UNIVERSIDAD
NACIONAL
DE COLOMBIA

Análisis de Vulnerabilidad en Arquitecturas de Comunicación en Subestaciones

Rafael Jaime SantaMaría Isaza – Ingeniero de Control

Universidad Nacional de Colombia

Facultad de Minas

Medellín, Antioquia, Colombia

2017

Análisis de Vulnerabilidad en Arquitecturas de Comunicación en Subestaciones

Rafael Jaime SantaMaría Isaza – Ingeniero de Control

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Ingeniería: Automatización Industrial

Director (a): German Dario Zapata Madrigal

Doctor en Ciencias Aplicadas de la Universidad de los Andes (Venezuela)

Línea de Investigación:

Comunicaciones en Sistemas Eléctricos

Grupo de Investigación:

Grupo T&T

Universidad Nacional de Colombia

Facultad de Minas, Departamento de Energía Eléctrica y Automática

Medellín, Colombia

2017

A mis padres y familia que siempre me apoyaron, creyeron en mí y me dieron mis bases morales. A mi profesor German Zapata que bajo su dirección me dio las herramientas y el apoyo con la posibilidad de trabajar en el laboratorio IEC 61850. A mi facultad que me forjó bajo su lema, trabajo y rectitud.

"El sabio no actúa para acumular, cuanto más entrega a los demás cuanto más posee para sí. Cuanto más dones ofrece a los demás, tanto más consigue para sí."

Lao-Tse

Resumen

En el presente trabajo se propuso un procedimiento aplicable a arquitecturas de comunicación en subestaciones digitales y permite construir modelos de gráficos de ataque para análisis de vulnerabilidades. En la investigación se utilizaron herramientas de redes de comunicaciones convencionales para test de penetración con un enfoque de prueba especializado para subestaciones digitales. Inicialmente se abordó el problema entorno a la necesidad de procedimientos y modelos que permitan cuantificar la vulnerabilidad dentro de una subestación debido a su alto impacto y criticidad. Una vez planteado el problema se formularon objetivos, alcance, metodología, marco teórico y estado del arte. Teniendo claras las bases de la investigación, fue posible proponer un paso a paso para construir un modelo de gráfico de ataque aplicable a subestaciones digitales para análisis de vulnerabilidades. Se realizaron pruebas en el laboratorio IEC 61850 de la Universidad Nacional a una arquitectura de prueba, en la cual se incluyeron los equipos de mayor importancia en una subestación digital. Finalmente todos los resultados fueron analizados mediante la teoría de estados prohibidos del autómata Büchi, permitiendo la construcción del modelo. Por último se validó la hipótesis, logrando exitosamente un ataque asociado a la vulnerabilidad más crítica, la cual fue detectada en la arquitectura utilizando el modelo propuesto.

Palabras clave: Seguridad Cibernética, Subestación Digital, Arquitectura de Comunicación, Vulnerabilidad, Gráficos de Ataque, Pruebas de Penetración, TIC (Tecnologías de la Información y Comunicaciones)

Abstract

In the present work, a procedure applicable to communication architectures in digital substations was proposed and allows to build attack graph models for vulnerability analysis. In the research, conventional communications network tools were used for penetration tests with a specialized test approach for digital substations. Initially the problem was addressed around the need of procedures and models that allow to quantify the vulnerability within a substation due to its high impact and criticality. Once the problem was raised, objectives, scope, methodology, theoretical framework and state of the art were formulated. Having clear the bases of the investigation, it was possible to propose a step by step to build an attack graph model applicable to digital substations for vulnerability analysis. Tests were conducted in the IEC 61850 laboratory of the National University to a typical communications architecture, in which the most important equipment in a digital substation was included. Finally all the results were analyzed by the theory of prohibited states of the Büchi automaton, allowing the construction of the model. Finally, the hypothesis was validated, successfully achieving an attack associated with the most critical vulnerability detected in the architecture.

Keywords: Cyber Security, Digital Substation, Communication Architecture, Vulnerability, Attack Graphics, Pentesting, ICT (Information and Communication Technologies).

Contenido

Pág.

INTRODUCCIÓN 13

1. PLANTEAMIENTO DEL PROBLEMA 14
1.1 Justificación 15

2. OBJETIVOS 17
2.1 OBJETIVO GENERAL 17
2.2 OBJETIVOS ESPECÍFICOS 17

3. ALCANCE Y METODOLOGÍA 18
3.1 HIPÓTESIS 19
3.1.1 Métricas de la Hipótesis 19

4. ESTADO DEL ARTE 21

5. MARCO TEÓRICO 24
5.1 Modelado del Gráfico de Ataque 27
5.1.1 Automata de Büchi 28
5.2 IEC 62351 29
5.2.1 Listado de Parámetros IEC 62351 30

6. Propuesta 32
6.1 Mapa Conceptual 32
6.2 Elaboración del Gráficos de Ataque 34
6.3 Procedimiento de Modelado Propuesto 36
6.4 Listado de Herramientas y Propuesta de Aplicación 37
6.5 Asignación de Importancia Relativa 38
6.6 Síntesis de Resultados de Prueba 38
6.7 Ponderación de Métricas 39
6.8 Resultados Esperados 39

7. Resultados 41
7.1 Arquitectura de Prueba 41
7.2 Equipos 42
7.3 Clasificación de Recursos de Red e Importancia Relativa 42
7.3.1 Gateway 42
7.3.2 IED 43
7.3.3 Merging Unit 43
7.3.4 Reloj GPS 43
7.3.5 Equipo de Comunicaciones 44
7.3.6 Tabla de Clasificación de Equipos 44
7.4 Identificación de Segmentos de Red 47
7.5 Identificación de Amenazas 49
7.6 Análisis de Registros de Prueba 50
7.7 Análisis de Métricas 51
7.8 Gráfico de Ataque 53
7.8.2 Conjuntos de Büchi 53

7.8.3 Interpretación 54
7.8.4 Resultados Finales 56
7.9 Validación de la Hipótesis 57

8 Conclusiones 60

9 Recomendaciones 61

10 BIBLIOGRAFIA 62

Lista de figuras

Pág.

Figura 1. Ataque a mensajes *Multicast* en un Switch [2]. 25
Figura 2. Arquitectura de Comunicaciones entre dos Subestaciones [2]. 26
Figura 3. Suite de Protocolos y Modelo de Datos del Estándar IEC 61850 [15]. 27
Figura 4. Mapa de Aplicación del Estándar IEC 62351 [9]. 30
Figura 5.Mapa Conceptual Sobre IEC 62351 [Fuente: Elaboración Propia]. 33
Figura 6. Metodología de Mapa de Ataque para Análisis de Vulnerabilidad [16]. 34
Figura 7. Arquitectura Bajo Prueba de Penetración [Fuente: Elaboración Propia]. 41
Figura 8. Netdiscover para Arquitectura Bajo Prueba [Fuente: Elaboración propia a partir de Software Netdiscover]. 47
Figura 9. Topología creada con Zenmap (interfaz gráfica Nmap) luego del análisis a IPs Objetivos [Fuente: Elaboración propia usando Zenmap]. 49
Figura 10. Resultados de Zenmap para IP del Switch [Fuente: Elaboración propia usando Zenmap]. 50
Figura 11. Gráfico de Ataque de Arquitectura Bajo Prueba [Fuente Propia]. 55
Figura 12. Gráfico de Ataque Simplificado para Validación. 58
Figura 13. Captura de Ingreso con contraseña correcta para identificación de campo de acceso. 58
Figura 14. Contraseña correcta encriptada y campo de autorización. 59

Lista de tablas

Pág.

Tabla 1. Lista de latencia máxima permitida para múltiples tipos de datos [9]. 19
Tabla 2. Características y Medidas de Seguridad SV, GOOSE, MMS [9]. 31
Tabla 3. Lista de Herramientas y Posible Aplicación en Subestaciones [Fuente: Elaboración propia]. 37
Tabla 4. Clasificación de Recursos de Red e Importancia Relativa [Fuente: Elaboración Propia]. 45
Tabla 5.Identificación de Segmentos de Red y Posibles Riesgos [Fuente: Elaboración Propia]. 48
Tabla 6. Análisis de Métricas en Registros Zenmap [Fuente: Elaboración Propia]. 50
Tabla 7. Análisis de Disponibilidad, Integridad y Confidencialidad [Fuente: Elaboración Propia]. 52
Tabla 8. Recomendaciones para Mitigación de Riesgos. 56
Tabla 9. Des-encriptada de clave correcta para suplantación. 59

INTRODUCCIÓN

Esta investigación se centró en la seguridad cibernética de las subestaciones digitales. A pesar de contar con soluciones existentes de seguridad, no era posible probar su correcta implementación y eficacia. Por lo tanto, fue propuesto un procedimiento para obtener modelos y métricas mediante el uso de herramientas de las TIC, teniendo en cuenta los conceptos de seguridad cibernética para subestaciones digitales planteados en el estándar IEC 62351.

Los ataques cibernéticos tienen un alto impacto en las subestaciones digitales, además los altos requisitos de desempeño en los protocolos *multicast* dificulta asegurar los recursos cibernéticos. Se han identificado varios ataques a nivel mundial en los últimos años, evidenciando vulnerabilidades en subestaciones digitales. A pesar de contar con diversas medidas para asegurar estos sistemas, es necesario ajustar los requerimientos de seguridad a los de desempeño y otros factores relevantes en la subestación.

Para lograr el nivel deseado de seguridad sin afectar los demás requerimientos de la subestación, se requieren modelos que permitan evaluar los riesgos asociados a las diferentes vulnerabilidades presentes en el sistema. A pesar de que en la literatura existen varios métodos para el desarrollo de estos modelos, no se han aplicado anteriormente a arquitecturas de comunicación de subestaciones digitales. Entre los métodos disponibles se seleccionan los gráficos de ataque como una alternativa aplicable a subestaciones digitales. Para la construcción del gráfico se propone utilizar la metodología del Autómata Büchi, teniendo en cuenta las recomendaciones planteados en el estándar IEC 62351. De este modo fue posible definir un procedimiento que permite modelar una arquitectura de una subestación digital en gráficos de ataque.

Una vez desarrollada la base de la investigación (problema, objetivos, estado del arte), se utilizó el mapa conceptual como herramienta de síntesis. De este modo fue posible relacionar las herramientas disponibles con las propuestas descritas en el estándar IEC 62351. Luego se propuso un paso a paso para la construcción del gráfico, estableciendo las consideraciones necesarias en cada paso.

Por último se aplicó la metodología propuesta a una arquitectura de prueba en el servicio de laboratorio IEC 61850 que ofrece el Grupo T&T la Universidad Nacional de Colombia. Los pasos a seguir fueron los siguientes: clasificación de equipos, detección de direcciones IP, escaneo intenso de puertos, síntesis de resultados, ponderación de métricas, análisis de riesgos y construcción del gráfico. Además se realizó una validación del modelo obtenido realizando un ataque a la vulnerabilidad más crítica detectada.

1. PLANTEAMIENTO DEL PROBLEMA

Debido a los *bugs* (errores de software o agujeros de seguridad) en los protocolos y su alto impacto en los equipos finales, la subestación digital se ha convertido en un objetivo prioritario para los ataques maliciosos de seguridad. Consecuentemente se crea la necesidad de encontrar alternativas para la solución a esta problemática [1].

Aunque muchas tecnologías de seguridad para los sistemas TIC tradicionales disponibles, con frecuencia no son utilizables o deben ser ajustadas en cuanto a su aplicación en subestaciones digitales, principalmente debido a requerimientos de desempeño. Por lo tanto, se deben explorar nuevos enfoques para estas tecnologías [2]. Además, la seguridad debe abordarse desde una perspectiva cibernética, analizando no solo los sistemas físicos de la red de energía, sino también los sistemas digitales. Estos también tienen riesgos que deben adaptarse a todos los enfoques de la seguridad.

Debido a la reciente adopción de tecnologías para digitalización de subestaciones y la modernización de implementaciones existentes, se requieren procedimientos de prueba para construir modelos que permitan el análisis de vulnerabilidades. Es necesario verificar el cumplimiento de las especificaciones técnicas de seguridad cibernética, sin afectar los requerimientos de las protecciones. Estos procedimientos pueden ser aplicados en el laboratorio IEC 61850 de la Universidad Nacional y servirán para realizar servicios de prueba, respondiendo a las necesidades del sector eléctrico y garantizando el cumplimiento de los requisitos técnicos reglamentados por la regulación o exigidos en una contratación.

Algunos de los requisitos principales de seguridad cibernética para la infraestructura crítica se describen en los acuerdos del Consejo Nacional de Operación (CNO). Existen dos acuerdos para las comunicaciones para infraestructura crítica (la cual aplica para las comunicaciones dentro de la subestación), la CNO 788 y la CNO 701. Esta normativa exige y específica las condiciones mínimas de seguridad que debe cumplirse por parte de las empresas del sector eléctrico en su infraestructura crítica.

- El Acuerdo CNO 788, documenta los lineamientos para la Ciber-seguridad necesarios para Colombia. El Documento, realiza un estudio para determinar las normas aplicables a las empresas eléctricas en cuanto a protección de datos, con el fin de mitigar el impacto sobre el Sistema Interconectado Nacional [3].
- El CNO 701 establece “Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas”. Por lo tanto, aplica para las funciones de control y tele-gestión

implementadas en las redes de comunicaciones dentro de las subestaciones eléctricas [4].

Las exigencias de los acuerdos presentan un gran reto para las comunicaciones e implica la necesidad de adoptar tecnologías de seguridad cibernética. La IEC 62351 propone herramientas y configuraciones que permiten obtener las medidas mínimas exigidas por la regulación. Sin embargo, es necesario realizar pruebas para validar su funcionamiento. Se requieren procedimientos de prueba para verificar aspectos de la CNO 701, CNO 708, IEC 62351 y evaluar la vulnerabilidad en cuanto a seguridad cibernética en una subestación digital. Además se evidencia la carencia de procedimientos de pruebas.

1.1 Justificación

La relación del sistema cibernético y el proceso físico en un sistema de automatización de subestaciones, permite que incidentes cibernéticos deliberados o inadvertidos, tengan el potencial de causar implicaciones físicas. Por lo tanto, es impráctico comprender el impacto de los incidentes cibernéticos basados exclusivamente en teorías de TI. Cada subestación depende en gran medida de flujos de datos eficientes y fiables para mantener la observabilidad y controlabilidad del proceso físico, mientras que los flujos de datos con retrasos o alterados pueden obstaculizar el buen funcionamiento de los dispositivos de campo.

En teoría, si no se toman las medidas preventivas, un atacante puede acceder de forma remota en un sistema cibernético de una subestación, elevar sus privilegios y realizar acciones no autorizadas para bloquear o manipular los flujos de datos; de este modo las operaciones no son observables, por ende incontrolables, poniendo en peligro la estabilidad, seguridad o eficiencia de las fuentes de alimentación [5].

En el 2017 se han tenido incidentes graves de seguridad cibernética a nivel mundial, según el reporte de daños de *ramsomware* de *Cybersecurity Ventures* [6]; los costos globales por daños de *ransomware* superan los US $ 5 mil millones. Se encontraron reportes en todo tipo de redes corporativas que podrían aplicarse al entorno industrial. El número de ataques de *ransomware* contra las empresas se triplicó el año pasado, saltando de un ataque cada dos minutos en el primer trimestre a uno cada 40 segundos en el tercer trimestre [6]. La aceleración de los ataques contra las empresas indica que más y más criminales están desarrollando campañas específicas y fijando sus miras en puntuaciones más grandes. En cuanto a la infraestructura crítica, se han presentado varias amenazas que han infectado diferentes sistemas a nivel mundial, como Stuxnet (2010), Industroyer(2015), Crash Override (2016), entre otros.

El incidente Stuxnet (2010) es un claro ejemplo de ataques que resultaron en graves consecuencias físicas. Los atacantes indujeron exitosamente vibraciones o distorsiones

excesivas para destruir el sistema de centrifugado rápido, retransmitieron al controlador mediciones erróneas de manera constante y burlaron los sistemas de alarma haciéndolo indetectable hasta ser catastrófico. En primer lugar, se dirigió a las máquinas y redes de equipos Windows, replicándose repetidamente a sí mismo y actualizándose al encontrar conexiones a internet. Luego buscó el software Siemens Step7 de Windows, el cual permite programar sistemas de control industrial. En Step 7 operaban equipos finales, en este caso las centrífugas. El virus puede comprometer los controladores lógicos programables enviando comandos en falso e interviniendo en las señales del SCADA [7].

Otro ejemplo de las consecuencias de los agujeros de seguridad, es el del código malicioso Industroyer; en Diciembre de 2015 la red eléctrica de Ucrania sufrió un ataque cibernético, sectores de Kiev fueron sometidos a la oscuridad total [8]. Fue el primer caso conocido de malware diseñado específicamente para los sistemas de red eléctrica y la segunda pieza de malware descubierto capaz de interrumpir procesos industriales sin la necesidad de intervenir manualmente (el primero fue Stuxnet). Un año después (Diciembre 2016) se repitió el mismo ataque con una actualización llamada *Crash Override*. Cuando penetra en un sistema de red eléctrica, utiliza los mismos protocolos de los sistemas; sin embargo, no tiene propósito de espionaje, y está diseñado únicamente con el fin de destruir. Una vez toma el control puede iniciar sus propios comandos controlando la red para encender o apagar líneas de subestación. El malware se reproduce y se modifica con facilidad; por lo tanto, podría dirigirse a otra infraestructura crítica como proveedores de transporte, agua y gas [8].

Finalmente, luego de analizar los incidentes cibernéticos alrededor del mundo, se hacen evidentes los riesgos incurridos al carecer de medidas de seguridad. Además de contar con estas medidas también es necesario un procedimiento de prueba como mecanismo de refuerzo y consolidación de las prácticas de seguridad para subestaciones digitales.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

- Proponer una metodología de prueba para el análisis de vulnerabilidad en una arquitectura típica de comunicaciones para automatización de subestaciones bajo el estándar IEC 61850.

2.2 OBJETIVOS ESPECÍFICOS

a) Identificar los conceptos y técnicas planteadas en el estándar IEC 62351 para seguridad cibernética en subestaciones, relacionadas con el análisis de vulnerabilidad de la infraestructura de redes de datos en dichas instalaciones.

b) Estructurar los procedimientos necesarios para medir o establecer el nivel de vulnerabilidad y desempeño de una arquitectura típica de comunicaciones para automatización de subestaciones bajo el estándar IEC 61850.

c) Aplicar los procedimientos planteados a una arquitectura de prueba obteniendo los registros necesarios de las vulnerabilidades detectadas para construir el modelo.

d) Construir el modelo en gráfico de ataque para una subestación bajo prueba a partir de los resultados obtenidos aplicando el procedimiento planteado anteriormente, además validar la vulnerabilidad más crítica detectada.

3. ALCANCE Y METODOLOGÍA

Para cumplir los objetivos fue necesario establecer estrategias metodológicas, a través de las cuales se llegó a un procedimiento de prueba para el análisis de vulnerabilidad en una subestación digital. A continuación se listan las metodologías que fueron necesarias y permitieron cumplir lo planteado anteriormente:

a) Mapa Conceptual IEC 62351:

Con el fin de cumplir el primer objetivo en el cual se analizaron los conceptos y técnicas planteadas en el estándar IEC 62351, se utilizó como mecanismo de síntesis la elaboración de un mapa conceptual. Este permitió categorizar, priorizar y evaluar los aspectos más relevantes del estándar para la investigación.

b) Procedimiento de Prueba Propuesto:

Inicialmente se listan las herramientas a utilizar, identificando su aplicación en subestaciones digitales. Teniendo definidas las herramientas, se propuso una secuencia de pasos estructurada para lograr obtener los modelos.

c) Resultados de Prueba

Una vez aplicados los procedimientos de prueba propuestos, se tomaron los registros de las herramientas utilizadas para su posterior análisis. Luego se sintetizaron los resultados mediante un modelo de gráficos de ataques.

d) Medios de Verificación:

Por último se cuantifica el nivel de vulnerabilidad correspondiente al modelo de la subestación bajo prueba. Se valida el modelo verificando la vulnerabilidad más crítica detectada.

3.1 HIPÓTESIS

A partir de un procedimiento de prueba, es posible modelar, medir o estimar el nivel de vulnerabilidad presente en una arquitectura de comunicaciones de una subestación digital.

3.1.1Métricas de la Hipótesis

Con el fin de validar la hipótesis, se plantean unas métricas cuantitativas, estas se ponderan específicamente en cuanto a la seguridad cibernética. Existen tres requisitos fundamentales de seguridad, las redes deben cumplir los siguientes atributos [3]:

•Disponibilidad:

Los datos son accesibles y oportunos, el acceso continuo a los datos es necesario para tomar decisiones operativas y adaptarse rápidamente a condiciones dinámicas en circunstancias críticas. Debido a la naturaleza temporal de los datos, cualquier latencia o pérdida de sincronización puede obstaculizar la conciencia de la situación y afectar el rendimiento operativo de los esquemas de protección. A continuación en la Tabla 1 se listan los requerimientos de disponibilidad para cada tipo de dato.

Tabla 1. Lista de latencia máxima permitida para múltiples tipos de datos [9].

Tipo de Dato	Latencia Máxima
Relé de Protección	<4ms
Unidades de Medición Fasorial (PMUs)	<1 Segundo
Control, Supervisión y Adquisición de Datos	Segundos
Gestión de energía	Minutos
Medición Inteligente	Horas

• Integridad:

Los datos son confiables y precisos, la autenticidad y la coherencia de los datos deben conservarse durante todo su ciclo de vida. Cualquier alteración de datos por partes no autorizadas debe ser frustrada; de lo contrario, es posible ser víctima de un ataque, incurriendo en efectos adversos sobre las funcionalidades del esquema de protección.

• Confidencialidad:

Los datos están accesibles y comprensibles únicamente para agentes autorizados. Cualquier acceso no autorizado puede revelar información sensible y confidencial, trayendo consecuencias en las operaciones de la red eléctrica.

Los requisitos de seguridad cibernética mencionados anteriormente se diferencian de los del dominio tradicional de la tecnología de la información (TI). La seguridad de TI se enfoca principalmente en garantizar el anonimato y la confidencialidad para preservar la privacidad del usuario; mientras que la seguridad cibernética en subestaciones, se enfoca en mantener la calidad de la energía suministrada, garantizando la continuidad y funcionalidad de los esquemas de protección. Por consiguiente, la disponibilidad y la integridad suelen priorizarse sobre la confidencialidad a fin de mantener flujos de datos oportunos y fiables para las aplicaciones autorizadas que rigen las operaciones de los esquemas de protección [5].

4. ESTADO DEL ARTE

Actualmente los sistemas modernos de automatización de subestaciones basados en el estándar IEC 61850 son ampliamente aceptados como alternativa tecnológica para proveer infraestructura de redes inteligentes en los sistemas de transmisión [10]. Su principal característica consiste en aprovechar los modelos de datos orientados a objetos de la tecnología Ethernet de manera estandarizada, logrando funciones de interoperabilidad avanzadas y cumpliendo con requerimientos de tiempos críticos de los sistemas de potencia. Adicionalmente la tecnología Ethernet también aporta menores costos de configuración y mantenimiento [11].

Las comunicaciones en las redes inteligentes deben ser fiables, flexibles, eficientes y seguras. A pesar de que el estándar IEC 61850 ofrece grandes beneficios, investigaciones recientes confirman que no cumple requisitos de seguridad cibernética [2]. La reducción de la complejidad del modelo de comunicaciones para los protocolos *multicast* GOOSE y SV representa riesgos de seguridad cibernética [5]. En estos protocolos, es posible obtener el desempeño deseado; sin embargo, se crean grandes retos, ya que al tener menos capas en el modelo de comunicación se facilitan los ataques cibernéticos.

Un ataque cibernético que afecte los sistemas de automatización de una subestación podría tener un impacto importante en la red eléctrica. Ya se han hecho antes algunas investigaciones que analizan los riesgos de seguridad de una subestación como un riesgo potencial [12]. Además, incidentes con malware como Industroyer, han demostrado que los ataques a los relés podrían causar inestabilidad a los generadores y el voltaje de la red; una muestra clara, fue el apagón de la red eléctrica Ucraniana el 23 de Diciembre del 2015 [8].Un vector de ataque es un camino que los atacantes pueden tomar para ganar acceso al sistema cibernético. Utilizando un vector de ataque los atacantes pueden obtener acceso no autorizado, comprometiendo directamente el sistema. Por ejemplo, los dispositivos de red a menudo son instalados con su configuración por defecto, incluyendo credenciales comprometidas y disponibles en los manuales de fabricante en la web. Además, aunque se tengan credenciales fuertes con contraseñas encriptadas, estas pueden ser vulneradas con ataques de fuerza bruta. Otra vulnerabilidad radica en las tecnologías de comunicación inalámbrica; con una configuración y administración inadecuada se conceden vectores de ataque a agentes no autorizados.

Además de los ataques locales mencionados anteriormente, existen ataques remotos a través de *malware* denominado “Troyano” [13]. Un “Troyano” es un código malicioso que oculta su identidad dentro de un software, aplicativo o dispositivo de hardware para lograr evadir los perímetros de seguridad. Por ejemplo, permiten a los atacantes acceder a un sistema que haya sido infectado concediendo privilegios administrativos. BlackEnergy,

Havex y Sandworm son ejemplos recientes que se dirigen a los sistemas de monitoreo y control [13]. En general, un “Troyano” puede infectar una red cibernética utilizando las siguientes estrategias:

• Ataques de phishing: se utiliza información fraudulenta como correos electrónicos se encuentran diseñados para parecer auténticos. Los operadores podrían inadvertidamente abrir archivos adjuntos contaminados que permitirán que el “Troyano” sea instalado y ejecutado automáticamente.

• Hardware externo infectado. Medios extraíbles tales como unidades de memoria flash utilizadas para transferencias de archivos, pueden fácilmente reproducir y distribuir el *malware* contenido tan pronto como se conecta a la red.

• Redes externas infectadas. Existen diferentes códigos maliciosos que permiten infectar las redes contagiando cualquier equipo conectado a esta.

En general, existen algunas medidas de seguridad cibernética para mitigar el riesgo que pueden ser implementadas considerando las características de la red, al igual que las propiedades de dispositivos de hardware y aplicaciones de software. Las siguientes medidas generalmente son consideradas para mejorar la seguridad cibernética en una red [13]:

• Implementación de *firewalls*, *software* antivirus e intrusión sistemas de detección para defenderse del *malware.*

• Crear zonas desmilitarizadas para proporcionar seguridad.

• Usando conexiones cableadas dedicadas para aplicaciones críticas.

• Monitorear el acceso remoto y local a los críticos componentes cibernéticos.

• Habilitar la autenticación de múltiples factores para el acceso controlar.

•Deshabilitar componentes y aplicaciones innecesarios que potencialmente podrían agrandar la superficie de ataque.

• Adaptación de los protocolos de comunicación con mejoras en mecanismos de seguridad.

• Cifrar datos confidenciales con criptografía sofisticada.

• Arreglar los defectos en aplicaciones y sistemas operativos.

• Perfeccionar los planes de respuesta y recuperación de incidentes.

Los ataques cibernéticos aumentan su complejidad, haciendo necesario el uso de sistemas cibernéticos robustos contra intrusiones maliciosas y aplicaciones tolerantes a fallas para poder mantener la seguridad física en sistemas cibernéticos defectuosos. Debido a la necesidad de detectar riesgos potenciales y determinar si un sistema cibernético es defectuoso, se requieren procedimientos de prueba que permitan evaluar estos sistemas en cuanto a su nivel de seguridad cibernética.

El grupo internacional de usuarios UCA, conformado por miembros de las empresas de servicios públicos, proveedores, entre otros; trabaja en el tema de interoperabilidad en la infraestructura de empresas de servicios públicos específicamente, electricidad, gas y agua. Dentro de sus talleres y reuniones se han desarrollado diversos procedimientos de prueba para la gran mayoría de factores relevantes en una subestación digital. Sin embargo, hasta ahora no hay ningún procedimiento que permita analizar la vulnerabilidad de un sistema contra ataques cibernéticos en una subestación. La digitalización de las subestaciones en todo el mundo justifica la definición de los procedimientos de prueba para aspectos de seguridad cibernética [11].

Finalmente se concluye que anteriormente se han propuesto diferentes técnicas para la prevenir las ataques cibernéticos [13]; sin embargo, no existe un procedimiento para determinar la eficacia de estas técnicas o comparar su efecto en el nivel de seguridad de una subestación digital.

5. MARCO TEÓRICO

Los ataques DoS (*Denial of Service*) dan a los atacantes la oportunidad de envenenar la red con datos falsos para tomar decisiones operacionales. Los atacantes con acceso directo a dispositivos pueden incluso modificar la configuración de red (por ejemplo apagar puertos de comunicación) logrando consecuencias físicas en las operaciones de la subestación. Las mediciones de monitoreo y los comandos de control deben cumplir con estrictos requisitos de puntualidad, especialmente en condiciones de emergencia debido a la ocurrencia de eventos extremos. Por un lado, cualquier retraso o pérdida de información puede interferir con el esquema de protección de la subestación. En consecuencia, impide al sistema tomar decisiones operativas en tiempo real. Por ejemplo, la latencia de tiempo podría anular la función de protección de sobre-corriente direccional de un IED e impedir la mitigación de fallos locales, lo que conduce a la propagación de cortes de energía [2].

Ademas de los ataques DoS existen otros ataques conocidos.Entre los posibles ataques están los siguientes:

DoS: Ataque de negación de servicio, se presenta cuando algún puerto de vital importancia se encuentra abierto y en riesgo de ser vulnerado, de modo que un agente no autorizado puede negar el servicio a un agente autorizado de la red.

Sniffing: Un ataque de *sniffing* se da cuando se ve comprometida la confidencialidad de la red. Esto se presenta generalmente en puertos abiertos y canales no seguros con información en texto plano.

Spoofing: Un ataque de tipo *spoofing* se da cuando se encuentra comprometida la autenticación de un puerto de comunicaciones por malas configuraciones de seguridad. Este ataque permite a un agente no autorizado suplantar la identidad de un agente autorizado y modificar la información a su voluntad.

Cracking: Un ataque de tipo *cracking* se presenta cuando es posible romper contraseñas, comunicaciones encriptadas o demás mecanismos de seguridad dentro de uno de los canales de comunicación de los equipos.

En la Figura 1, se puede ver como un atacante inyecta paquetes maliciosos a la red a través de un equipo de comunicaciones. Cuando la configuración del sistema tiene vacíos en cuanto a seguridad cibernética o control de acceso, permite a un atacante acceder a la red. El atacante no solo podrá ver todo el tráfico, sino que también tendrá la posibilidad de enviar a la red réplicas modificadas de la información original. Una operación del sistema indeseada (controlada por agentes no autorizados) puede dejar el

sistema vulnerable y conceder control de las funciones de automatización de la subestación al atacante.

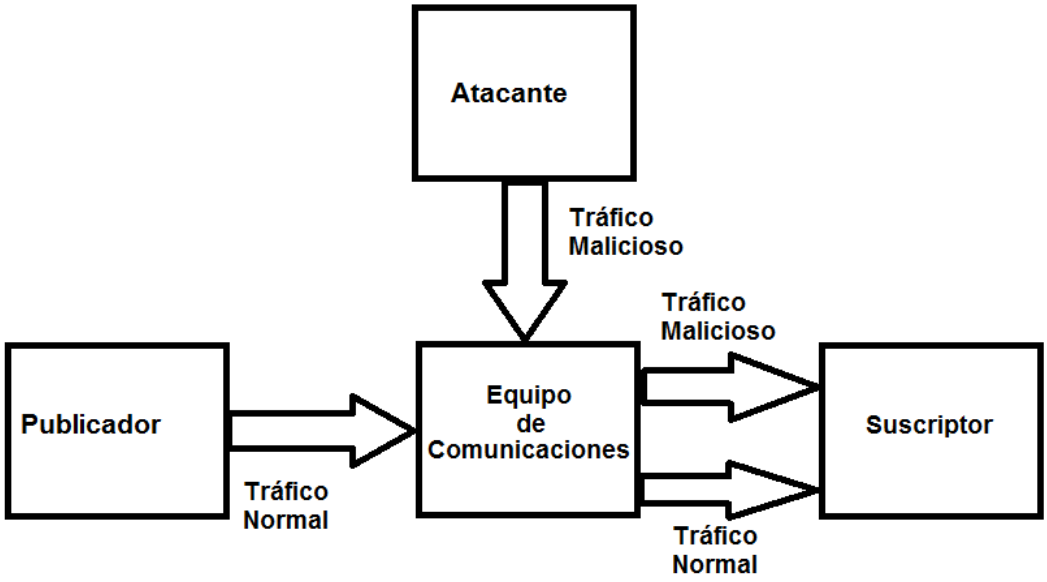


Figura 1. Ataque a mensajes *Multicast* en un Switch [2].

Los puntos más vulnerables de las arquitecturas de comunicaciones se encuentran en el bus de proceso, principalmente en los equipos de comunicaciones que transportan todos los datos intercambiados entre los IEDs [14]. El bus de proceso comunica los protocolos GOOSE y SV; ambos tienen requerimientos de desempeño en cuanto a tiempo de transporte muy exigentes, lo cual a su vez es lo que dificulta lograr un nivel de seguridad cibernética deseada.

En la Figura 2, se pueden ver claramente los puntos vulnerables en la arquitectura de comunicaciones de las subestaciones eléctricas basadas en el estándar IEC 61850. En la arquitectura se incluye la red WAN (*Wide Area Network*), a pesar de ser vulnerable ante malas configuraciones, tiene un nivel de seguridad mayor al bus de proceso; a diferencia de los protocolos *multicast*, el enrutamiento de protocolos TCP orientados a la conexión logra una comunicación segura entre subestaciones. El atacante intentará vulnerar el sistema a través de diferentes puntos débiles de la red en el bus de proceso, por ejemplo, podría acceder a través de puntos de acceso inalámbrico sin aislamiento entre la red del proceso y la red corporativa.

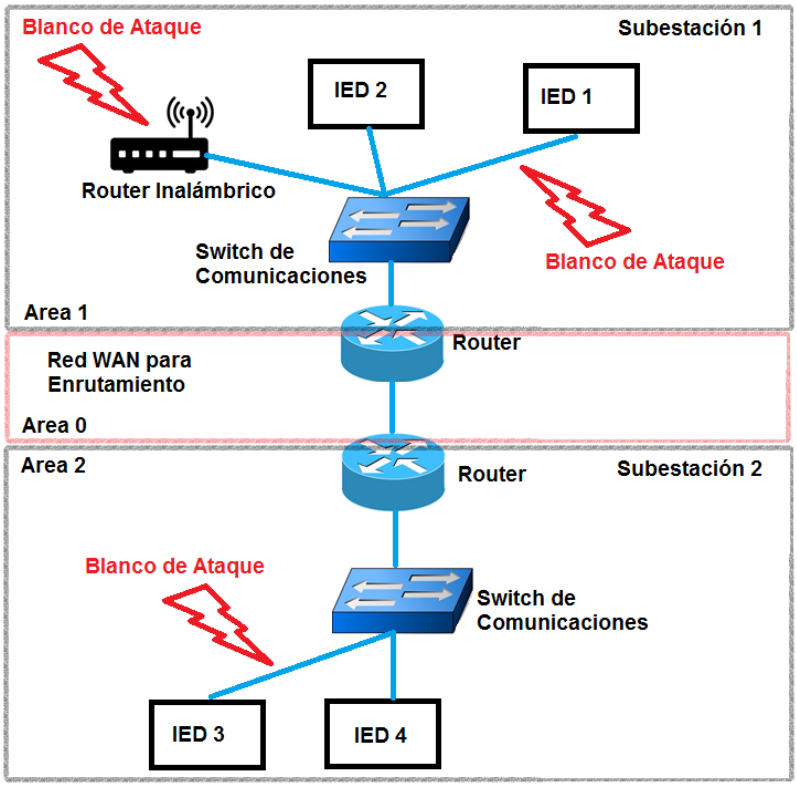


Figura 2. Arquitectura de Comunicaciones entre dos Subestaciones [2].

Existen diferentes niveles de prioridad dependiendo de las funciones y requisitos de desempeño de los protocolos de comunicación. La información operativa, como el estado y el control, es estandarizada y de prioridad media. La información de configuración, tales como transferencia de archivos y configuraciones cambiantes, es de baja prioridad. En cuanto a prioridad alta se tienen dos tipos de mensajes bajo condiciones estrictas en tiempo real, GOOSE y SV.

El primer tipo de mensaje contiene uno o unos pocos bits de información (de estados binarios, por ejemplo estado de interruptores, seccionadores, etc...) y es en su mayoría para el bloqueo, la liberación, el disparo, la indicación de la posición de conmutación en secuencias automáticas, enclavamiento, protección, así como para intercambios de datos entre dispositivos. Este tipo de mensajes se denomina mensajes GOOSE "*Generic Object Oriented Subestation Event*". El otro tipo de mensaje se denomina Valores Muestreados, SV (*Sampled Values*), utilizados para el envío de gran cantidad de flujo de datos analógicos tales como señales de corriente y tensión. En la Figura 3, se puede apreciar en la suite de protocolos del estándar que el protocolo GOOSE y SV pasa directamente a la capa de enlace de datos [15]. El hecho de tener un menor número de capas en el modelo de comunicaciones de los protocolos *multicast* representa grandes retos para la seguridad cibernética.

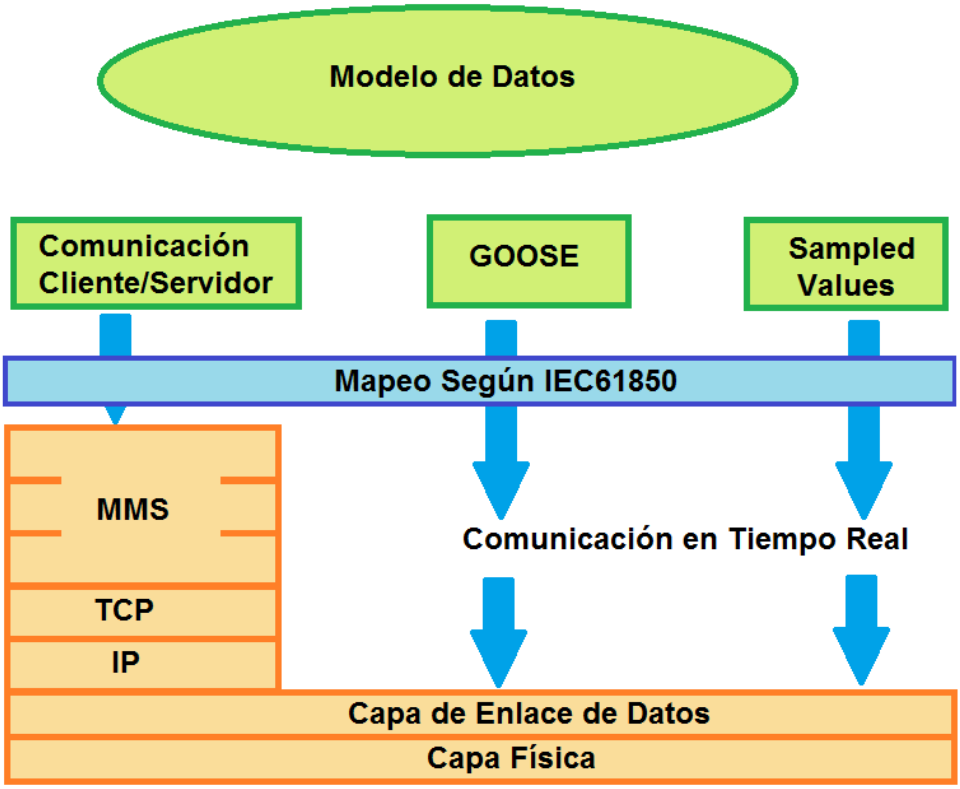


Figura 3. Suite de Protocolos y Modelo de Datos del Estándar IEC 61850 [15].

5.1 Modelado del Gráfico de Ataque

Los gráficos de ataque se han utilizado para modelar los sistemas y sus posibles vulnerabilidades. Es de gran interés identificar los ataques de mayor relevancia que conduzcan a una falla parcial o total de los sistemas. Una metodología útil para este análisis, es la construcción de gráficos de ataque del sistema, permitiendo el análisis para establecer estrategias de respuesta. Esto no solo proporciona la representación simplificada del sistema, sino que también permite priorizar las propiedades de seguridad cuyas violaciones son de mayor preocupación, tanto para la detección como para la reparación. Existen investigaciones que demuestran el potencial en el uso de gráficos de ataque para la caracterización de las métricas de seguridad [14]. La complejidad de los sistemas computacionales se gestiona creando modelos con diversos grados de detalle y asegurando las propiedades deseadas de esos modelos. Por lo tanto, a medida que los sistemas evolucionan, también lo hacen sus modelos y análisis.

Los sistemas y su comportamiento se modelan de modo que se puedan priorizar las propiedades de corrección importantes. Los recursos asignados a la seguridad

se deben gastar adecuadamente para localizar y solucionar las vulnerabilidades que violen las propiedades de alta prioridad. El modelado debe facilitar una representación natural de ejecuciones. Un ataque exitoso llevará al sistema a estados no deseados.

El modelado necesita facilitar una representación natural de recorridos de estados, ya que los sistemas de automatización de subestaciones funcionan continuamente. Una explotación exitosa de las vulnerabilidades, puede conducir a un estado indeseable. El autómata de Büchi no determinista [14] permite modelar sistemas para generar sus respectivos gráficos de ataque.

5.1.1 Automata de Büchi

El autómata no determinista de Büchi se expresa usando la lógica temporal lineal (LTL), mientras que se modela sistémicamente. El poder de modelar un sistema que genera, analiza y produce estrategias de recomendación para medidas de seguridad e interacciones con el entorno adverso, reside en la efectividad del autómata finito sobre el que se basa. Por lo tanto, siguiendo las recomendaciones de la bibliografía [14] se considera que la metodología de Automata de Büchi, permite crear gráficos de ataque de manera eficaz y bajo una base matemática que se explica a continuación.

Para fines de revisión, se presenta la definición de fondo del autómata Büchi no determinista. Un autómata de Büchi no determinista es un autómata definido como una 5-tupla donde:

(i) Q es un conjunto finito de estados de A

(ii) σ es un conjunto finito de símbolos llamados alfabeto de A

(iii) Δ es la función de transición: $Q\ x\ \sigma \rightarrow P(Q)$, donde $P(Q)$ es el "*powerset"* de Q.

(iv) Q_0 es un subconjunto de Q, llamado conjunto de estados iniciales.

(v) A_{CC} es la condición de aceptación, representada en un subconjunto de Q^{ω} (puesto que las secuencias son secuencias infinitas, el conjunto infinito de secuencias infinitas de estados en Q, denotado por Q^{ω}, tendrá el subconjunto de algunas secuencias infinitas que satisfacen la condición de aceptación).

La ejecución se define por cualquier secuencia $\rho = (q_0, q_1, q_2, \dots)$ infinita tal que,

(i) $q_0 \in Q_0$,

(ii) $q_0 \in \Delta(q_0, a_1)$, donde a_i es el primer elemento en la cadena de entrada,

(iii) $q_i \in \Delta(q_i - 1, a_i) \forall i$, con $0 \leq i$.

La entrada sólo se acepta si al menos una de las ejecuciones posibles pertenece a la condición de aceptación A_{CC}. La potencia de los automatismos de Büchi para modelar los gráficos de ataque, se encuentra en la expresividad de las condiciones de aceptación A_{CC} [14].

5.2 IEC 62351

La alternativa que permite solucionar la falta de documentación en el estándar en cuanto a temas de seguridad informática es la IEC 62351. El estándar IEC 62351 contiene información acerca del uso de *Transport Layer Security* (TLS) y esto puede prevenir algunos de los ataques conocidos [9]. El estándar IEC 62351, presenta la documentación de la IEC 61850 en cuanto a perfiles, guías, arquitecturas y demás aspectos documentados. En la Figura 4 se muestra la aplicación de cada parte del estándar, citando las relaciones con otros documentos.

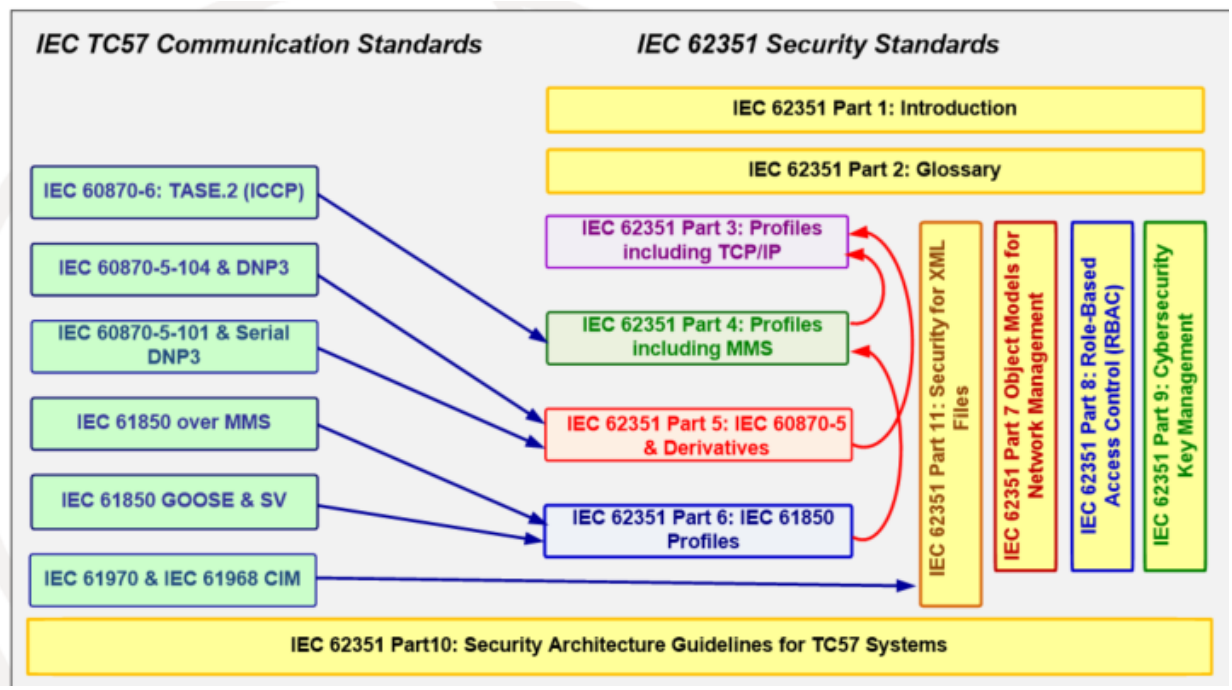


Figura 4. Mapa de Aplicación del Estándar IEC 62351 [9].

Además de tener la documentación en cuanto a los perfiles de comunicación, el estándar ofrece otras herramientas que permiten fortalecer la seguridad en las comunicaciones. Algunas de las diferentes partes de la norma contienen documentación en cuanto a controles de autenticación y acceso, administración de llaves, arquitecturas propuestas, entre otros.

5.2.1 Listado de Parámetros IEC 62351

A continuación, se listan algunos de los requerimientos y medidas de seguridad principales que documenta la norma IEC 62351.

Los perfiles que garantizan la seguridad cibernética para protocolo MMS de la IEC 61850 (el cual funciona sobre el modelo TCP / IP), se basan en la documentación presentada en la IEC 62351-3 e IEC 62351-4. GOOSE y SV son protocolos *multicast*, por lo tanto, la mayoría de las técnicas de cifrado u otras medidas de seguridad que afectan las tasas de transmisión no son aceptables. La autenticación a través de una firma digital es la única medida de seguridad incluida para estos protocolos utilizados para comunicación horizontal en el proceso de la subestación [9].

Las características principales y medidas de seguridad aplicables de los tres protocolos principales de la IEC 61850, se muestran en la Tabla 2 a continuación:

Tabla 2. Características y Medidas de Seguridad SV, GOOSE, MMS [9].

	SV	GOOSE	MMS
Tamaño PDU	1500	1500	30000
Desempeño	Stream	4ms	<1000ms
Tipo de Tráfico	Multicast	Multicast	Conexión Cliente Servidor
Certificados X509 (Identificación)	No	No	Si
Encriptación (Confidencialidad)	No	Solo GOOSE baja velocidad (>4ms)	Si
Sistema de Detección de Intrusos	Si	Si	Si

6. Propuesta

A continuación se describen los elementos que contienen la propuesta que permitió cumplir con los objetivos planteados. En esta investigación, se utiliza la metodología de gráficos de ataque para aplicarla a una arquitectura de comunicaciones de una subestación, teniendo en cuenta las recomendaciones del estándar IEC 62351. Esto se logró aplicando las herramientas disponibles en el sistema operativo Kali Linux, junto con el conocimiento de los estándares de comunicación de la subestación, determinando así un procedimiento que permite crear el modelo de gráfico de ataque. De este modo se llevan las herramientas y desarrollos para pruebas de penetración de las redes de comunicaciones convencionales y se aplican a las arquitecturas de comunicación de las subestaciones. Este procedimiento podrá ser utilizado para modelar diferentes arquitecturas de subestaciones digitales en el servicio de laboratorio IEC 61850 que ofrece el Grupo T&T de la Universidad Nacional de Colombia.

Se complementa el análisis aplicando la teoría de los autómatas de Büchi. De este modo se clasifican las vulnerabilidades detectando los estados prohibidos. Por último se valida la hipótesis de la investigación utilizando el gráfico de ataque para llegar a un estado prohibido detectado en la arquitectura propuesta. Se realiza la validación mediante un ataque, teniendo en cuenta la vulnerabilidad más crítica detectada.

6.1 Mapa Conceptual

Como parte de la metodología propuesta se parte de la elaboración de un mapa conceptual. Este mapa nos va a permitir relacionar los conceptos más importantes entorno a la problemática seleccionada. El mapa conceptual descrito en la Figura 5 relaciona los diferentes conceptos del marco teórico de la investigación (ver Figura 5); de este modo es posible identificar el objeto de estudio y cumplir con el primer objetivo, según la metodología propuesta.

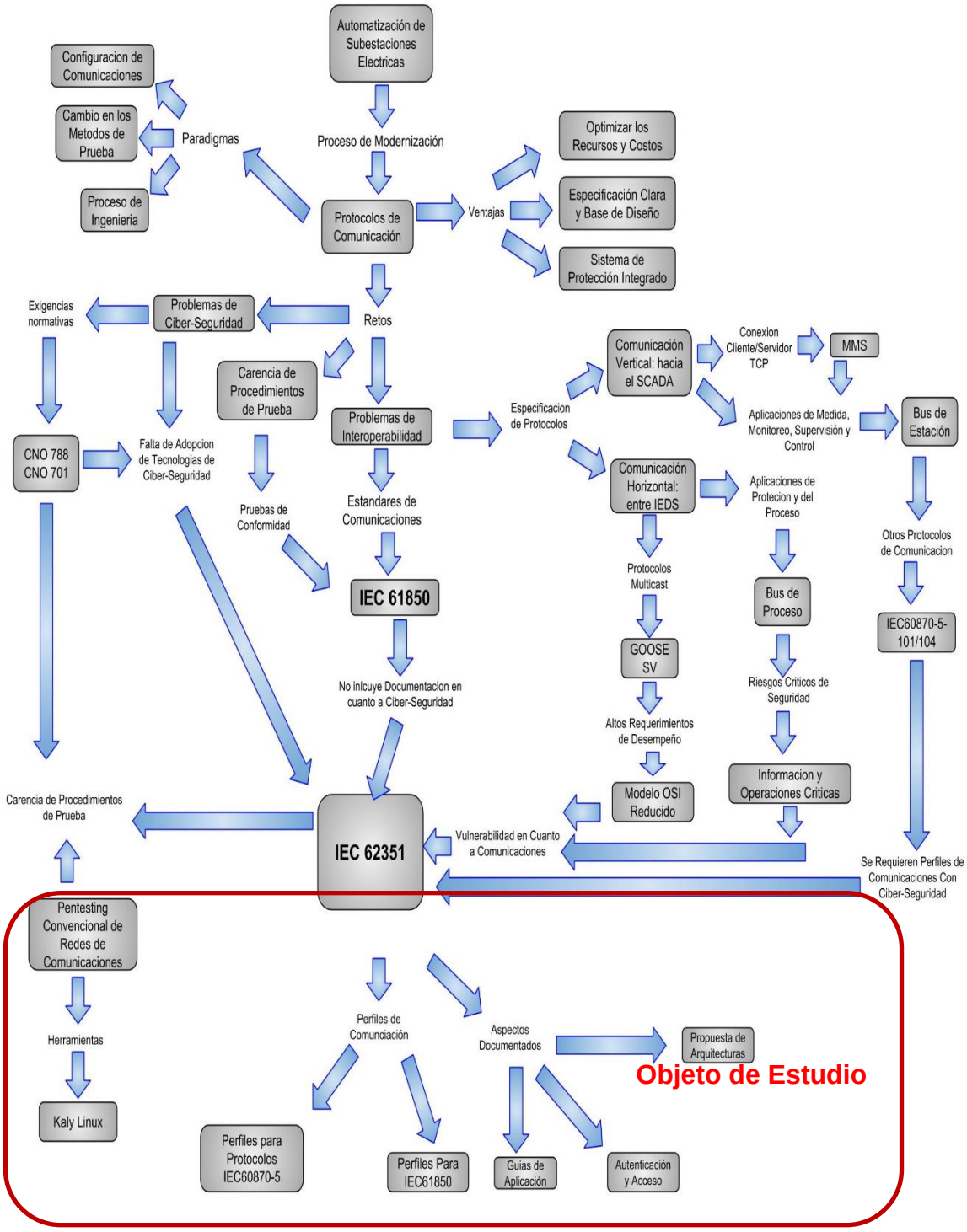


Figura 5.Mapa Conceptual Sobre IEC 62351 [Fuente: Elaboración Propia].

6.2 Elaboración del Gráficos de Ataque

En la literatura existen otros métodos para analizar los riesgos y las vulnerabilidades, sin embargo los gráficos de ataque ofrecen grandes ventajas en cuanto a la simplificación del modelo [16]. En la actualidad se han implementado algunos procedimientos para lograr exitosamente este proceso, pero únicamente para redes convencionales. A continuación en la Figura 6 se muestra un modelo conceptual de una metodología para lograr estructurar un gráfico de ataque.

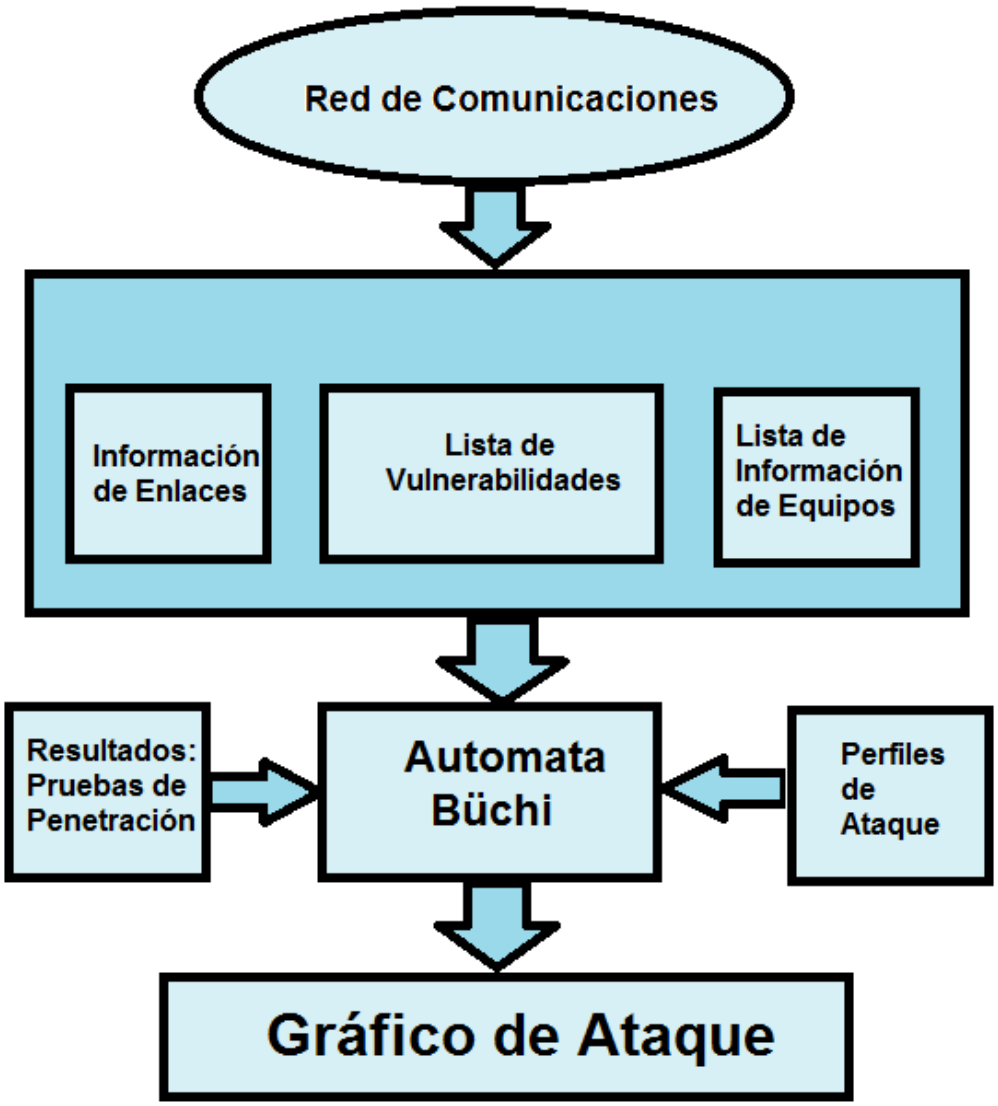


Figura 6. Metodología de Mapa de Ataque para Análisis de Vulnerabilidad [16].

Los pasos a seguir utilizados regularmente para construir estos modelos, se plantean a modo de pregunta y respuesta, como se ve a continuación [16]:

(1) ¿Qué parámetros del sistema se utilizan para construir el gráfico de ataque?
Definición y clasificación de recursos de red o de sistema, catalogación de activos y capacidades (recursos) en un sistema.

(2) ¿Como se clasifican los recursos de la red?
Asignar niveles relativos de importancia a los recursos, valor cuantificable (o al menos orden de clasificación) e importancia a esos recursos.

(3) ¿Cómo se generan las gráficas?
Aplicando la teoría del Automata Büchi.

(4) ¿Qué esfuerzos (métodos y herramientas utilizados) se hacen para los procedimientos de prueba?
Las pruebas de penetración con herramientas como Kali Linux.

(5) ¿Cuáles son las propiedades que se pueden analizar?
Las métricas propuestas inicialmente dentro de las hipótesis las cuales son: Disponibilidad, Integridad, Confidencialidad

(6) ¿Qué recomendaciones se obtienen de la gráfica para asegurar el sistema?
Desarrollar una estrategia para enfrentar los problemas potenciales más graves primero.

(7) ¿Qué métodos se utilizaron para evaluar el trabajo?
Definir e implementar maneras de minimizar las consecuencias si ocurre un ataque evaluando las vulnerabilidades más graves para los recursos más valiosos.

6.3 Procedimiento de Modelado Propuesto

La complejidad de los sistemas computacionales puede automatizarse mediante modelos con diversos grados de detalle, garantizando las propiedades deseadas de esos modelos. Los comportamientos de interés generados por los modelos se analizan para detectar problemas y localizar correcciones asociadas. Así, a medida que los sistemas evolucionan, también lo hacen sus modelos y análisis. En este trabajo, se pretende validar la hipótesis mediante el modelado de una subestación en gráficos de ataque. Se diseñaron una serie de pruebas utilizando herramientas especializadas para realizar ataques cibernéticos a una arquitectura de prueba y basado en los resultados se desarrolla un modelo de gráfico de ataque para estimar el nivel aproximado de vulnerabilidad de la arquitectura.

Como aporte en esta investigación se definió un paso a paso, que permite cumplir con los requisitos del modelado de gráficos de ataque. Además se modela una arquitectura de prueba para validar la hipótesis. Teniendo en cuenta las recomendaciones del estándar IEC 62351 mencionadas anteriormente, fue posible determinar los pasos para modelar el gráfico de ataque de la arquitectura de comunicaciones de la subestación. Cada paso se diseñó de manera que sea posible cumplir con la metodología de gráficos de ataque.

Los pasos propuestos para lograr obtener el modelo en gráfico de ataque son los siguientes:

1. Inicialmente se define la arquitectura bajo prueba, identificando los equipos presentes y clasificándolos de acuerdo a su importancia relativa.
2. Se trabajó bajo el supuesto de que se tiene acceso a la red. Es posible lograr entrar a una subestación a través de un enrutador inalámbrico u otro agujero de seguridad.
3. Luego teniendo acceso a la red, se utiliza una herramienta para descubrimiento IP basado en mensajes ARP, de este modo es posible identificar los segmentos de red en los cuales se encuentran configurados los equipos.
4. Una vez se tienen identificados los segmentos de red IP, se procede a hacer un escaneo de la red en esos segmentos específicos identificando puertos abiertos, información general de hardware y software y demás aspectos que permitan identificar posibles vulnerabilidades.
5. Se tabulan todos los resultados en una tabla de métricas, además se ponderan las vulnerabilidades y se proponen acciones correctivas y preventivas.
6. En caso de que se descubra algún puerto abierto, o cualquier tipo de vulnerabilidad, se valida realizando un ataque.

6.4 Listado de Herramientas y Propuesta de Aplicación

Según el objeto de estudio identificado anteriormente en el estado del arte, se requiere identificar los posibles usos y aplicaciones de las herramientas de pruebas de penetración, aplicado al área de subestaciones digitales según la IEC 62351. Por lo tanto para lograr aplicar la metodología propuesta y construir el gráfico de ataque, se utilizaron las herramientas de la Tabla 3. En esta tabla se listan las herramientas en el orden en el cual fueron aplicadas, según los pasos definidos anteriormente; además se especifica la función de cada software dentro de las pruebas.

Tabla 3. Lista de Herramientas y Posible Aplicación en Subestaciones [Fuente: Elaboración propia].

Herramienta	Funcionalidad	Descripción y Aplicación en Subestaciones
Netdiscover:	Escaneo de Segmentos de Red	La herramienta Netdiscover nos permitió identificar las direcciones IP objetivo para realizar el escaneo intenso de puertos.
Zenmap (Interfaz gráfica de Nmap):	Mapa de la Red	La herramienta Zenmap permitió obtener el mapa de red, dando una representación gráfica de todos los equipos y dispositivos de red mostrando cómo cada uno está conectado. Utilizando esta funcionalidad fue posible realizar un mapa de los dispositivos e identificar vulnerabilidades.
Wireshark:	Captura de Red	El software Wireshark permitió realizar capturas de red, probar vulnerabilidad de ataques man-in-the-middle, además permite verificar cifrado de contraseñas y comunicación.
Burp suite:	Seguridad de Aplicaciones Web	Debido a que muchos de los equipos de la subestación permiten gestión por aplicación web, la herramienta Burp Suite, permitió capturar los paquetes de red del puerto de comunicación web, para identificar vulnerabilidades.
John the Ripper:	Prueba de Seguridad de Contraseñas	Esta funcionalidad permitió evaluar vulnerabilidades en las contraseñas configuradas en los equipos dentro de la red.

6.5 Asignación de Importancia Relativa

Para cumplir con uno de los pasos necesarios en la construcción del modelo, fue necesario asignar niveles de importancia relativa a los equipos. Se propuso un análisis que permita la asignación de Importancia relativa para los equipos principales de la subestación. Para esto se realiza un análisis de riesgo, teniendo en cuenta los ataques en la red y sus posibles consecuencias para cada equipo.

En primer lugar se analizaron las consecuencias posibles de los tipos de ataques conocidos para cada equipo. En segundo lugar, se propuso analizar la correlación entre cada combinación de equipos, contabilizando el número de casos en los cuales existe dependencia. Por último, luego de contabilizar los riesgos y la dependencia se calcula la importancia relativa como la multiplicación de estos dos valores, el número de equipos dependientes se suma uno, para evitar la multiplicación por cero y tener en cuenta la dependencia del equipo de sus propias vulnerabilidades. Este resultado se utilizó para definir la importancia relativa como una medida de la dependencia de los demás equipos ante una condición de falla.

$$Importancia\ Relativa\ =\ (1 + \#Equipos\ dependientes) * \#Riesgo\ de\ Vulnerabilidad.$$

6.6 Síntesis de Resultados de Prueba

Dada la cantidad de información presente en los registros de prueba luego de realizar un escaneo profundo con la Herramienta Nmap, se propone sintetizar los resultados en una tabla. De este modo se facilita el análisis para identificar los riesgos de ataque presentes para la arquitectura. En primer lugar se identifican la proporción de puertos abiertos, sobre puertos seguros. En segundo lugar, se identifican el número de vulnerabilidades detectadas por el software para cada puerto abierto descubierto. Por último se relacionan las vulnerabilidades detectadas con los riesgos de ataques.

6.7 Ponderación de Métricas

Con el objetivo de establecer métricas cuantitativas que permitan estimar el nivel de vulnerabilidad de cada equipo presente en la arquitectura, se proponen ponderar en cuanto a disponibilidad, integridad y confidencialidad.

Para validar la hipótesis es necesario ponderar los valores correspondientes para calcular un valor representativo del nivel de seguridad. Una vez realizadas las pruebas de penetración, se sintetizan los resultados y se identificaron las vulnerabilidades presentes. Como las prioridades para estas métricas pueden variar según las políticas de los operadores de red, la relevancia de la infraestructura de la subestación digital con respecto al sistema nacional interconectado y demás factores; se propone que las constantes con las cuales se calcule el nivel de seguridad sean ajustadas con respecto al caso de aplicación. Para efectos prácticos en este trabajo se realiza una ponderación equitativa en las tres métricas; es decir, el “Nivel de Seguridad” se calcula como el promedio de las tres métricas. Si se requiere aplicar el método en un caso particular donde se desea dar mayor relevancia a alguna métrica, es necesario definir porcentajes para cada componente.

6.8 Resultados Esperados

Existen principalmente dos objetivos prácticos para el modelado. El primero es la gestión efectiva de entradas y salidas dentro del modelo de los gráficos de ataque. El segundo es la capacidad de generar estos gráficos de forma autónoma y eficiente con escalabilidad para sistemas más grandes. En este trabajo se describe únicamente como crear el modelo, pero se deja abierto como trabajo futuro proponer un método para automatizar el modelado. Los resultados esperados durante el proceso son los siguientes:

- Lograr establecer una arquitectura de prueba definiendo los equipos reales a utilizar en las pruebas.
- Crear una tabla de “Clasificación de Recursos de Red e Importancia Relativa”, según la propuesta realizada en el literal 6.3.
- Identificar los correspondientes segmentos de red para la arquitectura bajo prueba.

- Identificar las vulnerabilidades y riesgos de la arquitectura, mediante un escaneo profundo de las comunicaciones en los equipos.
- Realizar un análisis de los registros de prueba obtenidos y sintetizar los resultados en una tabla.
- Con los resultados sintetizados se espera obtener posteriormente la correspondiente Ponderación de Métricas según el procedimiento propuesto en el literal 6 .5.
- Lograr obtener el gráfico de Ataques a partir de los datos obtenidos en la ponderación de métricas y la metodología propuesta de los autómatas de Büchi.
- En caso de Identificar vulnerabilidades conocidas se propone probar en los equipos la vulnerabilidad más crítica detectada, verificando estados prohibidos del sistema por modificaciones de agentes no autorizados.

7. Resultados

A continuación se exponen los resultados, desde la arquitectura bajo prueba seleccionada y registros de prueba, hasta llegar finalmente al modelo de gráfico de ataque, incluyendo las recomendaciones para mitigar las vulnerabilidades identificadas.

7.1 Arquitectura de Prueba

Para obtener resultados representativos, se selecciona una arquitectura de prueba típica de una subestación, definiendo los equipos especificados dentro de la arquitectura según el estándar IEC 61850 [15]. En la arquitectura bajo prueba, se seleccionaron los equipos de mayor vulnerabilidad presentes típicamente dentro de una subestación. Por lo tanto se incluye un equipo para digitalización de señales o "*merging unit*", un equipo para protección principal de línea (IED – *Inteligent Electronic Device*), un equipo de comunicaciones, un equipo para conversión de protocolos y por último un Reloj GPS. Por otro lado para tener acceso a la red, se conecta un PC de captura con las herramientas para pruebas de penetración por medio de un enrutador inalámbrico. A continuación se muestra la arquitectura de prueba en la Figura 7.

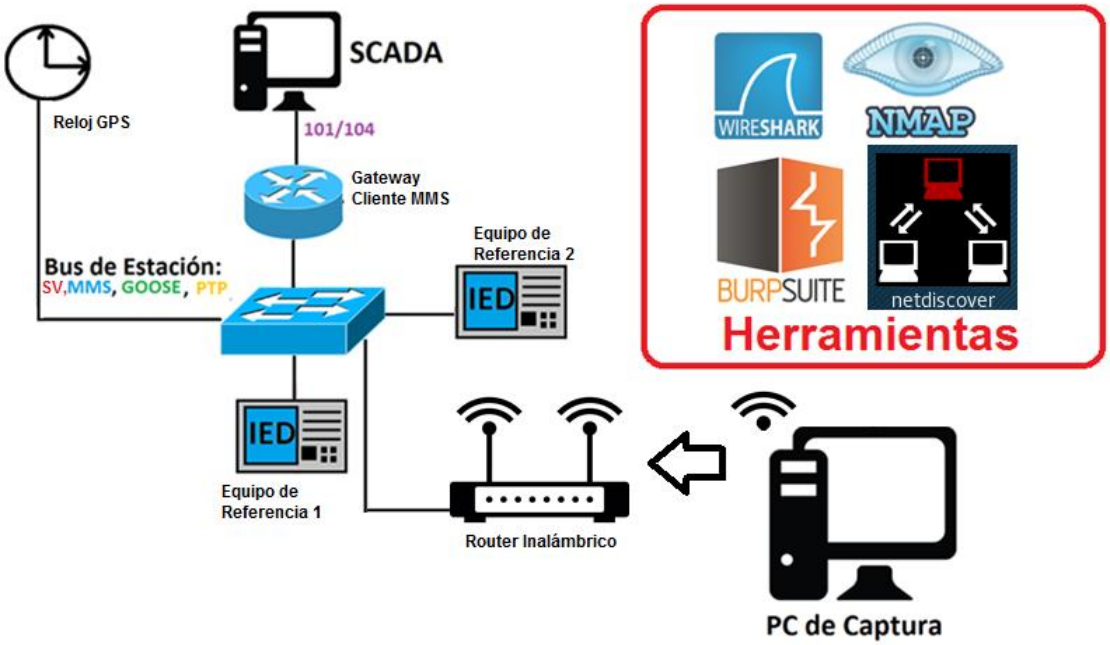


Figura 7. Arquitectura Bajo Prueba de Penetración [Fuente: Elaboración Propia].

7.2 Equipos

Para lograr la ejecución de las pruebas, se utilizaron equipos reales del servicio de laboratorio IEC 61850 ofrecido por el Grupo T&T de la Universidad Nacional de Colombia Sede Medellín. Los equipos disponibles para el montaje de la arquitectura propuesta fueron los siguientes:

- Switch: Switch de Bus de Proceso - S2024 G.E
- Gateway: Gateway SYNC3000 Kalkitech
- Equipo de Referencia 1: Mergin Unit MU320 G.E.
- Equipo de Referencia 2: IED para Protección de Línea 7SA87 SIEMENS
- Reloj GPS: RT430 G.E.

7.3 Clasificación de Recursos de Red e Importancia Relativa

Entre los primeros pasos para la construcción del modelo en gráfico de ataque, es necesario realizar una clasificación de los recursos de red de acuerdo a su importancia. El nivel de importancia se asigna según la criticidad y su importancia según la propuesta del literal 6.3 [15].

7.3.1 Gateway

Se encuentra bajo protocolos TCP orientados a la conexión, los cuales presentan menor riesgo; aunque esta es una función importante, no se considera tan crítica como las señales de disparo, los valores muestreados o los protocolos de sincronización.

Equipos dependientes: Ninguno de los demás equipos seleccionados dentro de la arquitectura de prueba depende directamente del Gateway. Al contrario este depende de todos los demás equipos.

$$\# \, Equipos \; dependientes = 0$$

Riesgos: Como riesgos se tiene la perdida de información en el SCADA (integridad), inhabilitación de comandos del centro de control (disponibilidad) y por último comandos y operación en falso (autenticidad).

$$\# \, Riesgos \; = 3$$

7.3.2 IED

Aunque este es supremamente importante y es el encargado de coordinar y ejecutar las funcionas de protección, depende directamente de otros equipos para su operación.

Equipos dependientes: El único equipo que depende del IED para la subestación digital es el Gateway como cliente IEC 61850, ya que el IED hace las veces de servidor IEC 61850 comunicándose con el cliente configurado en el Gateway.

$$\# \, Equipos \, dependientes = 1$$

Riesgos: Como riesgos se tiene la modificación indeseada de estados binarios (integridad), inhabilitación de medidas y disparos en funciones de protección (disponibilidad) y por último comandos y operación en falso (autenticidad).

$$\# \, Riesgos = 3$$

7.3.3 Merging Unit

Continuando con la clasificación, se tiene el equipo encargado de digitalizar las señales de los transformadores, estos son los que mantienen la conciencia de las señales físicas requeridas para la ejecución de las funciones de protección.

Equipos Dependientes: El IED depende directamente de las mediciones realizadas en este equipo, por lo tanto el Gateway también depende de manera indirecta de este al depender del IED.

$$\# \, Equipos \, dependientes = 2$$

Riesgos: Como riesgos se tiene la modificación indeseada de mediciones (integridad), inhabilitación del equipo de medición (disponibilidad) y por último comandos y operación en falso (autenticidad).

$$\# \, Riesgos = 3$$

7.3.4 Reloj GPS

El Reloj GPS se utiliza para sincronizar y coordinar todos los automatismos de la subestación.

Equipos Dependientes: El Gateway, el IED y la *Merging Unit* se sincronizan utilizando la señal enviada por el Reloj GPS, por lo tanto estos tres equipos dependen directamente de este.

$$\# \, Equipos \; dependientes \; = \; 3$$

Riesgos: Paquetes de sincronización no compatibles o dañados (integridad), desactivación inesperada de la señal de sincronización (disponibilidad) y por último tenemos un riesgo de señales de sincronización de suplantación por agentes no autorizados (autenticidad).

$$\# \, Riesgos \; = 3$$

7.3.5 Equipo de Comunicaciones

En el último lugar con la mayor importancia relativa se encuentra el *switch* de comunicaciones. Este es el que permite la comunicación y el intercambio de mensajes entre equipos. Si se pierde el *switch* de comunicaciones, se pierden todos los protocolos de la subestación, por lo tanto este tiene una gran relevancia en cuanto a seguridad cibernética.

Equipos dependientes: Todos los demás equipos de la subestación dependen del equipo de comunicaciones, ya que a través de el se comunican todos los protocolos.

$$\# \, Equipos \; dependientes \; = \; 4$$

Riesgos: Existe el riesgo de alteración de los protocolos de comunicación (integridad). Otro riesgo es el de perder puertos la disponibilidad parcial o total de los puertos de comunicación del equipo (disponibilidad). Por último existe el riesgo asociado a los ataques de *craking*, donde un agente no autorizado puede tener acceso a las credenciales de seguridad del equipo (autenticidad).

$$\# \, Riesgos \; = 3$$

7.3.6 Tabla de Clasificación de Equipos

En la Tabla 4 que se muestra a continuación se clasifican los recursos seleccionados dentro de la arquitectura bajo prueba.

Tabla 4. Clasificación de Recursos de Red e Importancia Relativa [Fuente: Elaboración Propia].

Equipo	**Funciones**	**Descripción**	**Nivel de Importancia Relativa**
SYNC3000 Kalkitech	Gateway	Este equipo se utiliza para realizar la conversión de protocolos de IEC61850 a IEC 60870-104 y/o 101 para lectura en SCADA. Es un equipo intermedio en las funciones de control y medición, que actúa como cliente en la comunicación MMS con el IED de protección de línea como servidor. Debe sincronizarse y los protocolos TCP se comunican a través de *switch*.	(0+1)*3= 3
7SA87 SIEMENS	Protección Principal	Los IEDs de protección se configuran con el fin de lograr la suscripción de SV publicados por las MU, además se configura la publicación de mensajes GOOSE que permiten enviar señales de disparo y demás información de estados con otros IEDs o MU´s. Por otro lado se comunica como servidor IEC 61850 enviando mensajes MMS a un cliente, en este caso el Gateway. La coordinación de todos estos protocolos debe realizar con sincronización de tiempo en todos los equipos de la red y se comunican a través de *switch*.	(2+1)*3=9
MU320 G.E.	Mergin Unit	Este equipo es el que se encarga de digitalizar las señales desde los equipos primarios hacia los IEDs. En algunos casos también es el encargado de accionar disparos binarios a partir de mensajes GOOSE *trip* publicados por	(3+1)*3=12

		el IED. La correcta suscripción de estos valores muestreados también depende de su correcta sincronización de tiempo, como también el cumplimiento de los requisitos de ancho de banda y tráfico en los *switch*.	
RT430 G.E.	Reloj GPS	El reloj GPS, es el que se encarga de enviar señales de sincronización de tiempo por medio de diferentes protocolos y medios, para coordinar todas las funciones de la subestación. Sin la sincronización de tiempo no es posible obtener referencia para los valores muestreados, no se tiene trazabilidad de eventos y algunos protocolos pierden fiabilidad, por estos motivos este equipo es de los más críticos. A pesar de esto, los protocolos de sincronización como PTP, SNTP y NTP, como también los protocolos de gestión del GPS, se comunican a través de los *switch*, haciéndolo dependiente.	(4+1)*3=15
S2024 G.E	Switch de Bus de Proceso	Este equipo podría considerarse el de mayor importancia, ya que toda la comunicación de la subestación se realiza a través de este. A pesar de que los IEDs y los MUs, son las que coordinan las funciones de protección y demás procesos automáticos dentro de la subestación, todos estos dependen netamente del *switch* y a través de este es por donde se logra llegar al control de los demás equipos y se comunican los protocolos de gestión.	(5+1)*3=18

7.4 Identificación de Segmentos de Red

Luego de tener acceso a una de las redes internas de la subestación, se quiere identificar todos los posibles segmentos de red IP, en los cuales pueda haber equipos configurados. El software “Netdiscover”, permite utilizar el protocolo ARP y los mensajes de este presentes en la red, escanear todos los posibles procesos de descubrimiento y aprovecharse de esto para extraer información valiosa. De este modo al obtener los resultados y conocer las direcciones de las redes configurados, es posible proceder a hacer un escaneo en estas e identificar las vulnerabilidades presentes en los equipos conectados, como también obtener información del fabricante, software, sistema operativo y demás.

A continuación en la Figura 8, se muestran los resultados obtenidos para la arquitectura de pruebas. Se puede ver cómo fue posible detectar todas las direcciones IP mediante la herramienta Netdiscover de Kali Linux.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Currently scanning: 172.27.246.0/16   |   Screen View: Unique Hosts

22 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 1374
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.199   f8:02:78:10:07:50      1      66  IEEE REGISTRATION AUTHORITY
192.168.1.71    f8:02:78:10:07:50      7     462  IEEE REGISTRATION AUTHORITY
192.168.1.199   f8:02:78:10:1f:44      5     300  IEEE REGISTRATION AUTHORITY
192.168.2.10    b4:b1:5a:00:6c:0c      1      66  Unknown vendor
192.168.2.199   f8:02:78:10:1f:44      1      60  IEEE REGISTRATION AUTHORITY
192.168.10.100  00:00:7a:cc:00:34      1      60  DANA COMPUTER INC.
192.168.1.110   f8:02:78:10:12:32      6     360  IEEE REGISTRATION AUTHORITY
```

Figura 8. Netdiscover para Arquitectura Bajo Prueba [Fuente: Elaboración propia a partir de Software Netdiscover].

La herramienta Netdiscover permite identificar las direcciones IP de los equipos conectados a la red mediante los mensajes ARP, sin embargo hay algunos equipos que no permiten aplicar este proceso. Por ejemplo la IP de gestión del módulo de bus de proceso en el IED, no pudo ser detectada; esto es un resultado positivo, ya que esta interfaz es crítica y a través de ella se cargan archivos de configuración desde una plataforma web. Si un atacante pudiera obtener esta IP, podría estropear la configuración del módulo para la suscripción de SV (*Sampled Values)*.

A continuación en la Tabla 5 se listan las direcciones IPs de la arquitectura de prueba, determinando si fue posible identificar su IP mediante el uso de

Netdiscover, además también se determinan los posibles riesgos asociados por la detección de la dirección IP.

Tabla 5.Identificación de Segmentos de Red y Posibles Riesgos [Fuente: Elaboración Propia].

Equipo	Puerto	IP	Detecto IP (SI/NO)	Posibles Riesgos
SYNC3000 Kalkitech	**Gestión**	192.168.0.199	SI	Es posible deshabilitar medidas y comandos
MU320 G.E.	**Único**	192.168.1.71	SI	Suplantación de medidas de SV (daños graves a equipos finales)
RT430 G.E.	**LAN 1**	192.168.1.199	SI	Perdida de reloj y sincronización de tiempo (errores en las protecciones)
	LAN 2	192.168.2.199	SI	
PC de Referencia	**Tarjeta de Red**	192.168.2.10 y 192.168.1.131	SI	Suplantación de Identidad, robo de información.
7SA87 SIEMENS	**Gestión**	192.168.10.100	SI	Cambio en Automatismos (daños a equipos finales e infraestructura)
S2024 G.E	**Puerto de Entrada de Ataque (IP de Gestión)**	192.168.1.110	SI	Perdida de toda la comunicación de la subestación y pór ende riesgo a todas las amenazas mencionadas anteriormente.
Módulo PB201 SIEMENS	**Puerto de Gestión (Carga de Archivos para SV)**	10.0.0.110	NO	No fue posible detectar esta IP, es necesario verificar mediante otros métodos.

7.5 Identificación de Amenazas

Utilizando los segmentos de red identificados anteriormente con la herramienta Netdiscover, fue posible tener un conjunto de direcciones IP objetivo, a partir de las cuales se realizó el análisis con la herramienta Nmap. Nmap permite especificar las IP objetivo para el análisis y se realiza un escaneo completo de la red, equipos, especificaciones y especialmente vulnerabilidades. Luego con estos registros tomados mediante el software Nmap, fue posible identificar ciertas amenazas presentes en los equipos, a continuación en la Figura 9 se muestra el mapa de la topología descubierta por el software en su versión de interfaz gráfica (Zenmap).

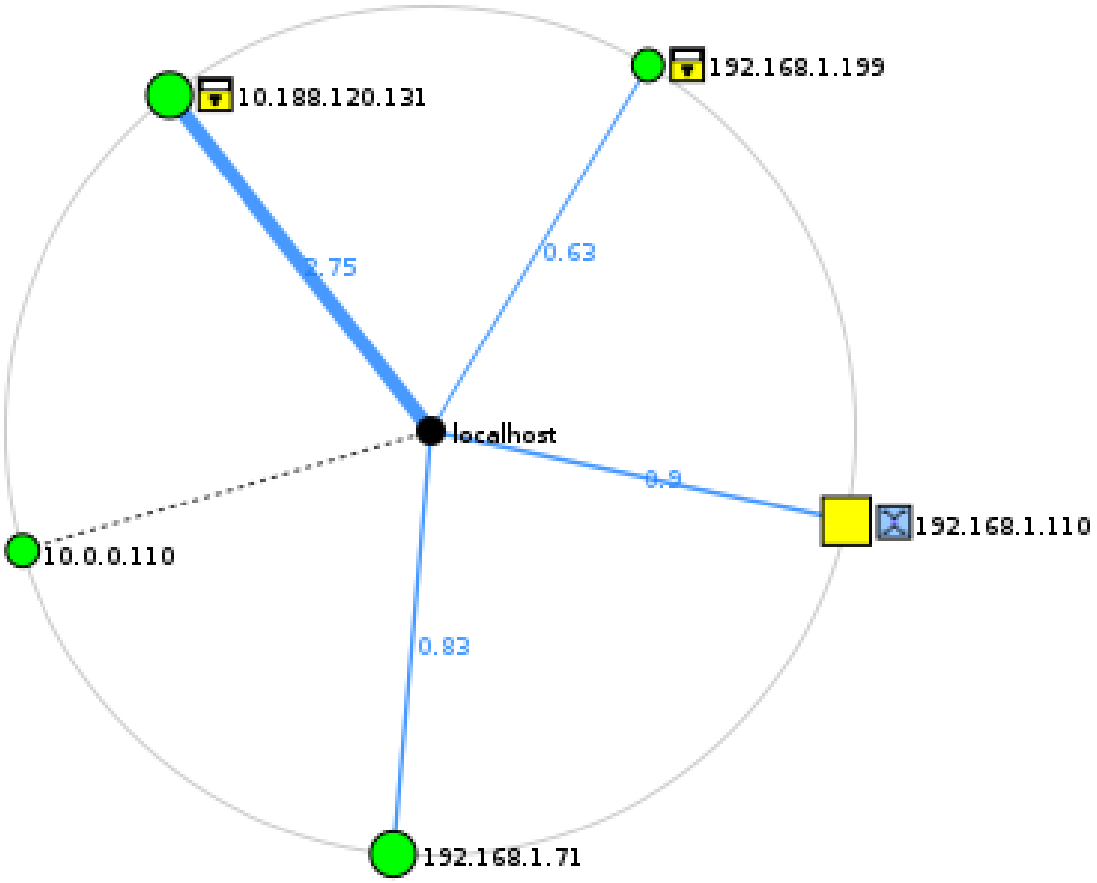


Figura 9. Topología creada con Zenmap (interfaz gráfica Nmap) luego del análisis a IPs Objetivos [Fuente: Elaboración propia usando Zenmap].

Una vez realizadas las pruebas de penetración con Zenmap (interfaz gráfica Nmap), se logran escanear los equipos en busca de puertos abiertos y agujeros de seguridad. La herramienta presenta un resumen detallado de los resultados que permitirá posteriormente realizar un análisis de mayor profundidad comparando los resultados para diferentes equipos. En la Figura 10 se muestra un ejemplo de captura para el *switch* de comunicaciones de la arquitectura, en este se encontró un puerto web abierto con vulnerabilidades.

```
Nmap scan report for 192.168.1.110
Host is up (0.00090s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE     VERSION
22/tcp open  ssh         Dropbear sshd 0.51 (protocol 2.0)
| ssh-hostkey:
|   1024 79:36:5b:b6:58:ac:09:c1:4d:92:a9:50:a1:60:1f:67 (DSA)
|_  1040 dd:15:6b:be:26:1d:b0:0c:ef:af:59:f2:83:e7:a7:47 (RSA)
23/tcp open  telnet
80/tcp open  tcpwrapped
| http-auth:                                  Vulnerabilidad más crítica detectada
| HTTP/1.1 401 Not Authorized
|_  Basic realm=S2024G
|_http-favicon: Unknown favicon MD5: 036A30B381204E5A3B997EDD3B7FEDF1
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: S20 Web Server
|_http-title: 401 Not Authorized
```

Figura 10. Resultados de Zenmap para IP del Switch [Fuente: Elaboración propia usando Zenmap].

7.6 Análisis de Registros de Prueba

Para cada uno de los equipos se consolidan los resultados obtenidos mediante la herramienta Zenmap. En la primera columna se identifica el número de puertos abiertos detectados sobre el número de puertos disponibles en el equipo. En la próxima columna se verifica el número de vulnerabilidades detectadas por cada puerto abierto descubierto. Por último teniendo identificadas las vulnerabilidades encontradas en los puertos abiertos de los diferentes equipos de la arquitectura, se definen los posibles ataques que pueden llegar a presentarse contra la red.

Por último se analizan los resultados encontrados de todos los equipos conectados a la red y se consignan en la Tabla 6, identificando los posibles ataques dentro de las clasificaciones presentadas anteriormente.

Tabla 6. Análisis de Métricas en Registros Zenmap [Fuente: Elaboración Propia].

Equipo	#Puertos Abiertos/ #Puertos Seguros	# de Vulnerabilidades detectadas	Posibles Ataques

			Detectados
Switch: Switch de Bus de Proceso - S2024 G.E	3/65532	Puerto22= 2 Puerto 23= 1 Puerto 80= 2 Total=5	Dos Sniffing Spuffing Craking (Basico) Total=3
Gateway: Gateway SYNC3000 Kalkitech	0/65535	Ninguna	Ninguno Total=0
Equipo de Referencia 1: Mergin Unit MU320 G.E.	2/65533	Puerto22=1 Puerto102=1 Total=2	Snifing Craking (tecnicas avanzadas) Total=2
Equipo de Referencia 2: IED para Protección de Línea 7SA87 SIEMENS	2/65533	Puerto102=1 Puerto443=1 Total=2	Snifing Craking (tecnicas avanzadas) Total=2
Modulo de Bus de Proceso PB201	0/65535	Ninguna	Ninguno Total=0
Reloj GPS: RT430 G.E.	0/65535	Ninguna	Ninguno Total=0

7.7 Análisis de Métricas

A partir de los resultados de prueba analizadas anteriormente, es posible evaluar los aspectos propuestos inicialmente dentro de la hipótesis; disponibilidad, confidencialidad e integridad. Para calcular la ponderación de las métricas con respecto al nivel de seguridad general del equipo dentro de la arquitectura, se utilizó el procedimiento propuesto en el literal 6.5.

Para este caso puntual se escoge una ponderación equitativa para las tres métricas (disponibilidad, integridad y confidencialidad). De este modo, el nivel de seguridad cibernética puede variar de cero a tres (0-1); donde cero (0) representa el peor de los casos en cuanto a seguridad cibernética e implica que el nivel de vulnerabilidad es alto y tres (1) implica el mayor nivel de seguridad cibernética dando a entender que se tiene un nivel de vulnerabilidad bajo. En la Tabla 7 se

pondera un valor numérico a cada uno de estos parámetros basado en las vulnerabilidades encontradas para cada dispositivo.

Tabla 7. Análisis de Disponibilidad, Integridad y Confidencialidad [Fuente: Elaboración Propia].

Equipo	**Disponibilidad (0-1)**	**Integridad (0-1)**	**Confidencialidad (0-1)**	**Nivel de Seguridad Cibernética (0-1)**
Switch: Switch de Bus de Proceso - S2024 G.E	Pt: 0.2 Posible ataque DoS por vulnerabilidad de contraseñas en puertos abiertos debido a encriptación pobre.	Pt: 0.2 Posible ataque de suplantación debido a vulnerabilidad en interfaz web.	Pt:0.2 Posibles ataques de sniffing por falta de mecanismos de encriptamiento.	0.2/1
Gateway: Gateway SYNC3000 Kalkitech	Pt:1 No se identificaron vulnerabilidades en cuanto disponibilidad	Pt:1 No se identificaron vulnerabilidades en cuanto Integridad	Pt: 0.5 A pesar de que no se presencian puertos abiertos, fue posible obtener la IP mediante envenenamiento ARP.	0.83/1
Equipo de Referencia 1: Mergin Unit MU320 G.E.	Pt:0.6 Se tienen protocolos encriptados en los puertos abiertos. Sin embargo es posible afectar la disponibilidad mediante técnicas avanzadas, ya que fue posible obtener el hostkey.	Pt: 0.6 Se tienen protocolos encriptados en los puertos abiertos. Sin embargo es posible afectar la Integridad mediante técnicas avanzadas, ya que fue posible obtener el hostkey	Pt: 0.6 A pesar de que los puertos abiertos están bajo protocolos seguros, se logró identificar el hostkey de SSH.	0.6/1
Equipo de Referencia 2: IED para Protección de Línea 7SA87 SIEMENS	Pt:1 No se encontraron Vulnerabilidades en cuanto a Disponibilidad	Pt:1 No se encontraron Vulnerabilidades en cuanto a Integridad	Pt:0.3 Es posible hacer sniffing debido a los puertos abiertos, sin embargo se requiere de encriptación y el uso de técnicas avanzadas para craquear contraseñas.	0.76/1
Módulo de Bus de Proceso PB201	No se identificaron vulnerabilidades en cuanto disponibilidad	No se identificaron vulnerabilidades en cuanto Integridad	No se identificaron vulnerabilidades en cuanto confidencialidad	1/1
Reloj GPS: RT430 G.E.	No se identificaron vulnerabilidades en cuanto disponibilidad	No se identificaron vulnerabilidades en cuanto Integridad	No se identificaron vulnerabilidades en cuanto confidencialidad	1/1

7.8 Gráfico de Ataque

Para lograr la construcción del gráfico de ataque, se definieron inicialmente los conjuntos de Büchi en el literal 10.1. Una vez definidos los conjuntos se aplicaron los pasos para la construcción del modelo (ver estado literal 7.2 del Estado del Arte), teniendo en cuenta los resultados obtenidos en las pruebas de penetración para cada uno de los equipos.

7.8.2 Conjuntos de Büchi

a) <u>Equipos (Conjunto de Estados)</u>

Inicialmente se modelan los equipos determinando las entradas correspondientes como vulnerabilidades y las salidas correspondientes como posibles ataques. También se utiliza el código de color para categorizar los equipos según su nivel de vulnerabilidad. El conjunto de estados para la construcción del autómata de Büchi está compuesto por los estados posibles dentro de la configuración de los equipos de la subestación. El conjunto de estados prohibidos está compuesto por todas las vulnerabilidades y los estados generados por su explotación.

b) <u>Vulnerabilidades Detectadas (Entradas al Modelo)</u>

Las vulnerabilidades detectadas se utilizan como entradas del modelo, a través de estas cuales un atacante puede llegar a un estado del conjunto de estados prohibidos utilizando diferentes ataques. Todos los puntos comunes de entrada pueden afectar a varios equipos con un mismo ataque.

c) <u>Definición de Estados Prohibidos (Riesgos de Ataques, Vulnerabilidades)</u>

Se sintetizan los resultados mediante un modelo de gráficos de ataques. De este modo se valida la hipótesis mediante los resultados finales, cuantificando el nivel de vulnerabilidad correspondiente al modelo de la subestación bajo prueba. Las salidas del modelo se representan como posibles ataques derivados de la explotación de las vulnerabilidades dentro del modelo. Los

estados prohibidos pueden darse en varios equipos en simultáneo derivado de la explotación de vulnerabilidades en paralelo.

7.8.3 Interpretación

En la Figura 11, se puede ver el gráfico de ataque resultante del análisis de vulnerabilidades utilizando la teoría de estas prohibidos del autómata de Büchi. En este se resaltan los diferentes conjuntos de Büchi identificados anteriormente. Por otro lado los colores de los estados indican el nivel de vulnerabilidad asociado. A continuación se describe la leyenda del gráfico con el fin de poder darle una mejor interpretación.

Como se puede ver en el gráfico, se tienen diferentes niveles de vulnerabilidades a lo largo de la arquitectura. Por un lado se tienen tres equipos en color verde, estos equipos tienen menor riesgo a ataques maliciosos comunes, ya que no se encontraron puertos de comunicación abiertos. En consecuencia estos equipos se representan con un nivel de seguridad cibernética alto en verde oscuro (Modulo PB) y seguridad cibernética media en color verde claro para los equipos Gateway y GPS. Por otro lado se tienen los demás equipos, el IED y la MU; estos tienen vulnerabilidades detectadas en algunos puertos abiertos. Sin embargo, al tener un menor número de vulnerabilidades y un nivel de importancia relativa menor al del *Switch* de comunicaciones, se consideran equipos con riesgo medio y se representan con un tono naranja medio claro. Por último, el equipo principal de comunicaciones se dibuja en naranja oscuro, esto por ser el equipo de mayor importancia relativa y debido a que se encontraron en las pruebas puertos vulnerables abiertos como es el caso del puerto de protocolos web (puerto 80).

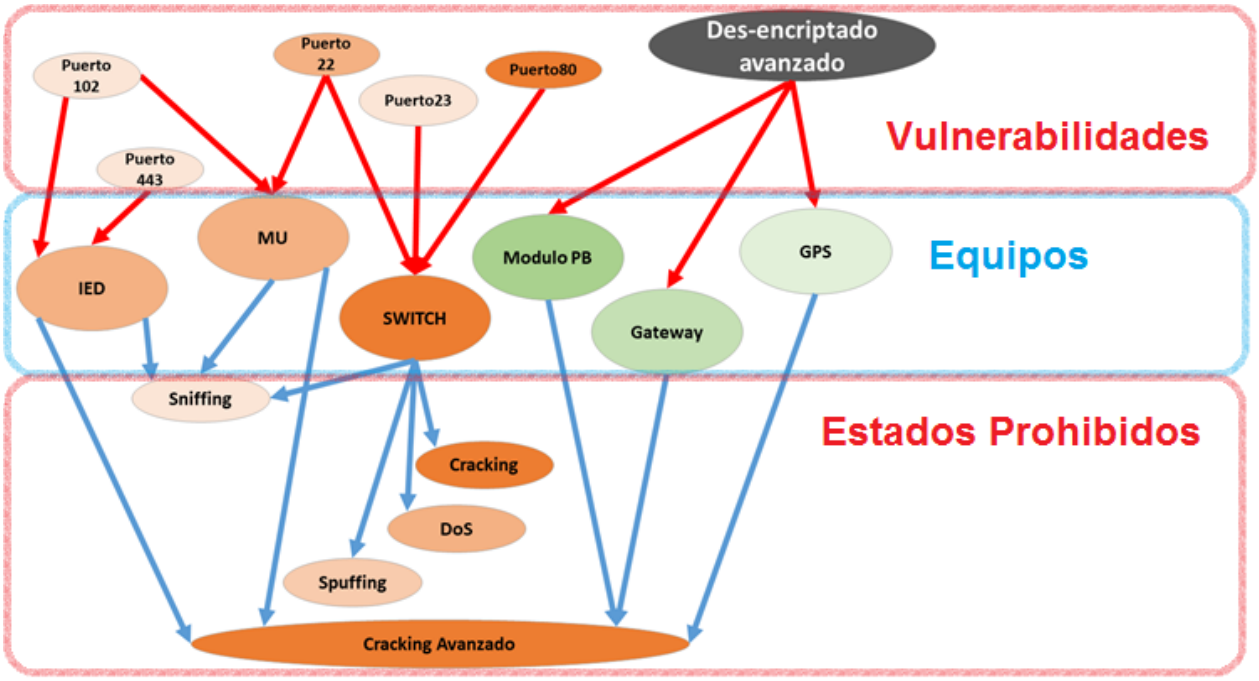


Figura 11. Gráfico de Ataque de Arquitectura Bajo Prueba [Fuente Propia].

En resumen, según la hipótesis planteada al principio de esta investigación, es posible aplicar el procedimiento descrito para modelar la arquitectura de comunicaciones en un gráfico de ataque. De este modo el gráfico permite evaluar cuales son las vulnerabilidades presentes en la red y evaluar los posible estados prohibidos a los que podrían conllevar estas vulnerabilidades.

Por último, para permitir al lector un mejor análisis de los resultados presentados anteriormente en la Figura 11, se lista a continuación las especificaciones para la leyenda del gráfico.

- Leyenda del gráfico:

  A) Escala de Colores:

  - Naranja: Se utiliza el color naranja dentro del gráfico de ataque para denotar posibles vulnerabilidades, los tonos claros y oscuros del color representa el nivel de criticidad de la vulnerabilidad. Entre más oscuro se considera de mayor criticidad.

- Verde: Se utiliza el color verde dentro del gráfico de ataque para denotar implementaciones seguras, el tono de verde representa la fortaleza de una implementación segura, los tonos del verde van de claro a oscuro denotando la dificultad de penetración de menor a mayor.

B) Color de las Flechas:

- Roja: Denota una entrada de un atacante mediante una vulnerabilidad detectada.
- Azul: Denota un posible ataque efectuado utilizando alguna de las vulnerabilidades de que se tenga como entrada al equipo.

7.8.4 Resultados Finales

Como parte del diagnóstico final del estado de la subestación en cuanto a vulnerabilidades y agujeros de seguridad, se listan unas recomendaciones a nivel correctivo (luego de tener un ataque), preventivo (de modo que se prevengan los ataques) y unas observaciones en cuanto a la relevancia específica de cada equipo en la Tabla 8. Vale la pena aclara que toda la información consignada a continuación se extrae a partir del análisis realizo en el gráfico de ataque.

Tabla 8. Recomendaciones para Mitigación de Riesgos.

Equipo	Acciones Correctivas	Acciones Preventivas	Observación
Switch: Switch de Bus de Proceso - S2024 G.E	Detectar IP y Puerto del intruso y denegar acceso, mediante listas de acceso y seguridad de puertos.	Configurar siempre seguridad de puertos, encriptación fuerte (algoritmo scrypt), y credenciales seguras para la gestión de equipos.	Este es el equipo más importante ya que a través de este pasa toda la comunicación de la subestación, si se tienen vulnerabilidades en este equipo se compromete los demás sistemas.
Gateway: Gateway SYNC3000 Kalkitech	Continuar con las buenas prácticas de seguridad, agregar sistemas de detección de intrusos	Implementar algún sistema de detección intrusos como honeypots.	A pesar de tener buena seguridad, a medida que avanza la tecnología aparecen prácticas que consigue romper la seguridad de estos sistemas, implementar sistemas de detección de intrusos.
Equipo de Referencia 1:	Encriptación fuerte	Filtrar todos los	Si este equipo es vulnerado pueden causar

Mergin Unit MU320 G.E.	para evitar sniffing y cracking	puertos abiertos para evitar conexiones indeseadas.	daños en la infraestructura física alterando sus comunicaciones, asegurar todos los puertos.
Equipo de Referencia 2: IED para Protección de Línea 7SA87 SIEMENS	Encriptación fuerte para evitar sniffing y cracking	Filtrar todos los puertos abiertos para evitar conexiones indeseadas.	Si este equipo es vulnerado pueden causar daños en la infraestructura física alterando sus comunicaciones, asegurar todos los puertos.
Módulo de Bus de Proceso PB201	Continuar con las buenas prácticas de seguridad, agregar sistemas de detección de intrusos	Implementar algún sistema de detección intrusos como honeypots.	Este equipo a pesar de estar protegido, igualmente es necesario mantener la seguridad para evitar daños en la infraestructura por alteración de las medidas en SV.
Reloj GPS: RT430 G.E.	Continuar con las buenas prácticas de seguridad, agregar sistemas de detección de intrusos	Implementar algún sistema de detección intrusos como honeypots.	La sincronización de tiempo es vital en la subestación para la coordinación de las funciones de protección, además de registro de datos y comandos hacia el sistema SCADA. A pesar de que el equipo se encuentra protegido, se recomiendan sistemas de detección de intrusos.

7.9 Validación de la Hipótesis

Con el fin de probar la hipótesis y comprobar las vulnerabilidades, efectivamente fue posible realizar un ataque a una arquitectura de comunicaciones de una red de una subestación bajo prueba en el laboratorio. Apoyado en el modelo de gráfico de ataque, se determina cual es la vulnerabilidad de mayor relevancia en la arquitectura bajo prueba. Por lo tanto se simplifica el gráfico de ataque en la Figura 12, de modo que se pueda evaluar el efecto de la vulnerabilidad en el puerto 80 del *Switch*, verificando si es posible llegar a un estado prohibido en el cual se pueda dar un ataque que permita romper las contraseñas en el equipo.

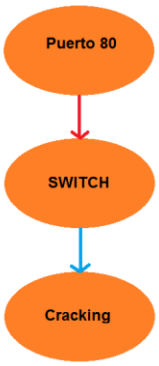


Figura 12. Gráfico de Ataque Simplificado para Validación.

Como una de las mayores amenazas encontradas en el análisis desarrollado anteriormente radica en la vulnerabilidad del *Switch* en la cual el puerto 80 se encuentra abierto, fue posible interceptar el tráfico web y obtener la contraseña para acceder a la gestión del equipo mediante *sniffing*. En la Figura 15 se puede observar cómo es posible interceptar las comunicaciones utilizando la herramienta Burpsuit. La captura de pantalla muestra el momento en el cual un usuario legítimo accede al equipo e ingresa las credenciales correctamente, estos paquetes se capturan para obtener dichas credenciales posteriormente mediante técnicas de des-encriptado.

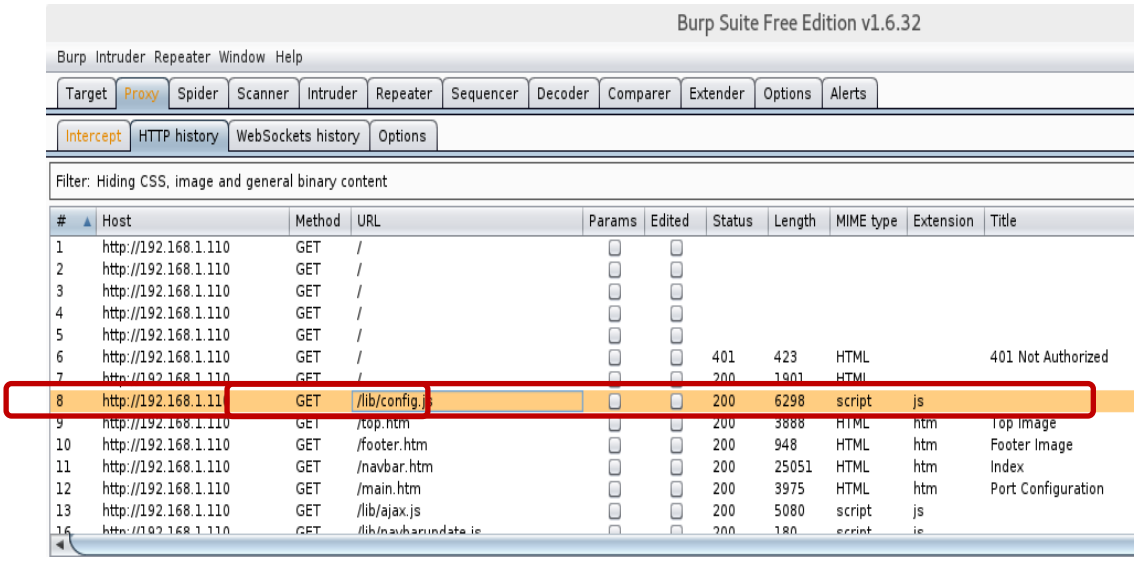


Figura 13. Captura de Ingreso con contraseña correcta para identificación de campo de acceso.

Una vez se tiene el paquete con las credenciales de acceso, se puede ver la información dentro de este, tal como se muestra en la Figura 16. Como se puede ver hay un campo de autorización, el cual contiene información sobre el protocolo de encriptado y las credenciales en un formato especial que no puede reconocerse a simple vista.

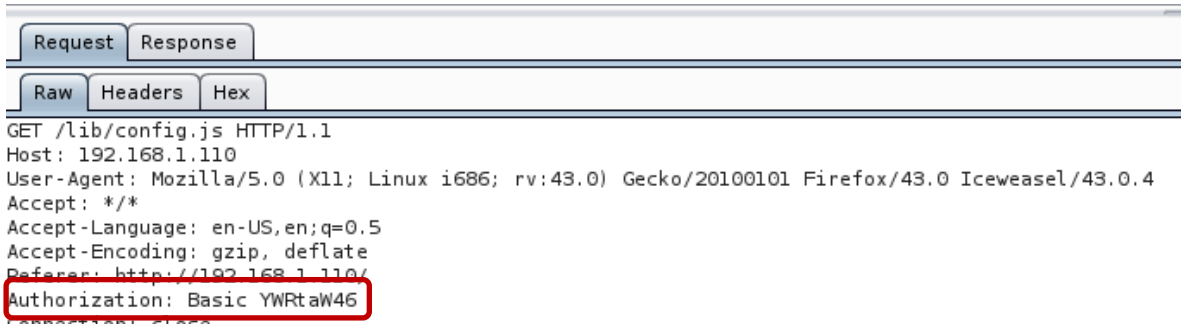


Figura 14. Contraseña correcta encriptada y campo de autorización.

Una vez identificado el algoritmo de encriptado y mediante una herramienta simple de *pentesting* para des-encriptar datos, fue posible obtener las credenciales y la contraseña (ver Tabla 10).

Tabla 9. Des-encriptada de clave correcta para suplantación.

Clave Encriptada (Hash)	**Algoritmo de Encriptado Identificado**	**Clave Des-encriptada**
YWRtaW46	ASCii	Admin:

Una vez se tiene la clave de acceso para la gestión del *switch* mediante la interfaz web, el atacante puede proceder a apagar puertos de configuración, modificar filtrados de MAC e introducir tráfico malicioso; todo esto puede poner en peligro la integridad de los esquemas de protección y toda la subestación, incluyendo infraestructura y equipos finales.

Por lo tanto, luego de haber aplicado exitosamente las metodologías para redes tradicionales en conjunto con el marco teórico, se desarrolló exitosamente un gráfico de ataque para una arquitectura de comunicación de una subestación digital. Este gráfico de ataque permitió validar la hipótesis probando el conjunto de entrada identificando el puerto 80 como una vulnerabilidad y fue posible llegar a un estado prohibido en el cual se ven comprometidas las credenciales para el acceso a la configuración del equipo.

8 Conclusiones

Los conceptos y técnicas planteadas en el estándar IEC 62351 para seguridad cibernética en subestaciones permiten identificar las herramientas y procedimientos necesarios para lograr modelar una subestación mediante gráficos de ataque.

Al estructurar los procedimientos necesarios para medir o establecer el nivel de vulnerabilidad y desempeño de una arquitectura típica de comunicaciones para automatización de subestaciones es posible obtener los registros de prueba necesarios para la construcción de un modelo para análisis de vulnerabilidades.

Luego de aplicar el procedimiento descrito, fue posible utilizar los registros obtenidos para construir un modelo que permitió el análisis de las vulnerabilidades detectadas.

Una vez construido un modelo en gráfico de ataque para una subestación bajo prueba, fue posible validar la vulnerabilidad más crítica detectada y realizar exitosamente un ataque que puede comprometer una subestación entera.

Gracias a las herramientas utilizadas en este trabajo y la metodología para el desarrollo de gráficos de ataque del autómata de Büchi, se demuestra la hipótesis, comprobando la posibilidad de realizar el análisis de vulnerabilidades en una arquitectura típica de comunicaciones para automatización de subestaciones bajo el estándar IEC 61850 utilizando un procedimiento de prueba.

Para trabajos futuros es posible desarrollar procedimientos que permitan realizar pruebas de conformidad a dispositivos, aplicando técnicas similares pero con un enfoque de pruebas de producto.

Una posible continuación del trabajo realizado es aplicar las técnicas como sistemas de identificación de intrusos, sistemas de *handshake* mejorado y sistemas con ambas implementaciones; luego aplicar este procedimiento a las tres implementaciones y luego comparar los resultados. De este modo es posible validar los efectos de estas implementaciones en materia de seguridad.

Por último otro posible trabajo que puede desarrollarse partiendo de este aporte, es el de realizar pruebas de desempeño en conjunto con los gráficos de ataque para lograr validar los efectos de la seguridad sobre el desempeño de las comunicaciones.

9 Recomendaciones

Se recomienda continuar investigando sobre procedimientos de prueba que permitan construir modelos para validar las condiciones necesarias de seguridad cibernética para las subestaciones de energía que son consideradas infraestructura crítica.

El software libre utilizado para pruebas de penetración representa un gran potencial para el proceso de ingeniería como herramientas de auditoria de seguridad y de diseño para subestaciones más seguras.

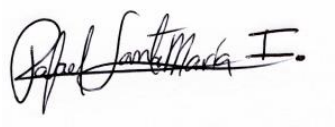
Con la ayuda de herramientas informáticas es posible construir modelos aún más complejos utilizando la teoría de los autómatas de Büchi, los cuales pueden ser herramientas útiles para hacer seguimiento a las condiciones de seguridad de la subestación.

Una vez desarrollados los gráficos de ataque, se pueden analizar las vulnerabilidades de mayor criticidad para verificar su relevancia y tomar acciones preventivas y correctivas.

10 BIBLIOGRAFIA

[1] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh, T. Jian-Cheng Tan, "An Intrusion Detection System for IEC 61850 Automated Substations," IEEE Transactions on Power Delivery. Octubre 2010.
[2] M. Talha, A. Rashid, S. Yussof, Y. Yusoff, R. Ismail. A Review of Security Attacks on IEC 61850 Substation Automation System Network.Center for Information and Network Security. College of Information Technology. University Tenaga Nasional. Malaysia. Noviembre 2014.
[3] Consejo Nacional de Operación. Acuerdo CNO788. Septiembre 3 de 2015. Tomado de: https://www.cno.org.co/sites/default/files/documentos/acuerdos/ACUERDO%20788.PDF
[4] Consejo Nacional de Operación. Acuerdo CNO701. Septiembre 10 de 2014. Tomado de: https://www.cno.org.co/sites/default/files/documentos/acuerdos/acuerdo701.PDF
[5] B. Nartmann, T. Brandstetter, Dr. K. Knorr, "Cyber Security for Energy Automation Systems – New Challenge for Vendors," Part 1, 2009. CIRED 2009, 20th International Conference on Electricity Distribution. Septiembre 2009.
[6] Cybersecurity Ventures. Ransomware Damage Report. Page One for Ransomware Statistics. Mayo 2017 Tomado de: http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
[7] L. O. Murchu. "Stuxnet – Infecting Industrial Control Systems". Symantec Security Response. Septiembre 2010.
[8] A. Cherepanov, R. Lipovsky. "Industroyer: Biggest threat to industrial control systems since Stuxnet". Junio 2017 Tomado de: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
[9] IEC TC57: Estándar IEC 62351 - Power systems management and associated information exchange - Data and communications security - ALL PARTS. Marzo 2013.
[10] A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger. "Towards the Smart Grid: Substation Automation Architecture and Technologies. Advances in Electrical Engineering". Agosto 2014.
[11] A. Elgargouri, R.Virrankoski, M. Elmusrati. "IEC 61850 Based Smart Grid Security.Department of Computer Science". University of Vaasa.Vaasa, Finland. Marzo 2015.
[12] S. Fries, H.-J. Hof, M. Seewald, "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments," 2010 Fifth International Conference on Internet and Web Applications and Services (ICIW). Mayo 2010.
[13] Z. Li, M. Shahidehpour, F. Aminifar. Cybersecurity in Distributed Power Systems. Mayo 2017.
[14] O. Mikhail Sheyner. Scenario Graphs and Attack Graphs. Department of Computer Science, University of Memphis. Abril 2004.
[15] IEC TC57: Estándar IEC 61850 - Communication networks and systems for power utility automation - ALL PARTS. Marzo 2013.
[16] T. Waluyo, B. Rahardjo, Kuspriyanto. Some Framework, Architecture and Approach for Analysis A Network Vulnerability. School of Electrical Engineering & Informatics, Institut Teknologi Bandung. Jl. Ganesha 10 Bandung 40132, Indonesia. Septiembre 2012.

Fecha de presentación: 13 de Diciembre del 2017



Firma del Autor

Firma del Director

Nota: Con su firma el(los) director(es) están aprobando el proyecto o la propuesta. El profesor responsable debe ingresar en el SIA la calificación del proyecto o la propuesta.