for electric utilities,” 2019.

[50] “Implementación de Soluciones TI para Seguridad Endpoint, Protección de Red, Perímetro y de Acceso a Contenidos. - hdl:11349/25066.” [En línea]. Disponible: https://repository.udistrital.edu.co/handle/11349/25066

[51] D. Villanueva, “Fundamentos de seguridad en redes Aplicaciones y estándares, 2da Edición.”

[52] “Control de acceso — Ciberseguridad.” [En línea]. Disponible: https://ciberseguridad.com/normativa/espana/medidas/control-acceso/

[53] “10 técnicas de control de acceso de seguridad informática.” [En línea]. Disponible: https://whitebearsolutions.grupocibernos.com/blog/10-tecnicas-de-control-de-acceso-de-seguridad-informatica-a-tener-en-cuenta

[54] “Modelos de control de accesos - Documentación de IBM.” [En línea]. Disponible: https://www.ibm.com/docs/es/sim/6.0.0.22?topic=planning-access-control-models

[55] “Qué es la autenticación de usuario y cómo mejorar su seguridad.” [En línea]. Disponible: https://www.redeszone.net/noticias/seguridad/que-es-autenticacion-usuario-mejorar-seguridad/

[56] N. E. González Tandazo, “Evaluar las vulnerabilidades de seguridad existentes en la red del sistema SCADA de la EERSSA,” 2016. [En línea]. Disponible: http://dspace.ucuenca.edu.ec/handle/123456789/23667

[57] “Antivirus: Una Herramienta Indispensable para Nuestra Seguridad — Revista .Seguridad.” [En línea]. Disponible: https://revista.seguridad.unam.mx/numero-04/antivirus-una-herramienta-indispensable-para-nuestra-seguridad

[58] M. Valdés Rodríguez, “Antispyware: Protegiéndote de los Espías,” jan 2010. [En línea]. Disponible: https://www.ru.tic.unam.mx/xmlui/handle/123456789/1718

[59] “Detección y Prevención de Intrusos (IDS/IPS) - Velorcios Group.” [En línea]. Disponible: https://velorciosgroup.com/sistemas-de-deteccion-y-prevencion-de-intrusos-ids-ips/

[60] “Descripción general de la detección y la prevención de intrusiones — Juniper Networks.” [En línea]. Disponible: https://www.juniper.net/documentation/mx/es/software/junos/idp-policy/topics/topic-map/security-idp-overview.html

[61] “¿Qué es la detección de anomalías? — TIBCO Software.” [En línea]. Disponible: https://www.tibco.com/es/reference-center/what-is-anomaly-detection

[62] V. Atluri y J. Horne, “A machine learning based threat intelligence framework for industrial control system network traffic indicators of compromise,” *Conference Proceedings - IEEE SOUTHEASTCON*, vol. 2021-March, mar 2021.

[63] “Auditoría de la actividad del usuario - Documentación de IBM.” [En línea]. Disponible: https://www.ibm.com/docs/es/urbancode-build/6.1.2?topic=security-auditing-user-activity

[64] “¿Qué es la auditoría? - Guía de administración del sistema: servicios de seguridad.” [En línea]. Disponible: https://docs.oracle.com/cd/E24842_01/html/E23286/auditov-2.html

[65] “Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones,” *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, num. 32, pp. 33–48, jun 2019.

[66] L. Vega de la Cruz, A. Nieves Julbe, y M. Pérez Pravia, “Procedimiento para evaluar el nivel de madurez y eficacia del control interno,” *Visión de futuro*, vol. 21, num. 2, pp. 0–0, 2017.

[67] J. A. Montoya y Z. Restrepo, “Gestión de identidades y control de acceso desde una perspectiva organizacional,” *Ingenierías USBMed*, vol. 3, num. 1, pp. 23–34, 2012.

[68] K. Keipi, S. M. Castro, y P. Bastidas, “Gestión de riesgo de amenazas naturales en proyectos de desarrollo lista de preguntas de verificación (“checklist”),” *Serie de informes de*

buenas prácticas del Departamento de Desarrollo Sostenible. Washington: Banco Interamericano de Desarrollo (BID), 2005.

[69] Y. Rojas Mesa, "De la gestión de información a la gestión del conocimiento," *Acimed*, vol. 14, num. 1, pp. 0–0, 2006.

[70] A. S. Chauhan, *Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus*. Packt Publishing Ltd, 2018.

[71] Ö. Aslan y R. Samet, "Mitigating cyber security attacks by being aware of vulnerabilities and bugs," in *2017 international conference on cyberworlds (cw)*. IEEE, 2017, pp. 222–225.

[72] K. Chhillar y S. Shrivastava, "University computer network vulnerability management using nmap and nexpose," *International Journal*, vol. 10, num. 6, 2021.

[73] T. Muliński, "Ict security in tax administration: Rapid7 nexpose vulnerability analysis," *Studia Informatica: systems and information technology*, vol. 1, 2020.

[74] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, y J. A. Saltos-Gómez, "La seguridad informática y la seguridad de la información," *Polo del conocimiento*, vol. 2, num. 12, pp. 145–155, 2018.

[75] "GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT MINISTERIO DEL INTERIOR SecrETARÍA de ESTADO de SEGURIDAD."

[76] P. Curtis, N. Mehravari, y J. Stevens, "Cybersecurity capability maturity model for information technology services (c2m2 for it services), version 1.0," CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States, Tech. Rep., 2015.

[77] J. Mejías Macías *y otros*, "Metodología para auditorías de ciberseguridad," 2016.

[78] R. A. T. Valero, "Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema scada," *Ingenierías USBMed*, vol. 11, num. 2, pp. 62–70, 2020.

[79] E. Zabalo Arteche, "La ciberseguridad como norma. estudio del estado del arte en estándares y certificación en materia de seguridad cibernética aplicada a industria 4.0 e iot," 2019.

[80] "Tipos de incidentes de ciberseguridad - Evaluando Cloud." [En línea]. Disponible: https://evaluandocloud.com/tipos-incidentes-ciberseguridad/

A. Anexo

El esquema que tienen los dominios para cumplir con cada uno de sus atributos es descrito mediante los diagramas de flujo presentados en las Figuras A.1-A.10, los cuales se basan en la condición de cumplir o no los atributos de cada nivel para avanzar al siguiente. La relación de cada dominio con su respectivo esquema se describe en la Tabla A.1.

Tabla A.1: Relación de los dominios con sus respectivos esquemas

Dominio	**Esquema**
Gestión de riesgos	Figura A.1
Gestión de activos	Figura A.2
Gestión de identidad y acceso	Figura A.3
Gestión de amenazas y vulnerabilidades	Figura A.4
Conciencia del estado actual	Figura A.5
Intercambio de información y comunicaciones	Figura A.6
Repuesta a incidentes	Figura A.7
Gestión de dependencias externas	Figura A.8
Capacitación del Personal	Figura A.9
Gestión del programa de ciberseguridad	Figura A.10

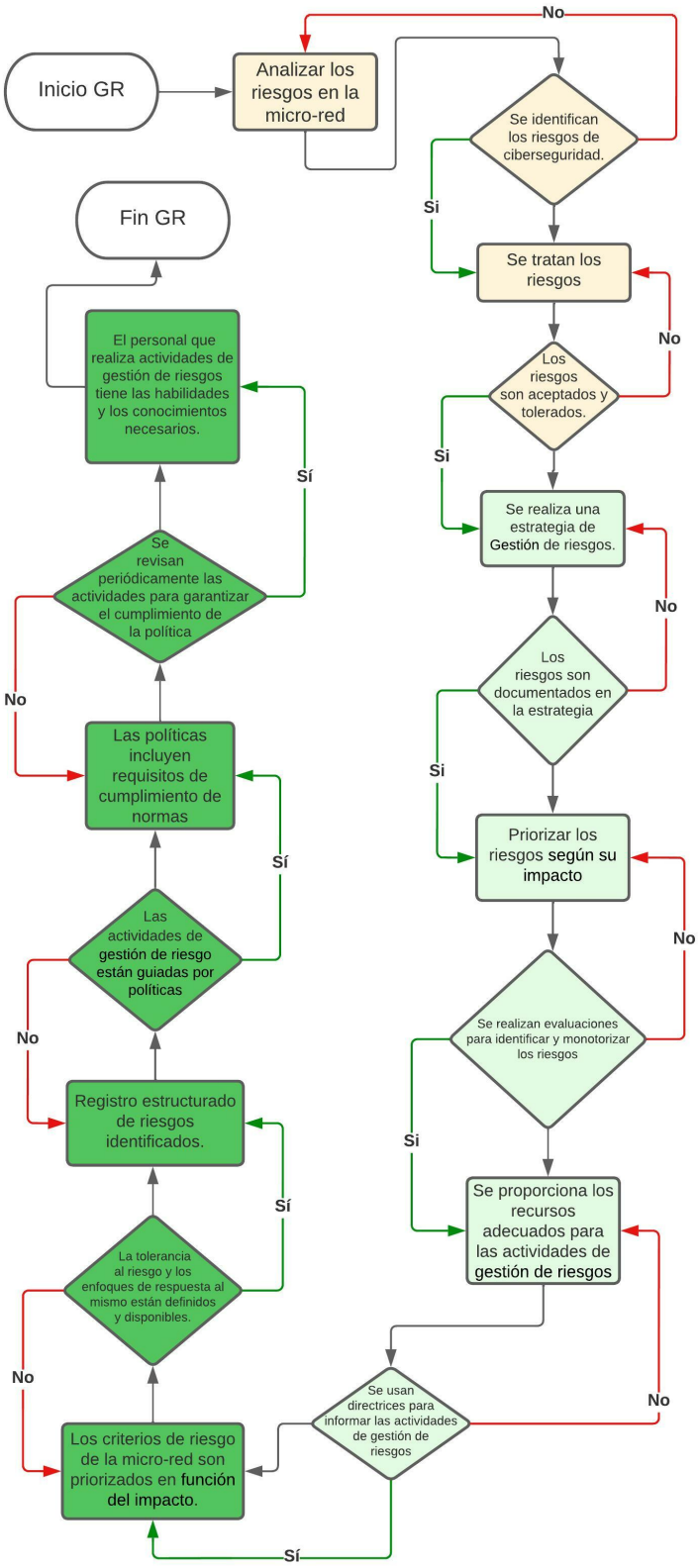

Figura A.1: Esquema a seguir para incrementar el nivel madurez en el dominio GR

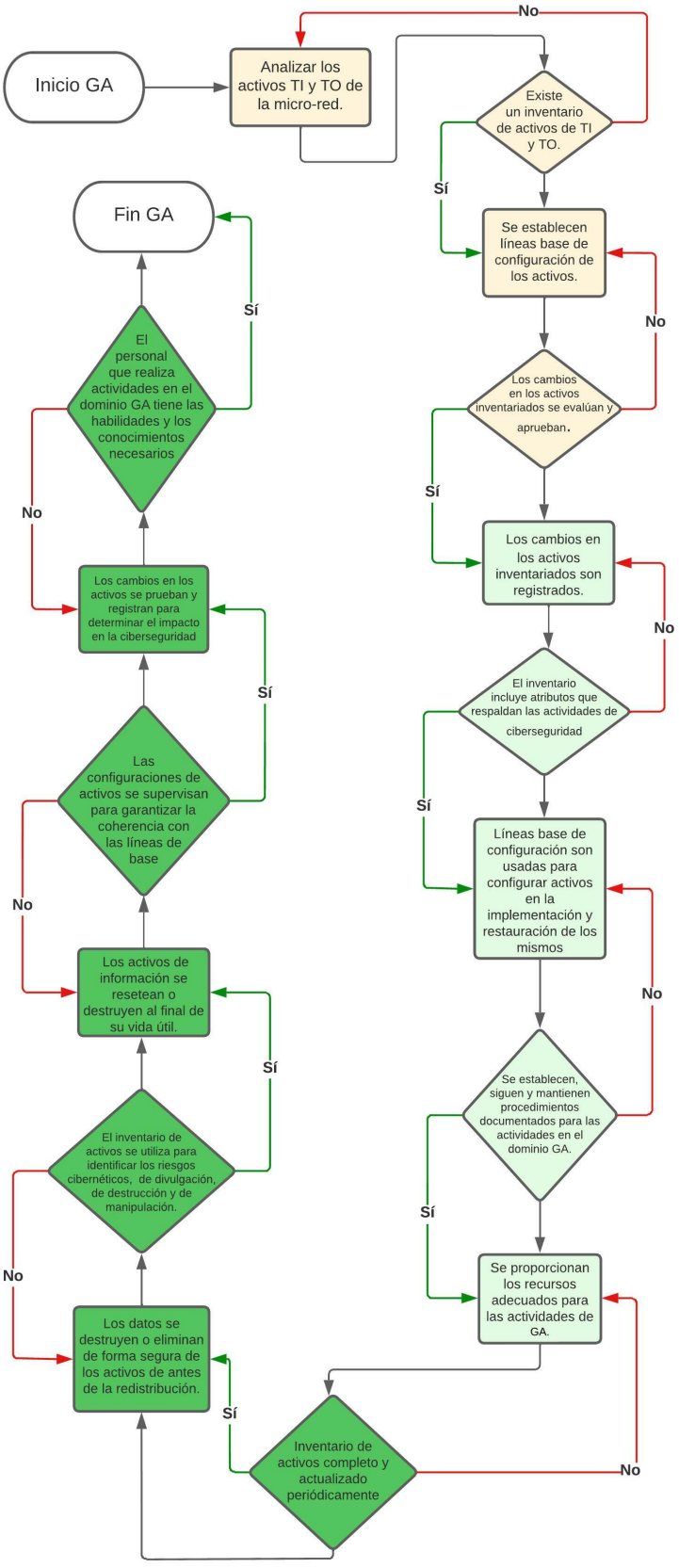

Figura A.2: Esquema a seguir para incrementar el nivel madurez en el dominio GA

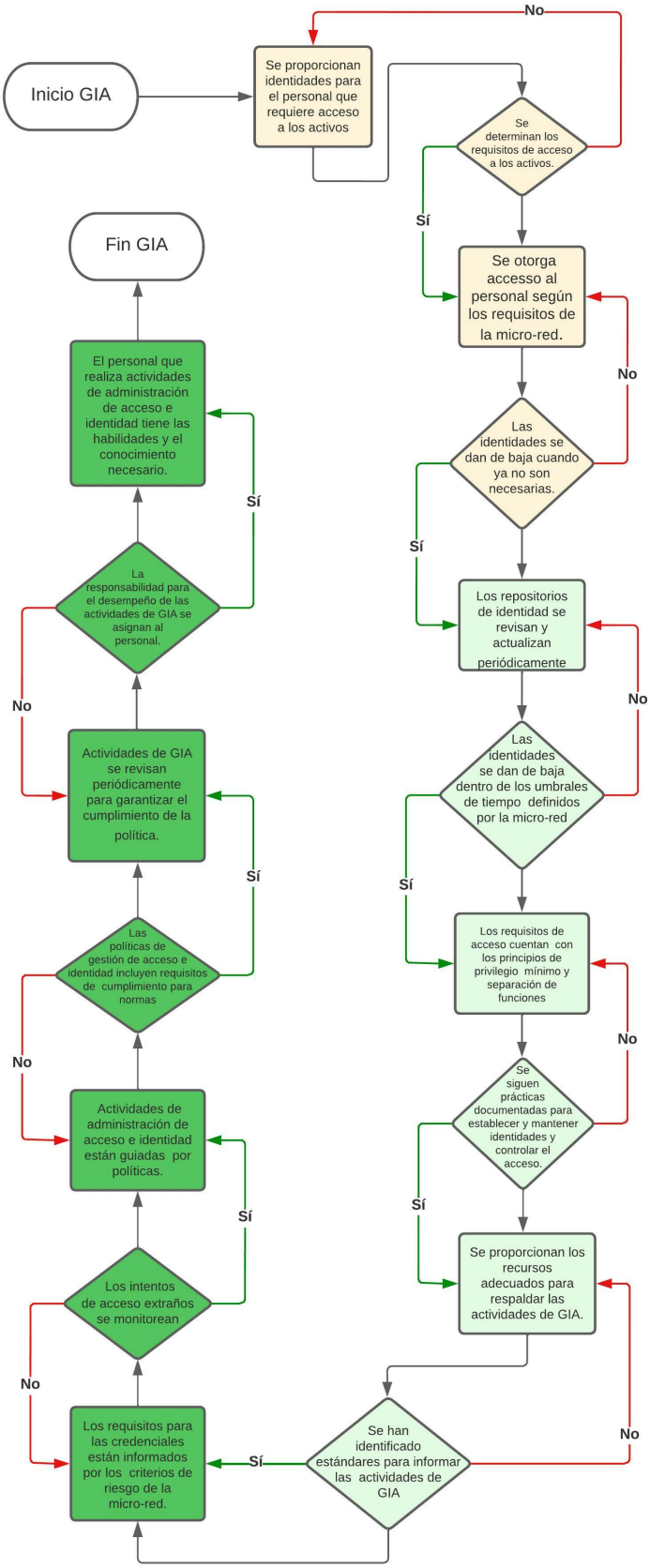

Figura A.3: Esquema a seguir para incrementar el nivel madurez en el dominio GIA

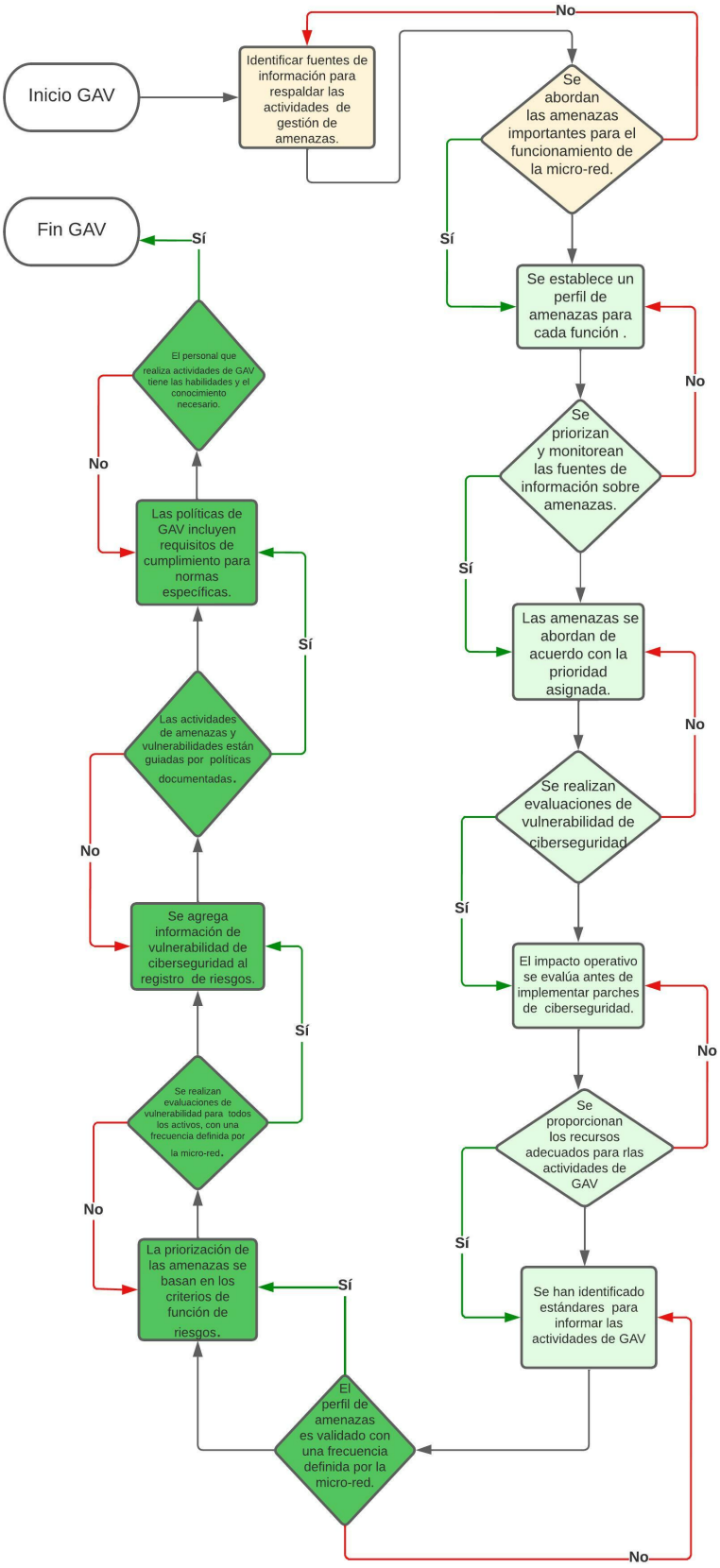

Figura A.4: Esquema a seguir para incrementar el nivel madurez en el dominio GAV

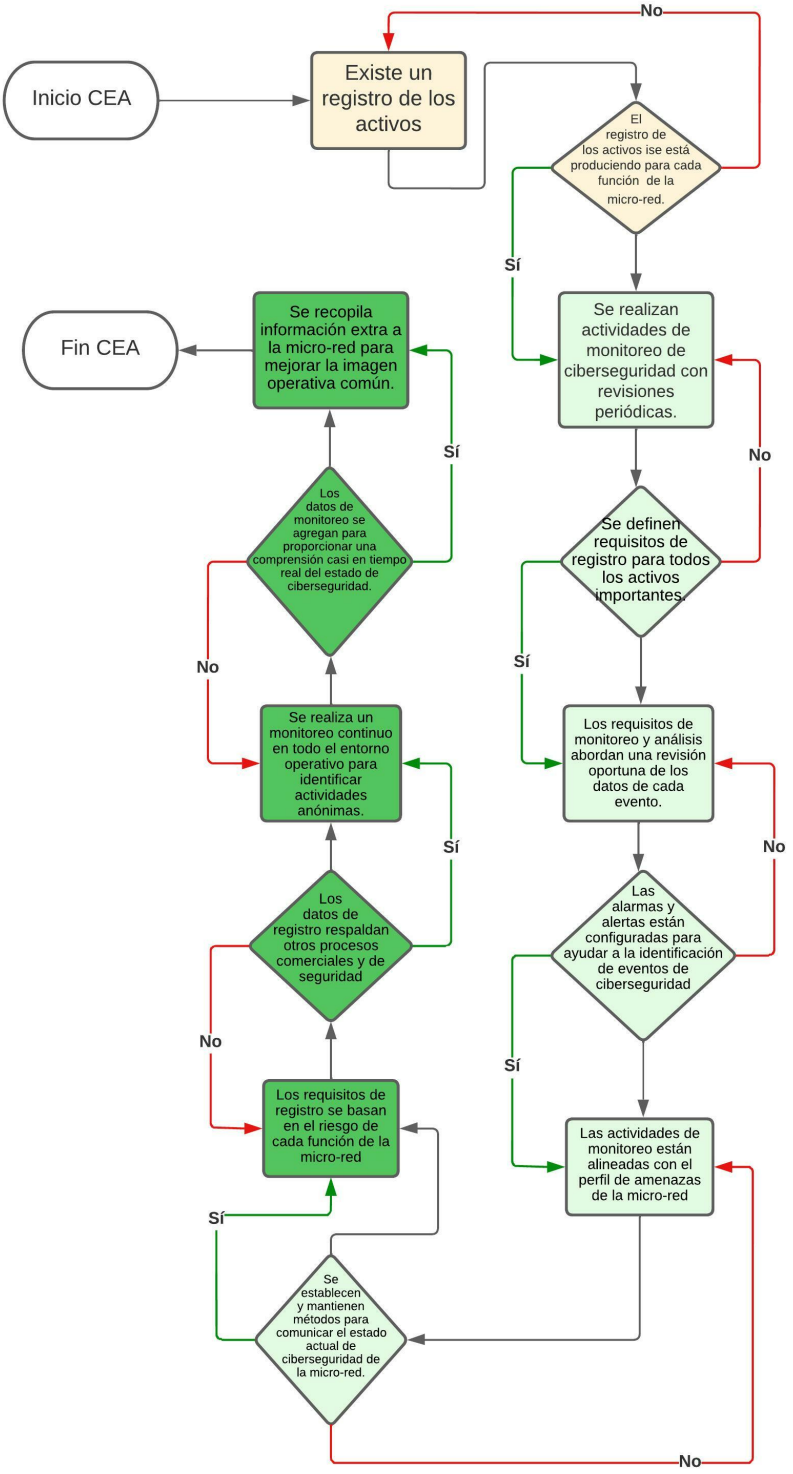

Figura A.5: Esquema a seguir para incrementar el nivel madurez en el dominio CEA

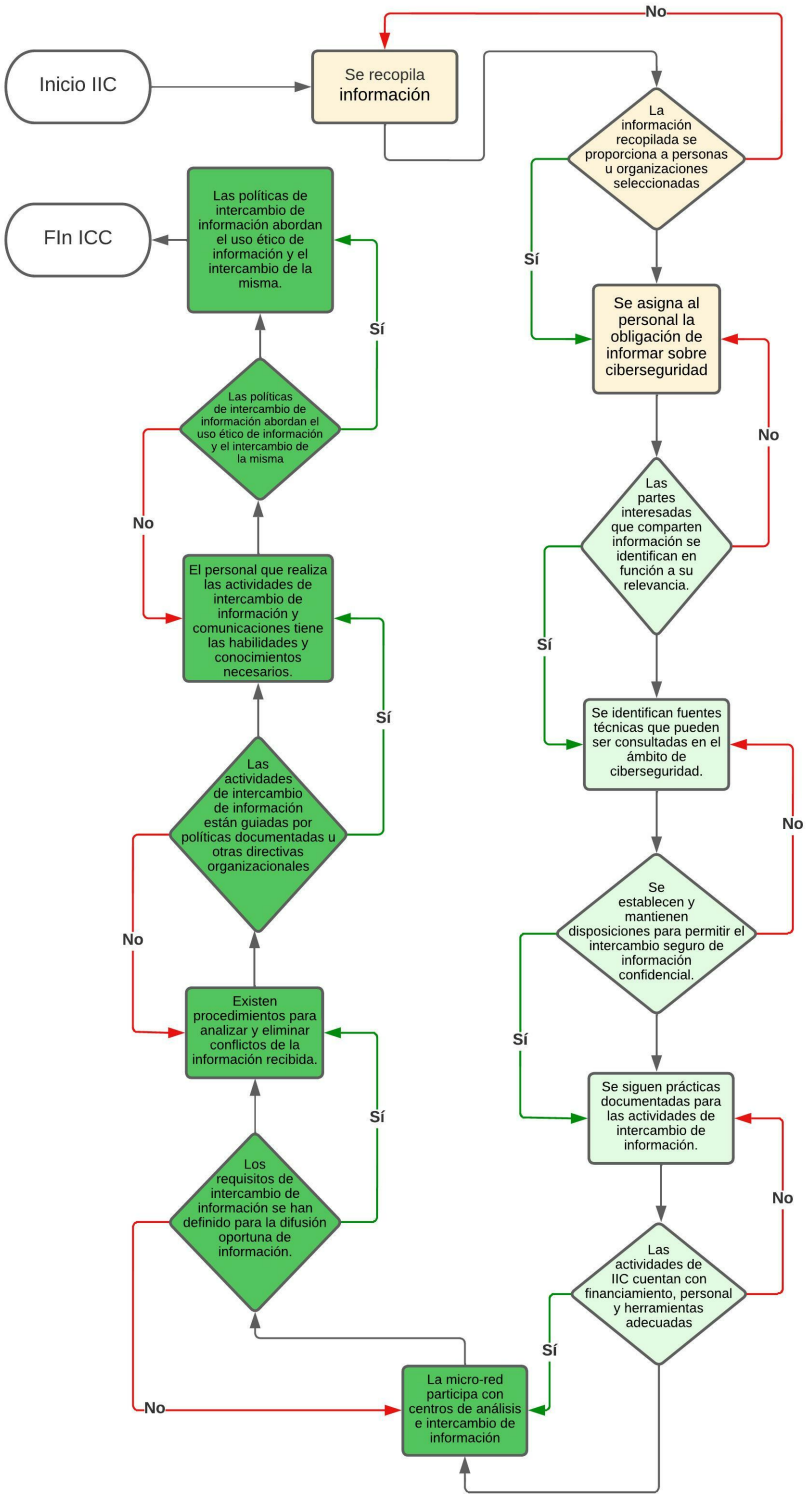

Figura A.6: Esquema a seguir para incrementar el nivel madurez en el dominio IIC

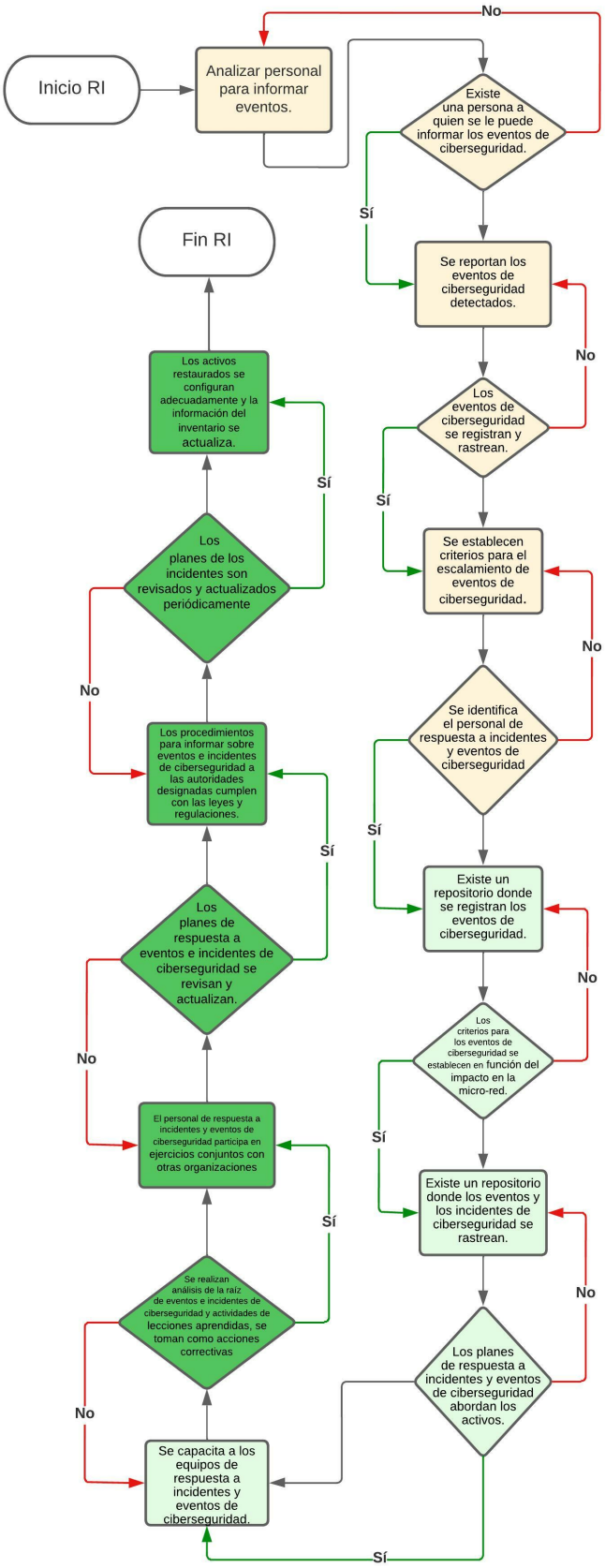

Figura A.7: Esquema a seguir para incrementar el nivel madurez en el dominio RI

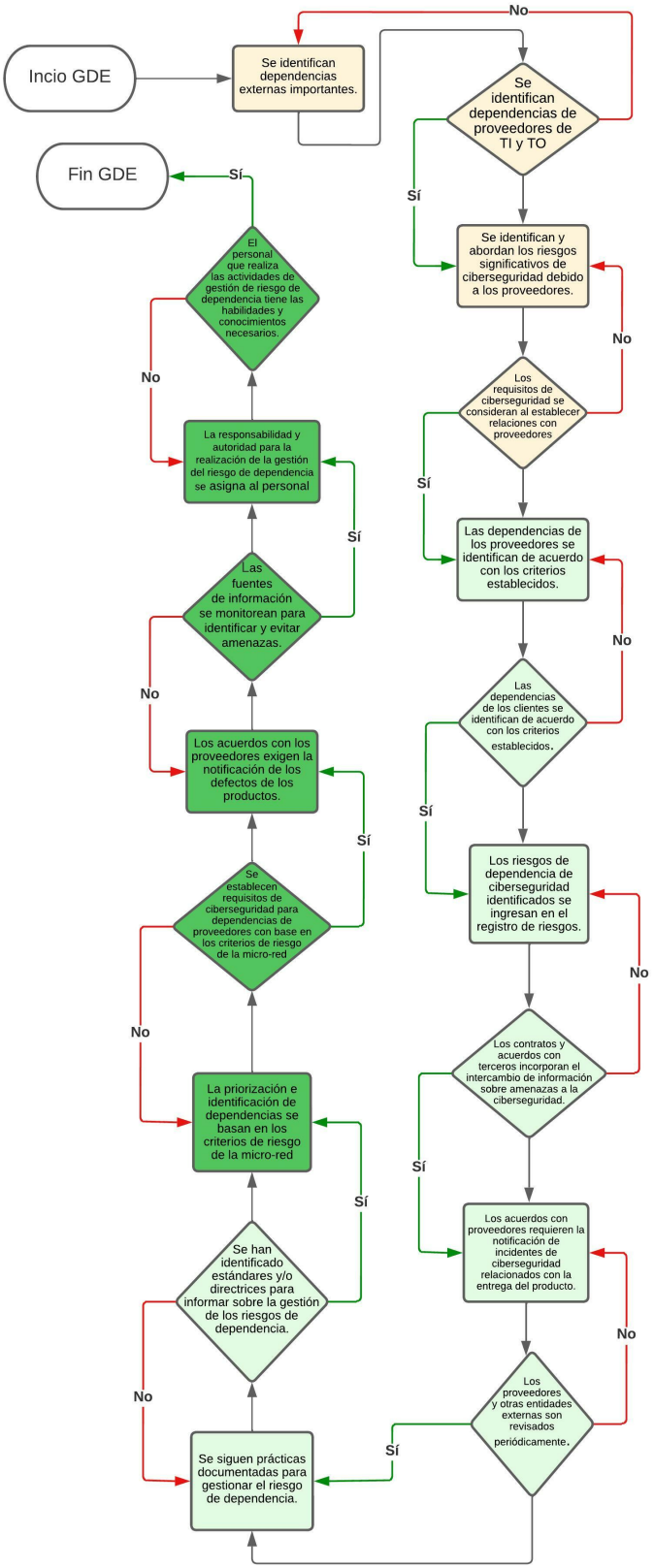

Figura A.8: Esquema a seguir para incrementar el nivel madurez en el dominio GDE

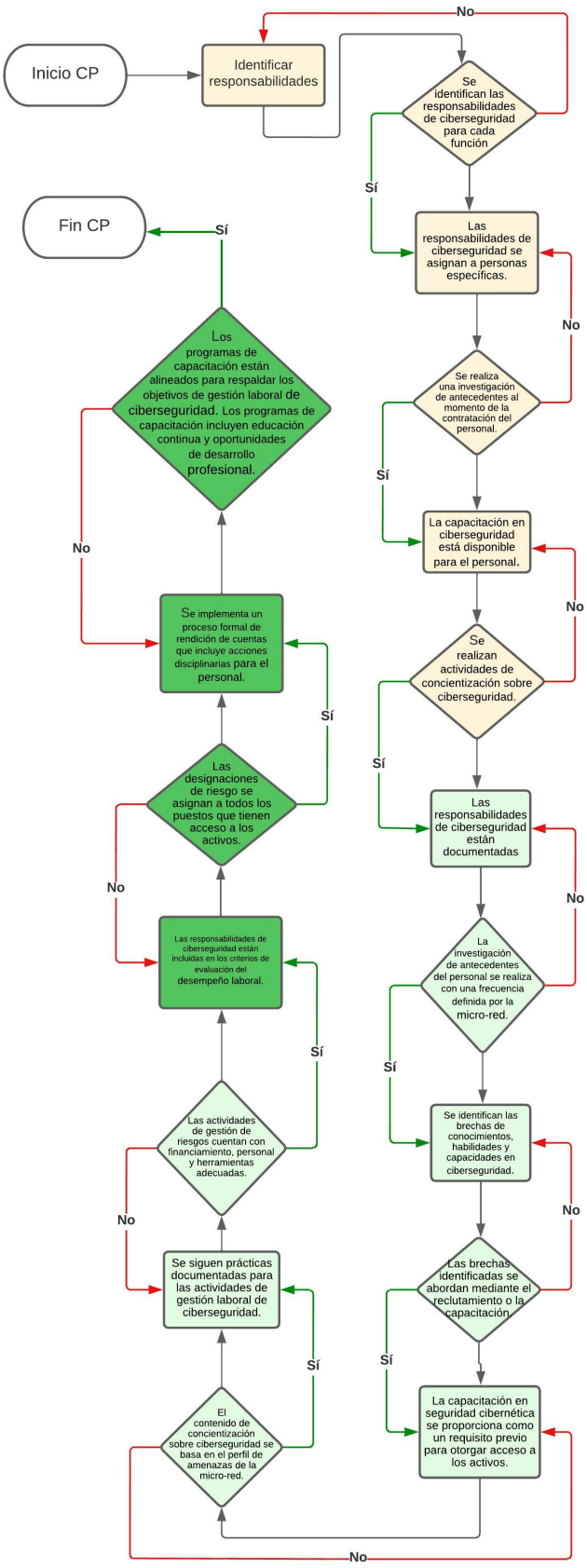

Figura A.9: Esquema a seguir para incrementar el nivel madurez en el dominio CP

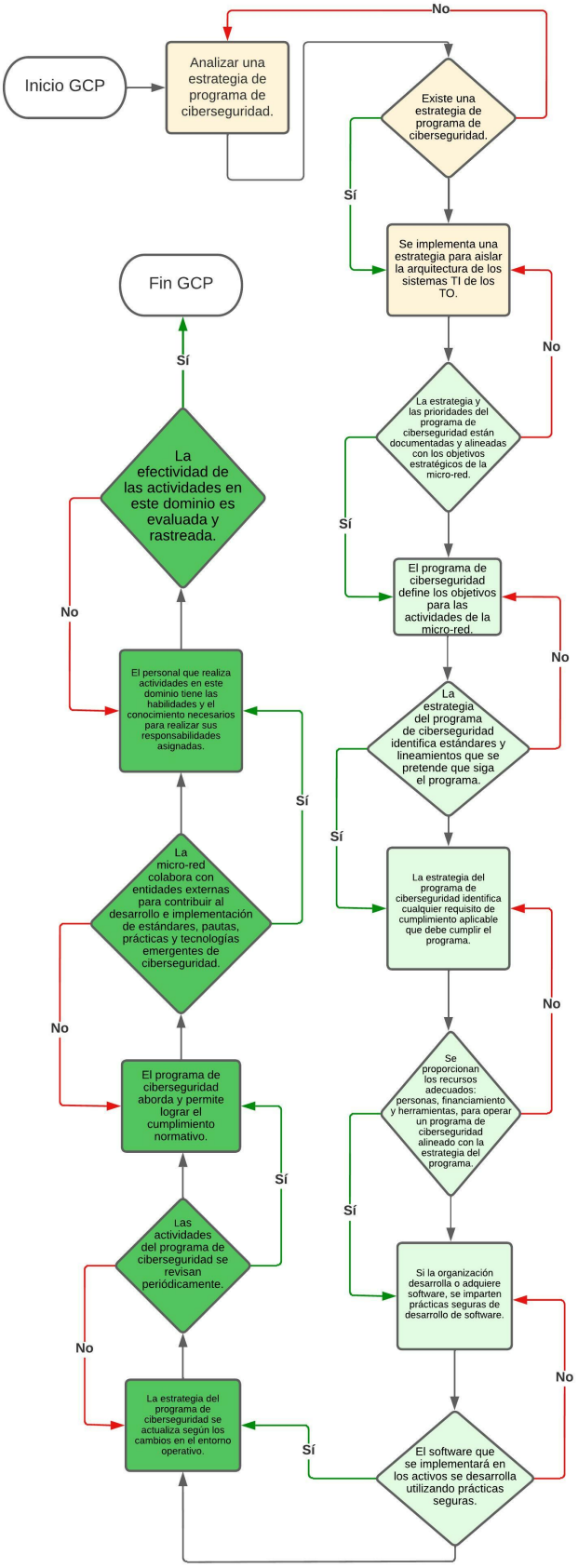

Figura A.10: Esquema a seguir para incrementar el nivel madurez en el dominio GPC

B. Anexo

La aplicación desarrollada se encuentra en el repositorio: https://github.com/AndresSumba/Modelo_Ciberseguridad_MicroRed.

B.1. Manual de usuario para la aplicación

Como se puede observar en la Figura B.1, la página principal consta de un inicio en donde se solicita iniciar sesión, para que de esta manera se pueda desplegar las preguntas emitidas en base a los dominios y atributos mencionados anteriormente.

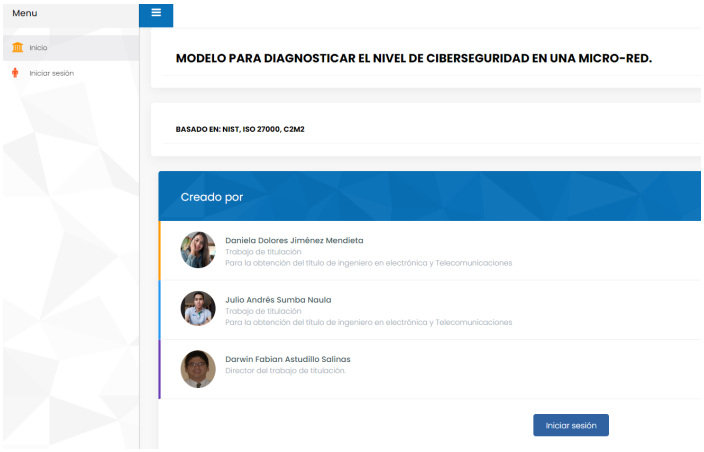

Figura B.1: Página principal

Una vez que se presiona en iniciar sesión, la página solicitará ingresar usuario y contraseña tal como se muestra en la Figura B.2.

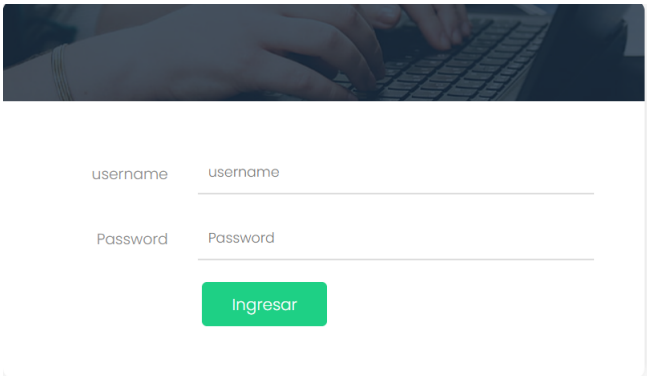

Figura B.2: Página principal

En las subsecciones siguientes se describe los procesos del cuestionario y el *dashboard*, de igual manera se presentan figuras a detalle de las distintas partes de la aplicación creada.

B.1.1. Cuestionario para realizar el diagnóstico

Una vez que se ha iniciado la sesión aparecerá la opción de elegir micro-red lo que se observa en la Figura B.3, en donde se podrá añadir la micro-red que va a ser evaluada para realizar el diagnóstico de la misma y observar los resultados. Como se muestra en la Figura B.4.

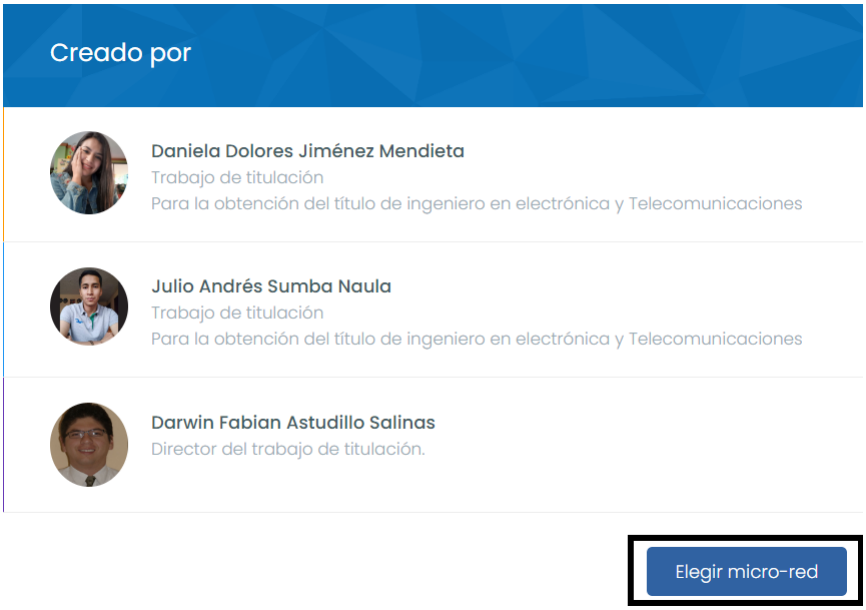

Figura B.3: Elegir micro-red.

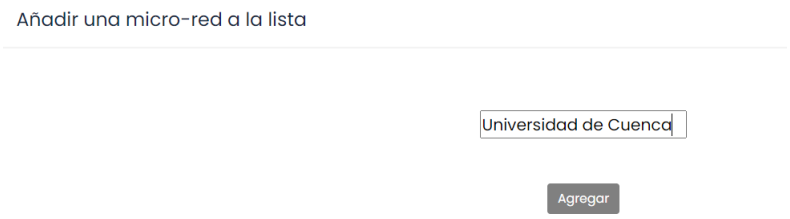

Figura B.4: Agregar micro-red.

Luego de que se ha añadido con éxito la micro-red aparecerán las opciones de realizar diagnóstico y ver resultados, tal como se muestra en la Figura B.5.

Las preguntas diagnóstico se las puede observar en la Figura B.6. Las mismas que están relacionadas con todos los atributos mostrados en el modelo creado descrito en la Sección

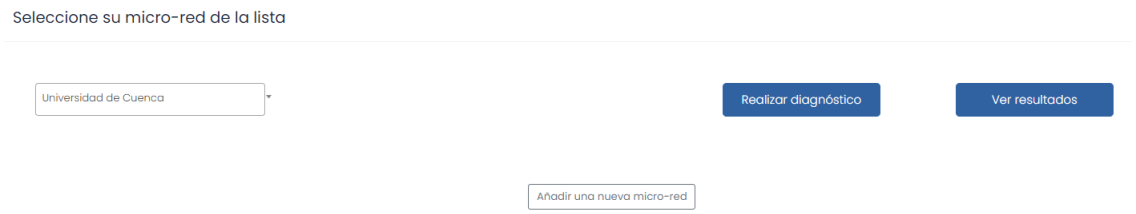

Figura B.5: Realizar diagnóstico.

3.5.

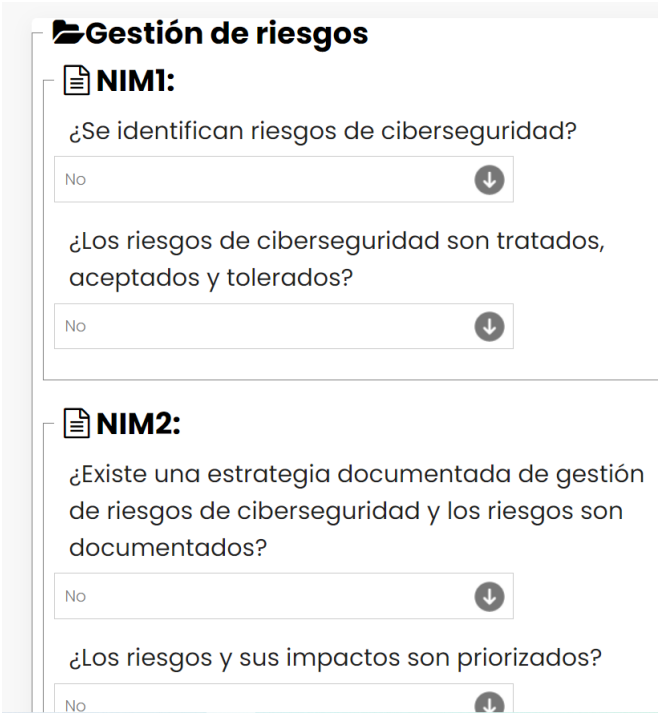

Figura B.6: Preguntas diagnóstico

B.1.2. Dashboard

Para observar los resultados alcanzados al realizar el diagnóstico se deberá ir a la opción *resultados* de la página web, en donde se desplegarán los puntajes que se han ido alcanzando en cada evaluación realizada, junto con la fecha del diagnóstico. Tal como se muestra en la Figura B.7.

Es así que se puede observar el *dashboard* del puntaje total alcanzado y las fechas en las que se ha emitido un diagnóstico, para observar la evolución de ciberseguridad dentro de una

Fecha del diagnóstico	Puntaje total	Link
Nov. 27, 2022, 9:18 a.m.	800	Ver grafico de radar
Nov. 27, 2022, 9:24 a.m.	600	Ver grafico de radar
Nov. 27, 2022, 10:57 a.m.	300	Ver grafico de radar
Dec. 6, 2022, 8:08 a.m.	200	Ver grafico de radar

Figura B.7: Resultados del diagnóstico

micro-red. El mismo que se lo puede observar en la Figura B.8.

Figura B.8: Resultados del diagnóstico

En cuanto al *dashboard radar* de cada fecha en la que se ha emitido la evaluación, se lo puede observar dando click en *ver gráfico radar*. En donde se desplegará el mismo dando mayor información de los puntajes alcanzados en cada dominio, observando así los resultados alcanzados como se muestra en las Figuras B.9 y B.10, respectivamente.

Modelo	Puntaje
Gestión de riesgos	50
Gestión de activos	50
Gestión de identidad y acceso	50
Gestión de amenazas y vulnerabilidades	50
Conciencia del Estado Actual	50
Intercambio de Información y Comunicaciones	50
Respuesta a Incidentes:	50
Gestión de dependencias externas:	50
Capacitación del personal	40
Gestión de programa de ciberseguridad	50
Total	490

Figura B.9: Puntaje del diagnóstico en cada dominio

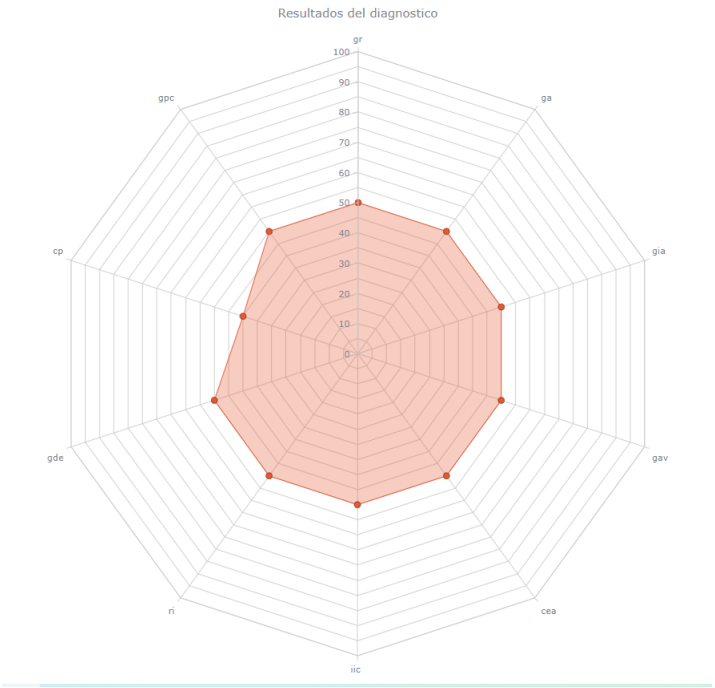

Figura B.10: Resultados radar del diagnóstico.

C. Anexo

C.1. Descripción de activos de la micro-red de la Universidad de Cuenca

C.1.1. Sistema de control y adquisición de datos

El sistema SCADA se encuentra en *LabVIEW* que es un entorno de programación gráfica dicho programa está funcionando en Windows 7 en una máquina virtual. Este sistema permite realizar un análisis de fallas, emite alarmas cuando se presenten algún tipo de vulnerabilidad o evento, permite el control de los equipos que se encuentran en la micro-red. Otro factor importante es que registra operaciones o maniobras, control de carga y energía. El panel del sistema se lo puede observar en la Figura C.1, mientras que el sistema físico del SCADA de la micro-red se lo puede observar en la Figura C.2.

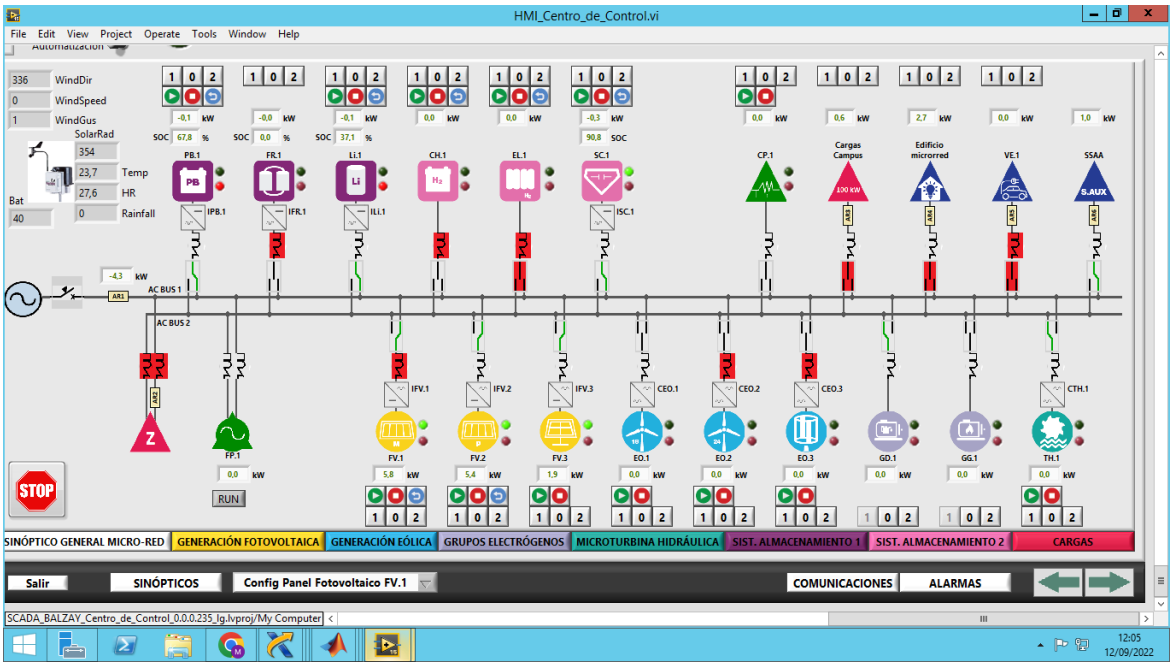

Figura C.1: Sistema SCADA de la micro-red

C.1.2. Servidor OPC

En el caso de la micro-red este servidor OPC se conecta con un *switch* y a partir del mismo se conecta a los PLCs y ellos a su vez con sus respectivos RTUs. El servidor usado es el SIMATIC S7-1500 de la marca SIEMENS. El dispositivo empleado en la micro-red, se lo puede observar en la Figura C.3.

Figura C.2: Sistema SCADA físico

Figura C.3: Servidor OPC

C.1.3. Control lógico programable

En la micro-red el PLC cuenta con un servidor que conecta a los mismos dispositivos mediante un *switch*. Controla las entradas y salidas de los dispositivos que son controlados en la micro-red. Los PLCs que se encuentran en la micro-red son del modelo M521 de la marca Schneider. Este dispositivo se lo puede observar en la Figura C.4.

Figura C.4: PLC empleado en la micro-red.

C.1.4. Unidades terminales remotas

Los RTUs instalados en la micro-red son del modelo TM3DQ8R de la marca Schneider. Las características de este dispositivo se encuentran disponibles en https://octopart.com/datasheet/tm3dq8r-schneider+electric-49251529. El dispositivo empleado en la micro-red se lo puede observar en la Figura C.5.

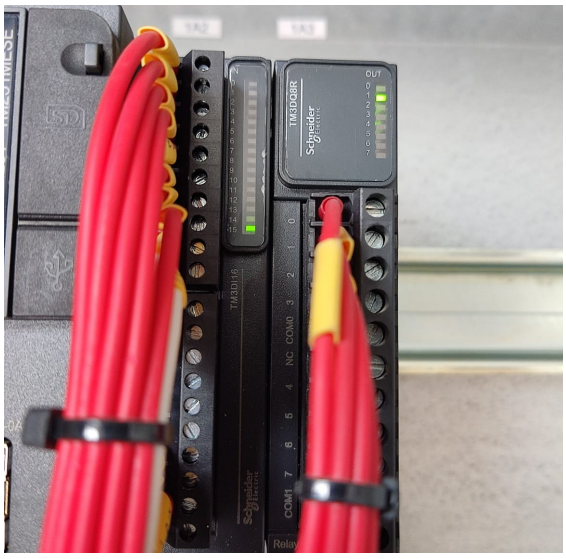

Figura C.5: RTU empleado en la micro-red.

D. Anexo

El uso de la herramienta *Nmap* en la máquina virtual *KaliLinux* permite conocer los dispositivos en la red, obteniendo la dirección IP y MAC además de puertos abiertos y servicios que se encuentran en estos, permitiendo así obtener la información necesaria para fijar un objetivo de ataque, un ejemplo de uso de esta herramienta se observa en la Figura D.1.

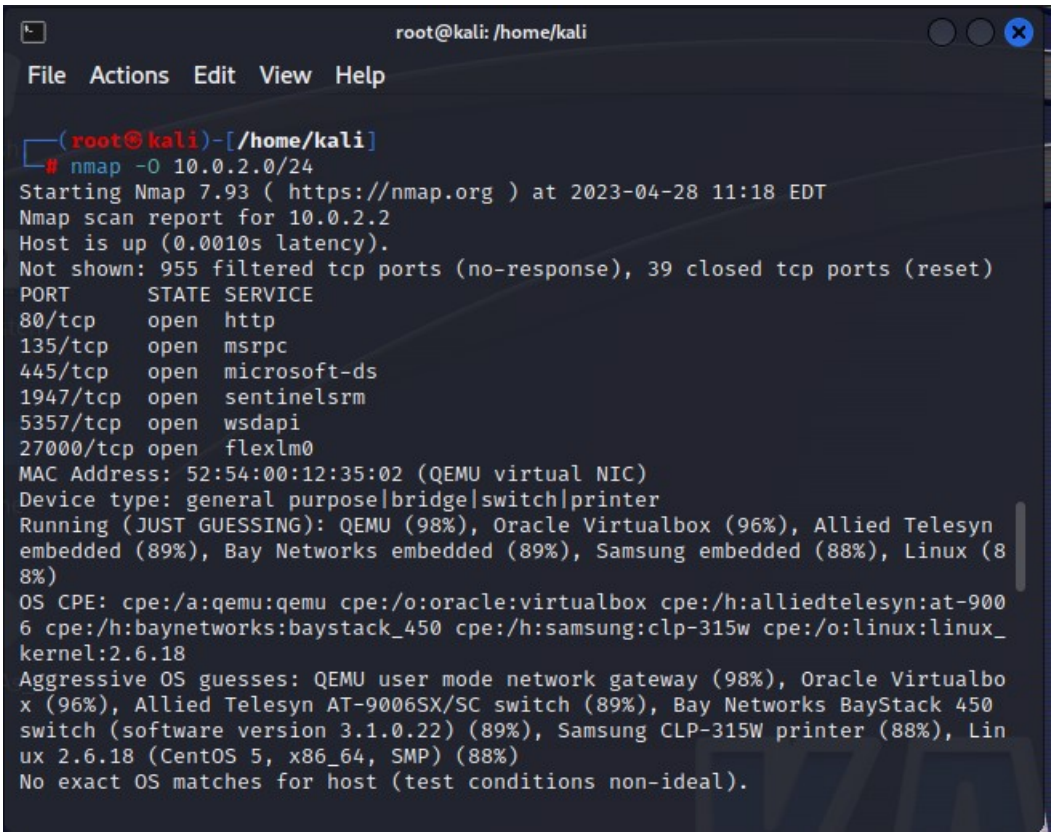

Figura D.1: Uso de *Nmap* para obtener información de posibles objetivos

Luego de tener la lista de objetivos para realizar el *pentesting*, se procede a usar la herramienta *Nexpose*. Se necesita crear un sitio, tal como se muestra en la Figura D.2, luego de asignarle un nombre y grado de importancia, se ingresan las direcciones IP de los objetivos a los cuales se les hará el *pentesting*, este paso se observa en la Figura D.3, por último se selecciona la plantilla (tipo) de escaneo, seleccionando la plantilla completa tal como se aprecia en la Figura D.4.

Una vez realizados estos pasos se procede a guardar el sitio y se selecciona la opción *SCAN*, dando inicio al *pentesting* desplegándose una pantalla igual a la Figura D.5, en la cual se describe el número de objetivos, vulnerabilidades, avance del proceso, etc.

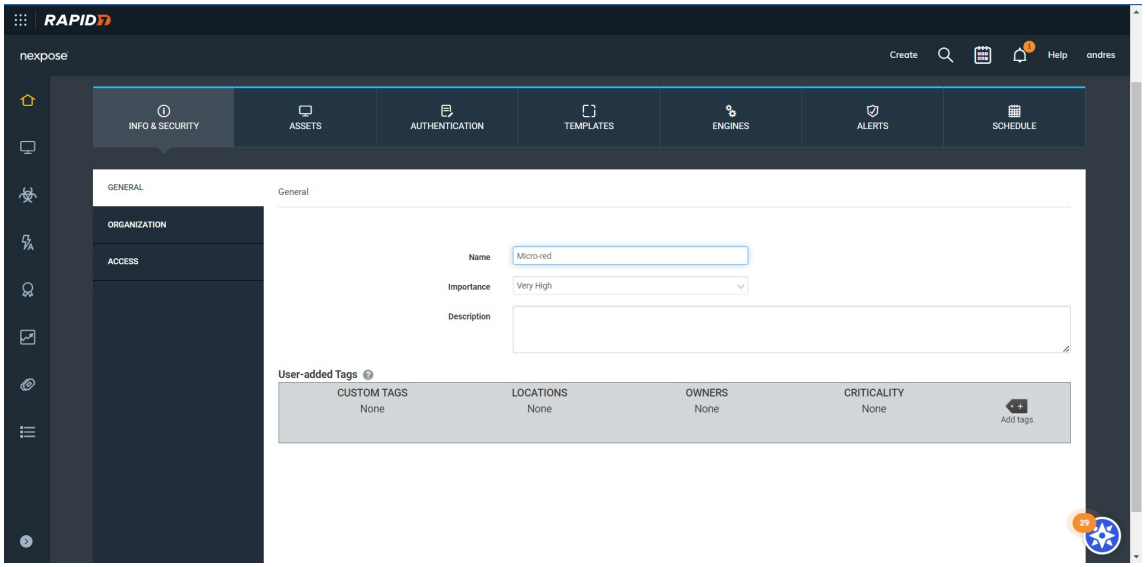

Figura D.2: Creación del sitio al que se le va a realizar el pentesting

Figura D.3: Ingreso de direcciones IP de los objetivos

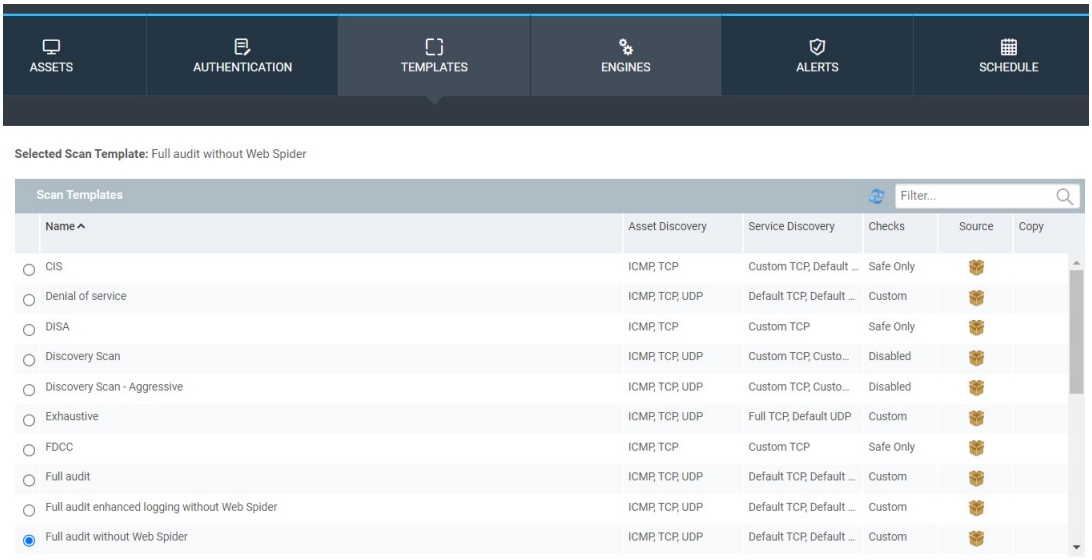

Figura D.4: Selección de la plantilla de escaneo

Conforme el proceso avanza, los resultados de algunos objetivos se mostrarán en la parte baja de la pantalla, similar a lo observado en la Figura D.6.

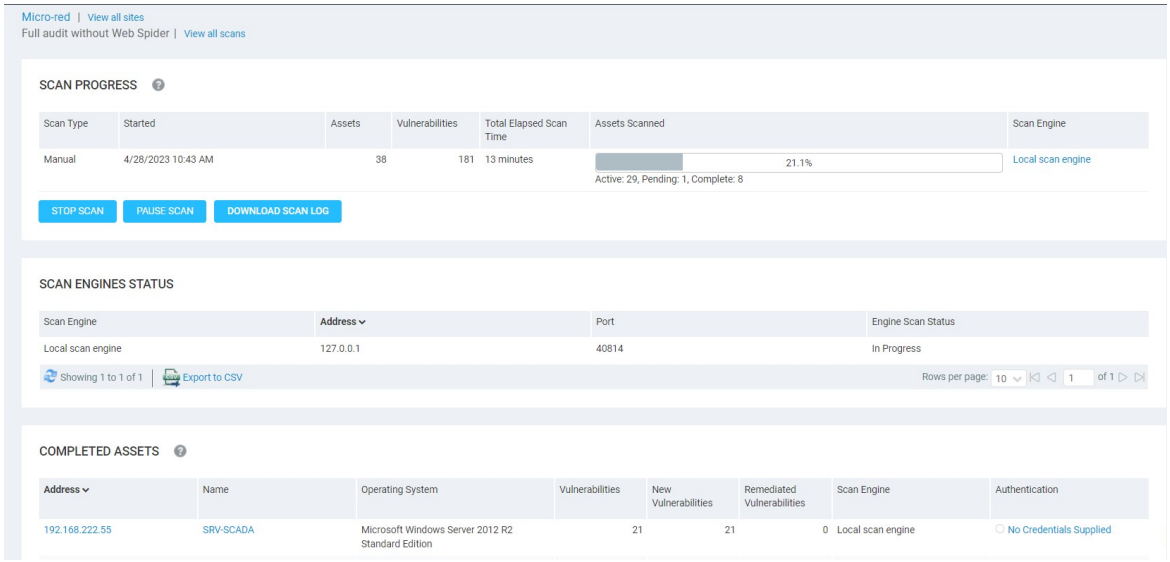

Figura D.5: Proceso de pentesting a los objetivos ingresados

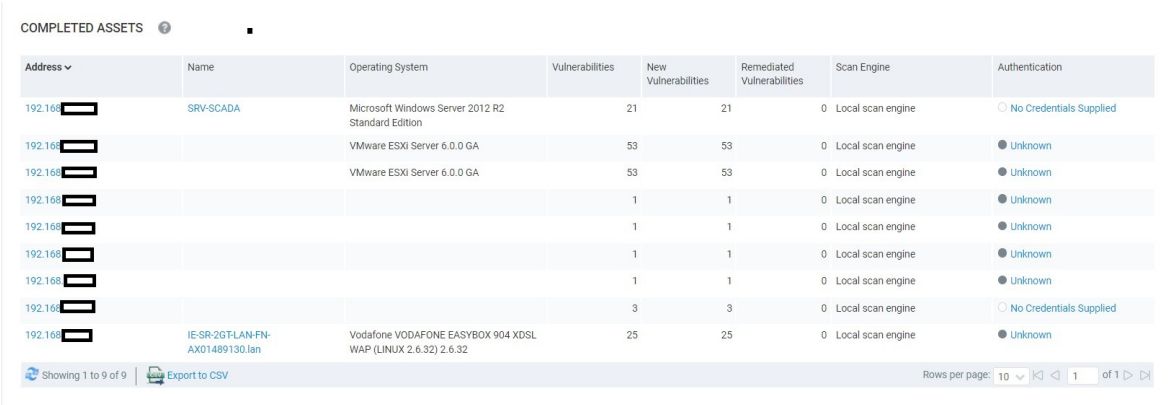

Figura D.6: Información de las pruebas finalizadas de algunos objetivos

Cuando se termine de realizar las pruebas en todos los objetivos se mostrará la información del total de vulnerabilidades encontradas y dispositivos escaneados tal como se muestra en la figura D.7. Se obtiene información sobre cada uno de los activos escaneados, el número de vulnerabilidades encontradas y el nivel de riesgo de cada una de estas.

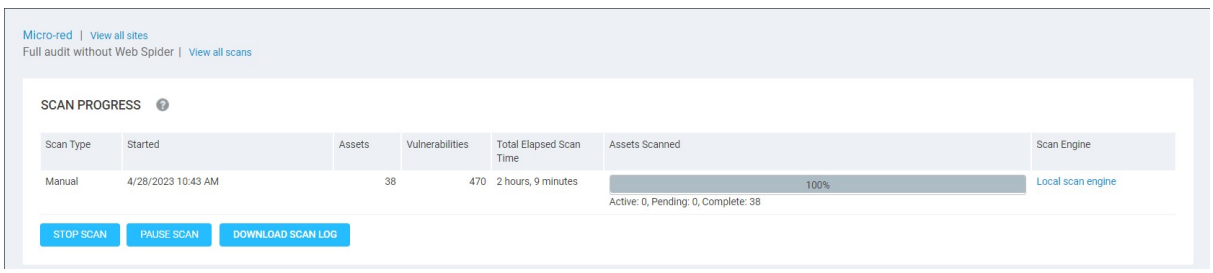

Figura D.7: Terminación del pentesting a los activos de la micro-red de la Universidad de Cuenca

El programa cataloga la severidad de cada una de estas, además que da una descripción de la vulnerabilidad, ya sea puertos abiertos o falta de mecanismos de seguridad en estos, entre otros. Con esta información se puede categorizar las vulnerabilidades según su tipo y su nivel de riesgo.

A continuación, en la Tabla D.1 se lista los activos de la micro-red con los respectivos nombres y notas con los que trabaja internamente la Universidad de Cuenca.

Tabla D.1: Activos a los que se realizó pentesting

ID Activo	Nombre	Equipo	Nota
1	Router		Router Micro-red
2	AR1		Analizador de red
3	AR4	Lab. Microred_15kw	Analizador de red
4	AR5	Vehículo eléctrico	Analizador de red
5	AR6	Servicio aux. 15kw	Analizador de red
6	APIS_1_FV	API Fotovoltaica/ Ethernet 1	Comm PLC-SCADA
7	CP.1	Carga programable	Modbus TCP
8	APIS_2_ALM_PLC_1	Api almacenamiento/ Bat. plomo/ Ethernet 1	Comm PLC-SCADA
9	APIS_2_ALM_PLC_2	Api almacenamiento/ Bat. litio/ Ethernet 1	Comm PLC-SCADA
10	APIS_2_ALM_PLC_3	Api almacenamiento/ Redox/ Ethernet 1	Comm PLC-SCADA
11	APIS_2_ALM_PLC_4	Api almacenamiento/ Supercap/ Ethernet 1	Comm PLC-SCADA
12	API_3_gen	Api generación/ Ethernet 1	Comm PLC-SCADA
13	UPS.1	UPS	
14	APIS_1_Switch	Switch gestionable	
15	PPC	Automata Siemens	Comm PPC-SCADA
16	APIS_2_Switch	Switch gestionable	
17	APIS_3_Switch	Switch gestionable	

18	APIS_5_Switch	Switch gestionable	
19	Cuadro Switch	Switch gestionable	
20	SCADA Switch	Switch gestionable	
21	APIS5_SH_Magelis		
22	APIS1_FV_Magelis		
23	APIS2_ALM_Magelis		
24	APIS3_GE_Magelis		
25	ISC.1_SWPEM	Inversor super-condensadores PV30	Comm PLC-Equipo/ Moxa Nport 5250
26	IPB.1_SWPEM	Inversor batería plomo PV50	Comm PLC-Equipo/ Moxa Nport 5250
27	ILI.1_SWPEM	Inversor batería ion litio PV80	Comm PLC-Equipo/ Moxa Nport 5250
28	IFV.1	Inversor fotovoltaico Mono. PV30	Comm PLC-Equipo/ Moxa Nport 5250
29	IFV.2_sFoto		Comm PLC-Equipo/ Moxa Nport 5150
30	IFV.1_sFoto		Comm PLC-Equipo/ Moxa Nport 5110
31	FP.1	Fuente programable	Comm SW sFoto/ Moxa Nport 5110
32	Servidor		Servidor que contiene la máquina virtual SCADA
33	Servidor		
34	Servidor		
35	Servidor		
36	Torre micro-red	Torre visualización SCADA	
37	SRV-SCADA		Máquina virtual que aloja el SCADA

38	Access Point		Enlace permanente con la interfaz inalámbrica, uso exclusivo de la micro-red