



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

**ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD
APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA
NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686**

José René Gallardo Monterroso

Asesorado por el Ing. Ernesto Rafael Estrada Quiñonez

Guatemala, septiembre de 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD
APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA
NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA

POR

JOSÉ RENÉ GALLARDO MONTERROSO

ASESORADO POR EL ING. ERNESTO RAFAEL ESTRADA QUIÑONEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRICISTA

GUATEMALA, SEPTIEMBRE DE 2022

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANA	Ing. Aurelia Anabela Cordova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANA	Inga. Aurelia Anabela Cordova Estrada
EXAMINADOR	Ing. José Guillermo Bedoya Barrios
EXAMINADOR	Ing. Gustavo Benigno Orozco Godínez
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD
APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA
NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE1686**

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 4 de noviembre de 2020.



José René Gallardo Monterroso



Ing. Fernando Alfredo Moscoso Lira
Coordinador Área de Potencia
Facultad de Ingeniería
Universidad de San Carlos de Guatemala


Estimado ingeniero,

Por este medio autorizo enviar a usted el informe final correspondiente al Trabajo de Graduación (Tesis) titulado: "ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686", desarrollado por el estudiante JOSÉ RENÉ GALLARDO MONTERROSO, con registro académico número 201020489, quien fue asesorado por el suscrito.

Por lo tanto, al encontrarlo satisfactorio en su contenido y resultados, me permito dar aprobación al mismo, remitiéndose a esa Dirección para el trámite pertinente.

Agradeciendo de antemano la atención a la presente, quedamos a sus órdenes.

Atentamente,


Ernesto Rafael Estrada Quiñonez
Ing. Mecánico Electricista
Colegiado No. 13,555

Ing. Ernesto Rafael Estrada Quiñonez
Colegiado 13555
Asesor

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE INGENIERÍA

Guatemala, 17 de mayo de 2022

Ingeniero
Armando Alonso Rivera Carrillo
Director
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Ingeniero Rivera:

Por este medio, con base a lo indicado en el REGLAMENTO DE TRABAJOS DE GRADUACION vigente, tengo a bien proponer la aprobación del trabajo de graduación titulado:

**ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD
APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA
NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686**

del estudiante JOSÉ RENÉ GALLARDO MONTERROSO, habiendo cumplido con los requisitos establecidos en el referido reglamento y conforme la aprobación del asesor y el revisor.

Sin otro particular

Atentamente,
ID Y ENSEÑAD A TODOS

Una firma manuscrita en tinta negra, que parece ser la del Ingeniero Fernando Alfredo Moscoso Lira, escrita sobre una línea horizontal.

Ingeniero Fernando Alfredo Moscoso Lira
Coordinador Área de Potencia
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería

REF. EIME 55.2022.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante José René Gallardo Monterroso: **ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686**, procede a la autorización del mismo.



Ing. Armando Alonso Rivera Carrillo

Guatemala, 29 de agosto de 2022.

LNG.DECANATO.OI.660.2022

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **ESTUDIO DE PRE-FACTIBILIDAD PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD APLICADA A SUBESTACIONES ELÉCTRICAS DE TRANSMISIÓN DEL SISTEMA NACIONAL INTERCONECTADO CON BASE EN LAS NORMAS IEEE C37.240 E IEEE 1686**, presentado por: **José René Gallardo Monterroso**, después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:



ing. Aurelia Anabela Cordova Estrada

Decana

Guatemala, septiembre de 2022

AACE/gaoc

ACTO QUE DEDICO A:

Dios

Por ser la fuente de inspiración y fortaleza para seguir adelante en la vida, y en el transcurso de la carrera.

Mis padres

Julio Gallardo y Carmen Monterroso de Gallardo, por todos su amor y apoyo en muchos aspectos, principalmente en los ámbitos moral y económico.

AGRADECIMIENTOS A:

- | | |
|---|---|
| Universidad de San Carlos de Guatemala | Por ser la casa de estudios donde puede nutrirme de conocimientos en el transcurso de toda la carrera. |
| Facultad de Ingeniería | Por brindarme la oportunidad de estudiar la carrera de ingeniería eléctrica y permitirme la formación y adquisición de conocimientos durante todos los cursos de la carrera en sus instalaciones. |
| Mis amigos de la Facultad | Por el apoyo brindado en los cursos y por sus recomendaciones y buenos consejos. |
| Mi asesor de tesis | Ernesto Estrada, por ser un apoyo fundamental en la elaboración del presente trabajo de graduación. |

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	IX
LISTA DE SÍMBOLOS	XIII
GLOSARIO	XV
RESUMEN	XXXIII
OBJETIVOS.....	XXXV
HIPÓTESIS.....	XXXVII
INTRODUCCIÓN	XLI
1. GENERALIDADES DE CIBERSEGURIDAD EN SUBESTACIONES	1
1.1. Implementación de seguridad cibernética en una subestación.....	4
1.1.1. Ciberseguridad en la red de comunicación en una subestación.....	9
1.1.1.1. SNMP.....	10
1.1.1.2. RADIUS.....	13
1.1.1.3. TACACS.....	14
1.1.1.4. SSH.....	15
1.1.1.5. Seguridad por medio de <i>switch</i> de comunicación	17
1.1.1.6. Seguridad con <i>router</i> (enrutador)	17
1.1.1.7. Seguridad por medio de <i>firewall</i>	18
1.1.1.8. Seguridad de <i>Gateway</i>	20
1.1.1.9. VPN.....	21
1.1.1.9.1. Open VPN.....	21
1.1.1.9.2. IPSec	22

1.2.	Las demandas e implicaciones de la colaboración de IT y OT	22
1.2.1.	Tecnología operativa (OT).....	24
1.2.2.	Tecnologías de la Información (IT)	25
1.2.2.1.	Impacto de la IT en la infraestructura de la industria eléctrica	26
1.2.3.	Colaboración entre IT y OT	27
1.2.4.	IT y OT tienen criterios de aceptación muy diferentes.....	29
1.2.5.	Intersecciones IT y OT	33
1.3.	Ataques a sistemas eléctricos	34
1.3.1.	Ataque a la red eléctrica de Ucrania.....	34
1.3.1.1.	Descripción de las tácticas del ataque.....	36
1.3.1.2.	Las vulnerabilidades del sistema	38
1.3.1.3.	Uso de la cadena de Cyber Kill de ICS.....	39
1.3.1.4.	Ataque a Ucrania aplicado a etapa 1	44
1.3.1.5.	Aplicado a etapa 2	46
1.3.2.	Otros ataques en el transcurso de la historia	47
1.4.	Normas aplicables para ciberseguridad en subestaciones eléctricas	50
1.4.1.	IEEE C37.240.....	51
1.4.2.	IEEE 1686	52
1.4.3.	IEC 62351	54
2.	SUBESTACIONES ELÉCTRICAS	55
2.1.	Subestaciones convencionales	55
2.1.1.	Subestaciones aisladas en aire (AIS).....	58

2.1.2.	Subestaciones aisladas en gas (GIS)	58
2.1.3.	Aparamenta de tecnología mixta (MTS)	59
2.1.4.	Tipos de subestaciones	60
2.1.4.1.	Subestaciones de generación	61
2.1.4.2.	Subestaciones de maniobra	61
2.1.4.3.	Subestaciones de transformación	61
2.1.5.	Configuraciones de las subestaciones.....	62
2.1.6.	Niveles de control/operación de las subestaciones	63
2.1.6.1.	Nivel de patio (nivel 0).....	64
2.1.6.1.1.	Interruptores de potencia	67
2.1.6.1.2.	Seccionadores	68
2.1.6.1.3.	Transformadores de instrumentos	69
2.1.6.1.4.	Transformadores de corriente	70
2.1.6.1.5.	Transformadores de tensión	76
2.1.6.1.6.	Clases de precisión para protección	77
2.1.6.2.	Nivel de automatización (nivel 1)	77
2.1.6.2.1.	Relevadores de protección	78
2.1.6.2.2.	Registrador de fallas	85
2.1.6.2.3.	Controlador de bahía	86
2.1.6.2.4.	Equipos de medición.....	87
2.1.6.2.5.	Equipos de monitoreo ...	88

2.1.6.3.	Nivel de control de la subestación (nivel 2)	88
2.1.6.3.1.	<i>Switch</i> de comunicación.....	88
2.1.6.3.2.	<i>Gateway</i>	99
2.1.6.3.3.	Unidad Terminal Remota (RTU)	101
2.1.6.3.4.	Human Machine Interface –HMI-	108
2.1.6.4.	Nivel 3, nivel de estación (Centro de Control)	111
2.1.6.5.	Generalidades Estándar IEC 61850 ...	116
2.1.6.6.	Clasificación de redes.....	121
2.1.6.6.1.	Redes de Área Local (LANs)	121
2.1.6.6.2.	Redes de área metropolitana (MANs)..	122
2.1.6.6.3.	Redes de área amplia (WANs).....	123
2.1.6.6.4.	Redes Virtuales Privadas (VPNs)	124
2.1.6.7.	Topologías de red de comunicaciones	125
2.1.6.7.1.	Bus	125
2.1.6.7.2.	Cascada	126
2.1.6.7.3.	Estrella.....	127
2.1.6.7.4.	Anillo.....	128
2.1.6.7.5.	Malla	129
2.1.6.8.	Comunicaciones en la subestación	129

	2.1.6.8.1.	Conexión serial	130
	2.1.6.8.2.	Protocolo Ethernet	139
3.	SUBESTACIONES DIGITALES		147
3.1.	Arquitectura de las subestaciones digitales		148
3.2.	Equipos de subestaciones digitales		150
3.2.1.	Transformadores ópticos		150
	3.2.1.1.	Transformadores ópticos de corriente	153
	3.2.1.2.	Transformadores de tensión	157
	3.2.1.3.	Mergin Unit.....	160
	3.2.1.4.	Bus de proceso	163
		3.2.1.4.1.	MMS..... 166
		3.2.1.4.2.	GOOSE..... 167
		3.2.1.4.3.	Sampled Values..... 169
3.2.2.	Redundancia.....		170
	3.2.2.1.	Tipos de redundancia..... 170	
		3.2.2.1.1.	PRP
		3.2.2.1.2.	Principio de operación
			HSR
			173
4.	CASO DE SUBESTACIÓN DE 230/69 KV DEL SISTEMA NACIONAL INTERCONECTADO.....		179
4.1.	Análisis causa raíz del problema		179
4.2.	Estudio de mercado		187
4.2.1.	Empresas de transmisión		192
	4.2.1.1.	ETCEE-INDE	193
4.2.2.	TRELEC.....		195
4.2.3.	TRECOSA		198

4.2.4.	Proveedores de equipos con requisitos de ciberseguridad.....	200
4.2.4.1.	SIEMENS.....	200
4.2.4.2.	SEL.....	201
4.3.	Estudio técnico	201
4.3.1.	Vulnerabilidades para nivel 0 (equipos de patio)	205
4.3.2.	Vulnerabilidades para el nivel de automatización (nivel 1).....	206
4.3.2.1.	Vulnerabilidades que aplican a IED's..	206
4.3.2.1.1.	Relevadores de protección	206
4.3.2.1.2.	Vulnerabilidades específicas según estándar IEEE 1686 de los relevadores de protección propuestos en el diseño de la subestación caso de estudio	209
4.3.3.	Vulnerabilidades para el nivel de estación (nivel 2).....	217
4.3.3.1.	<i>Switch</i> de comunicación	218
4.3.3.2.	Unidad Terminal Remota (RTU)	223
4.3.3.3.	<i>firewall</i>	225
4.3.4.	Vulnerabilidades para el nivel Centro de Control (nivel 3).....	229
4.3.4.1.	Vulnerabilidades de la red de la subestación.....	232

4.3.4.2.	Vulnerabilidades en la red del Centro de Control.....	233
4.3.5.	Solución técnica.....	234
4.3.5.1.	Para el nivel 0 de la subestación.....	234
4.3.5.2.	Para el nivel 1 de la subestación.....	235
4.3.5.3.	Nivel de estación (nivel 2)	242
4.3.5.3.1.	<i>Switch</i> de comunicación	251
4.3.5.3.2.	Unidad Terminal Remota (RTU).....	259
4.3.5.3.3.	Solución propuesta para arquitectura incluyendo DMZ	261
4.3.5.3.4.	<i>firewall</i>	262
4.3.5.4.	Recomendaciones para Centro de Control (nivel 3).....	270
4.3.5.5.	Recomendaciones para la red de comunicaciones en la subestación.....	281
4.3.5.6.	Recomendaciones en la red del Centro de Control	291
4.3.6.	Subestación digital.....	293
4.4.	Estudio económico.....	296
CONCLUSIONES		307
RECOMENDACIONES		311
BIBLIOGRAFÍA.....		313
ANEXOS		323

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Diseño de SSH.....	16
2.	Interacción entre IT y OT.....	26
3.	Arquitectura entre IT y OT.....	33
4.	Componentes necesarios para el ciberataque en Ucrania.....	37
5.	Estructura etapa 1.....	41
6.	Estructura etapa 2.....	42
7.	Modelo del mapa del ciberataque con Cyber Kill.....	44
8.	Análisis estático de API.....	47
9.	Países afectados por Dragonfly.....	48
10.	Configuración de subestaciones según su tendencia.....	63
11.	Niveles de mando de subestaciones.....	64
12.	Interruptores de potencia de tanque muerto.....	68
13.	Seccionadores de apertura central.....	69
14.	Simbología para transformadores de corriente.....	71
15.	Curva de saturación del transformador de corriente.....	73
16.	Gráfica del punto rodilla según norma ANSI.....	74
17.	Forma de onda para el flujo magnético.....	75
18.	Esquema de funcionalidades de los relevadores de protección.....	80
19.	Zonas de protección de una subestación.....	81
20.	Zonas de protección definidas por los CTs.....	81
21.	Zonas de protección definidas para un sistema completo.....	82
22.	Relevadores marca SIEMENS y SEL.....	83
23.	Switch de comunicación.....	89

24.	Conmutación en un <i>switch</i> de comunicación	98
25.	Funcionalidad de la RTU aguas abajo	105
26.	Funcionalidad de la RTU aguas arriba.....	106
27.	Clasificación de protocolos de comunicación	130
28.	Configuración <i>Full Duplex</i>	137
29.	Configuración <i>Half Duplex</i>	138
30.	Capas del modelo OSI.....	140
31.	Limitaciones de capa 1 y capa 2.....	141
32.	Subcapas IEEE mayores	144
33.	Topología de los sistemas de automatización de subestaciones digitales.....	148
34.	Clasificación de los transformadores ópticos	152
35.	Esquema de constitución de elementos de un transformador óptico	153
36.	Diagrama de transformador de corriente óptico con elementos pasivos.....	156
37.	Conversión de señales eléctricas a ópticas	157
38.	Estructura de un captador por efecto Pockels	158
39.	Implementación de una Mergin Unit 6MU85	161
40.	Entradas en una <i>Merging Unit</i>	163
41.	Mensajería según estándar IEC 61850.....	166
42.	Esquema de configuración de PRP	172
43.	Esquema de configuración de HSR para Multicast.....	174
44.	Esquema de configuración de HSR para Unicast.....	176
45.	Diagrama de eventos y factores causales	186
46.	Variación del PIB de Guatemala del año 2014 al 2022.....	188
47.	Variación en millones de GTQ de la categoría de suministro de electricidad en el periodo del año 2014 al 2022.....	190
48.	Diagrama unifilar de subestación.....	203

49.	Arquitectura de comunicación de subestación	204
50.	Zona DMZ propuesta	248
51.	Solución propuesta para Arquitectura de comunicación incluyendo la DMZ	261
52.	Diseño de arquitectura de comunicación en un Centro de Control implementando defensa en profundidad	272
53.	Niveles de mando de una subestación digital	294
54.	Diagrama de flujo de la implementación en subestaciones.....	304

TABLAS

I.	Niveles de seguridad.....	7
II.	Partes que conforman el estándar IEC 62351	54
III.	Valores normales de tensiones entre fases	56
IV.	Valores de relaciones para transformadores de corriente según ANSI.....	72
V.	Clase de precisión para PT según norma IEC	77
VI.	Partes del Estándar 61850	119
VII.	RS-232 DB-9 Pinout (DTE)	133
VIII.	RS-232 DB-9 Pinout (DCE).....	134
IX.	Rango de voltaje para las lógicas en EIA-232.....	134
X.	Estándares LAN basados en Ethernet	145
XI.	Formas para diagrama de eventos y factores causales	185
XII.	Variación del PIB de Guatemala durante el periodo 2014 al 2018.....	187
XIII.	Variación del PIB de Guatemala durante el periodo 2019 al 2022.....	188
XIV.	Porcentaje de participación de la categoría de suministro de electricidad, agua y saneamiento en el PIB de Guatemala	190
XV.	Longitud de líneas de transmisión, en kilómetros, por nivel de tensión y por tipo de propiedad, al mes de diciembre de 2018.....	192

XVI.	Costos para la implementación de ciberseguridad en nivel de patio nivel 0	297
XVII.	Costos para la implementación de ciberseguridad en nivel 1	298
XVIII.	Costos para la implementación de ciberseguridad en nivel 2	299
XIX.	Costos para la implementación de ciberseguridad en nivel 3	301
XX.	Costos de equipos que incluyen funciones de ciberseguridad	302
XXI.	Costos para la implementación de ciberseguridad en su totalidad para subestaciones eléctricas en servicio (basado en las características técnicas indicadas en el caso propuesto del presente estudio de prefactibilidad)	303

LISTA DE SÍMBOLOS

Símbolo	Significado
A	Amperio (s)
Gbps	Gigabit por segundo
Hz	Hercio
kA	Kiloamperio (s)
km	Kilómetro (s)
kV	Kilovoltio (s)
kW	KiloWatt (s)
m	Metro (s)
Ω	Ohm
%	Porcentaje
s	Segundo (s)
V	Voltio (s)

GLOSARIO

AAA	<i>Authentication, Authorization and accounting.</i>
ACL	<i>Access Control List.</i>
ACL	Una lista de control de acceso es una serie de instrucciones que permite seleccionar el paso o bloqueo de paquetes IP hacia una red interna, es para uso exclusivo en <i>routers</i> o <i>firewall</i> y se puede configurar de acuerdo a las necesidades del usuario.
AIS	Subestación Aislada en aire.
Ancho de banda	Capacidad de transporte de datos de un canal de comunicación. Rango de frecuencia donde se concentra la mayor potencia de la señal.
Anillo	Topología de red en la que cada dispositivo en dicha red, se unen unos con otros formando un lazo cerrado por medio de conductores. El último nodo de la cadena se conecta al primero cerrando el anillo.
ANSI	American National Standards Institute (Instituto Nacional Estadounidense de Estándares). Organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios,

procesos y Sistemas en los Estados Unidos de América.

Arquitectura

Estructura de la disposición de equipos organizada jerárquicamente con la finalidad de permitir el intercambio de datos entre los diversos dispositivos ubicados en los distintos niveles de una red de comunicación.

AT

Alta Tensión.

Auditoría

En este proceso se lleva un control de las actividades de ingresos exitosos de los diversos usuarios y los intentos de ingreso fallidos que se realizan en los dispositivos protegidos y en general para el sistema.

Autenticación

Procedimiento que permite asegurar que un usuario de un servicio sea quien dice ser al identificarse.

Autorización

Es la acción que determina si un usuario puede acceder al sistema de un dispositivo IED o al sistema de la subestación.

BFA

Brute Force Attack.

Broadcast

Es la difusión de paquetes de datos a través de redes, la información se transmite a todos los dispositivos de la red y se envían al mismo tiempo en toda la subred

IP, de manera que todos los Host reciben los paquetes.

BT	Baja tensión.
Bus	Topología de comunicación que trabaja de forma horizontal para enviar la información entre equipos.
CA	Certification Authority.
Cifrado	El cifrado o encriptación de datos, es la conversión de datos de un formato legible a un formato codificado, de manera que los datos cifrados solo se pueden leer o procesar después descriptarlos.
CNEE	Comisión Nacional de Energía Eléctrica.
Corriente eléctrica	Flujo de electrones que recorre un material conductor de electricidad.
DDoS	Los ataques de negación de servicio distribuido dejan sin acceso a los usuarios a su equipo o red, enviando una cantidad masiva de peticiones al servicio desde múltiples direcciones IP.
Defensa en profundidad	Conjunto de medidas de seguridad para proteger la integridad de la información.

<i>Display</i>	Dispositivo que permite mostrar información al usuario de forma visual.
DMZ	<i>Desmilitarized Zone.</i>
DMZ	La zona desmilitarizada o red perimetral se encuentra entre una red interna y una red externa. Se implementa para proteger la red interna por medio de <i>firewall</i> , este elige la información que ingresa y egresa de la red interna, y la DMZ también cuenta con servidores destinados a realizar diversas funciones.
DNP	Por sus siglas en inglés <i>Distributed Network Protocol</i> , es un protocolo industrial que se utiliza para la comunicación que implica la adquisición de información y envío de comandos de control entre dispositivos separados físicamente. Se utiliza frecuentemente para enviar datos a sistemas SCADA.
DoS	<i>Denial of Service.</i>
Dos	Por su significado en inglés <i>Denial of Service</i> , es un ataque cuya función es privar a los usuarios del acceso a su red o equipo. Se logra enviando una cantidad masiva de peticiones al servicio desde una misma dirección IP.
EAP	<i>Extensible Authentication Protocol</i> , es un marco arquitectónico que proporciona extensibilidad para los

métodos de autenticación en tecnologías de acceso a redes protegidas más usadas.

EAP

Extensible Authentication Protocol.

Energía eléctrica

Es la forma de energía causada por un diferencial de potencial entre dos puntos entre los que se establece una corriente eléctrica.

Equipo primario

Conjunto de equipos que se encuentran instalados en el patio de una subestación y cuya funcionalidad es realizar operaciones de maniobra, apertura y cierre, de circuitos en las diversas bahías que conforman la subestación y medición de magnitudes eléctricas en los sistemas de potencia de alta tensión.

ETCEE

Empresa de transporte y control de energía eléctrica.

firewall

Es un dispositivo de seguridad que monitorea la información contenida en el tráfico de una red, dependiendo de la lista de control de acceso que se configure, esta deja pasar únicamente la información seleccionada a la red interna evitando que los virus o cualquier *malware* infecten los elementos contenidos dentro de la red protegida.

Firmware

Software que maneja físicamente al hardware para que las instrucciones externas se ejecuten de forma correcta.

FO	Fibra óptica.
GIS	Subestación aislada en Hexafloruro de Azufre.
GOOSE	Estructura y metodología que pertenece al estándar IEC 61850, facilita compartir información de tiempo real entre equipos que conforman una red de comunicación LAN.
GTQ	Moneda Quetzal de Guatemala.
<i>Hacking</i>	Conjunto de técnicas a través de las que se accede ilícitamente a un sistema informático haciendo vulnerables las medidas de seguridad implementadas.
<i>Hardening</i>	Es un conjunto de medidas cuyo objetivo es reforzar el sistema contra amenazas cibernética, de manera que se reducen sus vulnerabilidades haciendo un sistema confiable.
<i>Hardware</i>	Conjunto de materiales que conforman la parte física de un ordenador o sistema informático que se compone de elementos electromecánicos y electrónicos.
<i>Hash</i>	Es una función criptográfica que consiste en un algoritmo matemático que transforma cualquier bloque arbitrario de datos, independientemente de su

longitud, en una nueva serie de caracteres con una longitud fija.

HMI

Human Machine Interface.

Host

Es un nodo, ordenador o conjunto de dispositivos que funcionan como el punto de inicio y final de una transferencia de datos. Un host de internet tiene una dirección de internet única, la IP, y un nombre de dominio único o nombre de Host.

HSR

Por sus siglas en inglés *High-available Seamless Redundancy*, realiza redundancia en una red de comunicación donde envía dos tramas idénticas que son enviadas por medio de dos puertos del IED hacia una red con topología en anillo.

HTTP

HyperText Transfer Protocol.

HTTPS

HyperText Transfer Protocol Secure.

HTTPS

Por sus siglas en inglés Hypertext Transfer Protocol Secure, el protocolo seguro de transferencia de hipertexto es una versión del protocolo de transferencia que utiliza un cifrado seguro para la comunicación. La comunicación entre el cliente web y el servidor se envía cifrada.

ICS	Sistema de Control Industrial, abarca varios tipos de sistemas de control e instrumentos utilizados para el control de procesos industriales.
IDS	<i>Intrusion Detection System</i> , el Sistema de detención de intrusiones es una aplicación usada para detectar accesos no autorizados a la red y a los dispositivos que la conforman.
IDS	<i>Intrusion Detection System.</i>
IEC	Comisión electrotécnica internacional. International Electrotechnical Commission por sus siglas en inglés. Organización de normalización en los campos de electricidad, electrónica.
IED	Por sus siglas en inglés <i>Intelligent Electronic Device</i> , un dispositivo electrónico inteligente se utiliza en la industria del campo de potencia eléctrica para realizar funciones vitales de protección, control y medición de los elementos primarios y activos de una subestación.
IEEE	Instituto de ingeniería eléctrica y electrónica. Institute of Electrical and Electronics Engineers por sus siglas en inglés.
IHM	Interfaz Hombre máquina.
INDE	Instituto Nacional de Electrificación.

Interfaz	Es la representación de la conexión funcional entre dos sistemas, programas, dispositivos o componentes ya sea de hardware o software.
IP	Es una dirección única, cuya función principal es identificar a un dispositivo en una red local o en internet; es una cadena de números separados por puntos, el rango va desde 0.0.0.0 hasta 255.255.255.255.
IPsec	Conjunto de protocolos que asegura la comunicación sobre una red insegura, de manera que realiza cifrado en cada paquete IP en un flujo de datos.
IPsec	<i>Internet Protocol Security.</i>
IT	<i>Information Technology.</i> Abarca las tecnologías referidas a la gestión de información; implica un área de dispositivos que hacen posible el flujo de datos en una red.
LAN	La red de área local consiste en una estructura que permite vincular sus diversos componentes para compartir información entre ellos, la conexión se realiza por medio de cable normalmente Ethernet de cobre o fibra óptica.
LAN	<i>Local Area Network.</i>

Línea de transmisión	Es el medio físico que permite conducir energía eléctrica entre dos puntos. Las líneas podrán ser de transmisión o de distribución de acuerdo con su función.
MAC	<i>Media Access Control.</i>
Malware	Es un software malicioso cuyo objetivo es infiltrarse en un dispositivo y realizar daños o extracción de información en los mismos. Existen diversos tipos bajo la categoría de <i>malware</i> , como son los virus informáticos, gusanos informáticos, Troyanos, <i>Spyware</i> , <i>Adware</i> y <i>Ransomware</i> .
Mergin Unit	Es un IED que permite digitalizar las señales analógicas que provienen de los equipos de patio, específicamente de los transformadores de instrumentos.
MMS	Tipo de mensaje que se implementa al hacer uso del estándar IEC 61850, se utiliza para transmitir comunicación de manera vertical debido a que puede intercambiar información entre nodos lógicos en la red de comunicación.
MT	Media Tensión.
MU	<i>Mergin Unit.</i>

Multicast	Es un protocolo estándar para hacer uso en redes LAN e internet, se envían mensajes utilizando direcciones IP, direccionándolas en toda la red y permitiendo la transmisión desde un punto a múltiples dispositivos destinatarios, de manera que solo reciben el mensaje los dispositivos interesados dependiendo la dirección que se le asigne al mensaje. Se conoce también como conexión punto o multipunto.
NAS	Servidor de Acceso a Red.
NTP	Network Time Protocol.
OSI	<i>Open Systems Interconnection.</i>
OT	Operation Technology. Abarca las tecnologías que se utilizan para la operación de activos físicos.
PCyM	<i>Protección, Control y Medida.</i>
Phishing	Conjunto de técnicas cuyo objetivo es el robo de contraseñas e información confidencial por medio del envío de correos electrónicos de personas, empresas o servicios de confianza que fingen ser auténticos.
PIB	Producto Interno Bruto.
PKI	Por su acrónimo en inglés <i>Public Key Infrastructure</i> , permite a los usuarios autenticarse entre sí mediante

certificados digitales emitidos por una Autoridad de Confianza (AC).

Potencia eléctrica Es la cantidad de energía entregada o absorbida por un elemento en un tiempo determinado.

Proxy Es un tipo de *firewall* que brinda seguridad y almacenamiento de contenido, son equipos intermediarios entre la red interna y externa, analiza y registra todo el tráfico de entrada y salida.

PRP Por sus siglas en inglés *Paralell Redundancy Protocol*, permite una comunicación de datos sin tiempos de conmutación, haciendo posible que en el caso de que un IED falle, se encuentre otro de respaldo manteniendo el servicio.

RADIUS Remote Authentication Dial in User Service. Es un protocolo que utiliza la autenticación y autorización para usuarios antes de brindarle acceso a una red.

Ransomware Es un tipo de *malware* que, por medio de diversos métodos, restringe el acceso a partes del sistema operativo infectado y extrae información de manera que pide un pago (extorsión), al usuario afectado a cambio de la recuperación de información.

RBAC Por sus siglas en inglés, el control de acceso basado en roles consiste en definir roles para los usuarios de

manera que se tengan niveles de acceso a la red e información confidencial.

RDP	<i>Remote Desktop Protocol.</i>
Router	Es un dispositivo de red cuya función es administrar el tráfico que circula en una red.
RSA	El sistema criptográfico con clave pública es un algoritmo asimétrico de bloques; se basa en números primos para generar las claves para descifrado.
RTU	Unidad Terminal Remota, se encarga de reunir toda la información que los IEDs envían hacia niveles superiores de la subestación. Este dispositivo se encuentra ubicado físicamente en el bus de estación y prepara la información para enviarlo a un SCADA.
Sampled Values	Esta clase de dato se utiliza para representar muestras de valores analógicos instantáneos, provenientes de una <i>Mergin Unit</i> y los introduce en una red de comunicaciones donde se utilice el estándar IEC 61850, tiene mayor aplicación en subestaciones digitales.
SCADA	Sistema de supervisión y adquisición de datos (<i>Supervisory Control and Data Acquisition</i>).

Señal analógica	Es una onda sinusoidal con variación continua de amplitud y periodo en función del tiempo.
Señal digital	Es el tipo de señal que presenta su contenido en valores discretos. Se utiliza en la lógica binaria.
SFTP	Por sus siglas en inglés <i>Secure File Transfer Protocol</i> , es un protocolo de nivel de aplicación que permite la transferencia y manipulación de archivos de archivos sobre un flujo de datos fiable, se utiliza con SSH para brindar seguridad mediante cifrado de datos.
SIEM	Su significado en español es la gestión de información y eventos de seguridad. Es un software cuya función es detectar fallas y amenazas de seguridad y al mismo tiempo tiene la capacidad de neutralizar dichas fallas.
Sistema monofásico	Sistema eléctrico caracterizado por constituirse de una sola fase eléctrica.
Sistema trifásico	Sistema eléctrico caracterizado por constituirse de tres fases eléctricas.
SNI	Sistema Nacional Interconectado.
SNMP	Por sus siglas en inglés <i>Simple Network Management Protocol</i> , es un protocolo de la capa de aplicación, facilitando el intercambio de información entre los dispositivos de red; posee diversas versiones, siendo

la tercera edición la más confiable pudiendo encriptar la información que se transfiere.

Software

Es el soporte lógico de un sistema informático que comprende del conjunto de componentes lógicos que hacen posible la realización de tareas específicas.

SSH

Por sus siglas en inglés *Secure Shell*, es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente servidor y que permite a los usuarios conectarse a un host remotamente utilizando un canal donde toda la información se transfiere de manera cifrada.

SSL

Secure Sockets Layer.

SV

Sampled Values.

TACACS

Terminal Access Controller Access Control System.

TCP

Es un protocolo de comunicaciones donde los datos pueden enviarse de forma bidireccional una vez establecida la conexión y asegurando la transferencia de datos a través de los sistemas de red.

Tensión

Voltaje o diferencial de potencial que existe entre dos puntos.

TLS	Por sus siglas en inglés <i>Transport Layer Security</i> , seguridad en la capa de transporte, es un protocolo de los más utilizados para el cifrado de datos. Se utiliza para transmitir información en redes inseguras como es el internet, asegurando el grado más alto de integridad para los usuarios.
TLS	<i>Transport Layer Security.</i>
TOC	Es la tabla de cumplimiento que propone el estándar IEEE 1686 para que se implementen buenas prácticas de ciberseguridad en los IEDs.
TOC	<i>Table of Compliance.</i>
Topología de red	Es la forma en que se organizan, distribuyen y conectan entre ellos los equipos que conforman una red de comunicaciones.
TRECSA	Transportadora de Energía de Centroamérica, S.A., es una empresa transportista de energía eléctrica en alta tensión, es filial del Grupo Energía Bogotá.
TRELEC	Transportista Eléctrica Centroamericana, S.A., es una empresa transportista de energía eléctrica en alta tensión que forma parte del Grupo EPM.
UDP	Es un protocolo, por su significado en <i>inglés User Datagram Protocol</i> , de la capa de transporte que

permite la transmisión de datos sin conexión previa, por consiguiente, es posible enviar información sin confirmar la conexión y esperar respuesta de que los datos se entregaron correctamente en el equipo de destino.

USD

Dólar de los Estados Unidos de América.

Virus informático

Es un tipo de *malware* cuya función después de infiltrarse es modificar y alterar el funcionamiento del equipo infectado.

VLAN

Red de área Local Virtual permite crear redes lógicas independientes dentro de la misma red física de red de área local (LAN).

VPN

Una *Virtula Private Network*, consiste en un método para obtener una conexión a internet de forma privada.

Zona segura

Es un perímetro conformado por diversos activos que se agrupan según su ubicación física en la subestación o bien, por su funcionalidad dentro de una subestación y son protegidos por diversos elementos.

RESUMEN

El presente trabajo de graduación propone una guía, para la implementación de ciberseguridad en las subestaciones eléctricas de transmisión del Sistema Nacional Interconectado, dada la migración que desde hace varios años las tecnologías dependen cada vez más del internet de las cosas y de protocolos de comunicación, estos son muy vulnerables desde las redes que se diseñan para elementos de tecnologías operativas.

Las subestaciones eléctricas actualmente cuentan con ciertas medidas de seguridad, sin embargo, la ciberseguridad aún no se implementa como un requisito fundamental para la protección de los activos de las subestaciones y la protección de información. Se consideran principalmente las recomendaciones indicadas en los estándares IEEE C37.240 e IEEE 1686, son los focos de estudio para el presente trabajo.

En el capítulo uno se plantean conceptos generales de ciberseguridad quienes son importantes para ayudar a comprender las buenas prácticas y protocolos que se pueden implementar en las subestaciones eléctricas, como lo es la implementación de defensa en profundidad, al mismo tiempo se plantean las diferencias y la necesidad de colaboración entre las tecnologías de la información y las tecnologías operativas, también se hace referencia a antecedentes de ataques cibernéticos a sistemas eléctricos de potencia.

En el capítulo dos se indican los conceptos básicos de una subestación convencional, realizando descripciones de los equipos principales que la conforman, dependiendo del nivel de mando donde se ubican como son: los

equipos primarios, los relevadores de protección, controladores de bahía, medidores de energía, unidades terminales remotas, HMIs y sistemas SCADA. Al mismo tiempo se describen diversos protocolos que son aplicados en los distintos niveles de la subestación.

En el capítulo tres se realiza una introducción de los conceptos fundamentales para la implementación de subestaciones digitales, haciendo énfasis en los equipos que difieren de las subestaciones convencionales y mencionando los elementos fundamentales para la operación como es el bus de proceso y el uso definitivo del protocolo IEC 61850 para la comunicación en toda la subestación.

En el capítulo cuatro se realiza los diversos estudios para el desarrollo del estudio de prefactibilidad, siendo estos: el estudio técnico, el estudio económico, el análisis causa raíz del problema y un estudio de mercado. En el estudio técnico se analizan las características de IEDs de las marcas SIEMENS Y SCHWEITZER ENGINEERING LABORATORIES (SEL), y se comparan con los requisitos que indica el estándar IEEE 1686.

Al mismo tiempo se propone un modelo de estudio de una arquitectura de comunicación; es elaborada con condiciones supuestas para proteger la información privada de las distintas subestaciones y se compara el sistema con las recomendaciones que propone el estándar IEEE C.37.240 desde el equipo de patio y acceso físico a la subestación, los equipos de control y protección sus protocolos de comunicación y los equipos del bus de estación y sus protocolos, estableciendo una zona segura dentro de la subestación.

OBJETIVOS

General

Realizar un estudio de prefactibilidad para la implementación de ciberseguridad en proyectos de subestaciones eléctricas del Sistema Nacional Interconectado (SNI), definiendo un análisis de beneficios técnicos con base en las normas aplicables y preparando la viabilidad de aspectos estructurales, técnicos y económicos. Este estudio puede servir de referencia y ser una guía para las empresas transportistas nacionales que estén interesadas en implementar ciberseguridad en sus proyectos de subestaciones eléctricas de transmisión.

Específicos

1. Elaborar un análisis causa raíz del motivo por el cual no se ha considerado la adecuada implementación de ciberseguridad en las subestaciones de transmisión que actualmente funcionan en el sistema nacional interconectado (SNI).
2. Determinar desde un punto de vista general, la posibilidad de inversión que las distintas empresas de transmisión de energía eléctrica, podrían tener para proyectos de ciberseguridad en sus subestaciones eléctricas de transmisión, tomando como referencia el comportamiento del producto interno bruto de Guatemala en los últimos años.

3. Definir los beneficios económicos de la implementación de ciberseguridad en las subestaciones eléctricas de transmisión, cuando la ciberseguridad es considerada desde el diseño de las mismas, y para las subestaciones eléctricas de transmisión ya construidas y en funcionamiento, considerando tanto los elementos propios de la subestación y en el Centro de Control.
4. Hallar los diferentes métodos técnicos de implementación de protección para el acceso a los dispositivos de operación de una subestación eléctrica; equipos primarios (de patio), equipos de protección, control y monitoreo.
5. Obtener la viabilidad de implementar una arquitectura de comunicación segura en las subestaciones eléctricas de transmisión de acuerdo con las normas aplicables, de manera que se consideren buenas prácticas de ciberseguridad entre equipos IEDs, RTUs, *switches* de comunicación, *firewall* y su interacción con el Centro de Control de la subestación.
6. Establecer los trabajos de configuración necesarios a realizar en sitio de equipos ya instalados en las subestaciones eléctricas de transmisión, para aprovechar las funciones de ciberseguridad que incluyen los relevadores de protección y unidades terminales remotas de las marcas SIEMENS y SEL.

HIPÓTESIS

En su totalidad, la Ciberseguridad en subestaciones eléctricas de transmisión en Guatemala no se ha aplicado debido a diversas causas de origen económico y técnico, factores como filosofía de diseño, o complicaciones durante el desarrollo de proyectos para la implementación en la automatización, protección, control y comunicación en subestaciones.

Si bien es cierto que en Guatemala se realiza constantemente un salto positivo hacia las tecnologías actualizadas, esto se hace de una manera no segura, principalmente por la falta de asignación presupuestaria en los proyectos y falta de prevención, además que la cultura de ciberseguridad principalmente, no se tiene totalmente adquirida en el medio de las subestaciones eléctricas de Guatemala, dado que la implementación de ciberseguridad se aplicó primeramente a tecnologías de la información (IT), y ha sido con el paso del tiempo que se ha implementado a las tecnologías de la operación (OT), así mismo, la falta de capacitación al personal de las empresas transmisoras ha sido un factor importante, estas causas y sus efectos son ampliados en el análisis causa raíz en el capítulo cuatro del presente estudio de prefactibilidad

La Ciberseguridad en las subestaciones eléctricas del sistema nacional interconectado contribuirá reduciendo y previniendo cortes de energía inesperados provenientes de ataques o terrorismo cibernético dirigidos a subestaciones eléctricas de transmisión convencionales y en un futuro no muy lejano, cuando se tengan incluidas subestaciones digitales en el SNI. Si las subestaciones se preparan contra este tipo de eventos, será posible evitar pérdidas en el sector energético e industrial del país y también evitar como

consecuencia, conflictos y afectaciones de otra índole que no son parte de los objetivos de investigación del presente estudio, por ejemplo, asuntos políticos y sociales.

Un ejemplo de ataque cibernético a subestaciones eléctricas es el ocurrido en el sistema eléctrico de transmisión de Ucrania el 23 de diciembre del año 2015 en Ivano Frankivsk donde se tuvo un evento de desconexión en el sistema eléctrico debido a la intrusión de Spear Phishing para robo de información y con esto, la introducción de *malware* a la red de control del sistema eléctrico ucraniano aprovechando las vulnerabilidades del sistema, inhabilitando 100 MW de carga y como consecuencia afectando a más de 225 000 usuarios. El antes mencionado y otros ataques adicionales se indican con mayor detalle en la sección 1.3 del capítulo 1.

La viabilidad de la implementación de ciberseguridad en subestaciones eléctricas que actualmente se encuentran en servicio se ve afectada por varios aspectos importantes a considerar, como la antigüedad de los equipos que conforman los sistemas, o simplemente porque los protocolos y estándares elegidos en su momento que actualmente no cuentan con herramientas para garantizar una comunicación segura. Esto no es motivo para dejar desde el punto de vista de seguridad, indefensas a las subestaciones eléctricas que operan actualmente ante un ataque cibernético, debido a que incluso en subestaciones eléctricas convencionales es posible adaptar medidas de ciberseguridad en su sistema, previniendo de esta manera la intrusión de atacantes que puedan aprovechar las vulnerabilidades de los sistemas actuales.

El presente estudio de prefactibilidad reflejará las mejores prácticas para apoyar y orientar de manera efectiva a los transportistas nacionales y realizar este tipo de proyecto. Es mucho más fácil de tomar en cuenta la implementación

de ciberseguridad desde el diseño de las subestaciones eléctricas para garantizar su viabilidad económica y al mismo tiempo la seguridad en las mismas.

La implementación de ciberseguridad es necesaria buscando la solución más viable en el aspecto técnico y económico, dado que, si no se tienen las medidas preventivas de ciberseguridad, las subestaciones de transmisión se convertirán en un blanco fácil de sabotaje energético en el Sistema Eléctrico del país.

INTRODUCCIÓN

En la actualidad el mundo del sector eléctrico de potencia está migrando a tecnologías con mayor nivel de digitalización, por consiguiente, es importante considerar maneras de proteger la subestación eléctrica de ataques cibernéticos que tengan como finalidad interrumpir la continuidad del servicio.

La implementación de sistemas de ciberseguridad en las subestaciones eléctricas es importante en la red del Sistema Nacional Interconectado de Guatemala para asegurar su fiabilidad, seguridad y eficiencia. La ciberseguridad es un tema que ha ido tomando auge a nivel mundial en los últimos años, pero su implementación ha sido más aplicada en tecnologías de la información y con la actualización de las tecnologías de operación, como lo son los relevadores de protección, se han implementado muchas funciones que dependen de software y lenguajes de programación para la ejecución de sus funciones, por consiguiente, la digitalización en las subestaciones eléctricas es ahora una necesidad.

La norma IEEE C.37.240 contiene los requerimientos y al mismo tiempo, realiza las referencias necesarias a otras normas, para implementar buenas prácticas de ciberseguridad para toda la subestación eléctrica. Dicha norma se toma como guía para detectar vulnerabilidades y realizar diversas recomendaciones de ciberseguridad para todos los niveles de la subestación.

Para el nivel de patio, el nivel 0, se recomiendan diversas medidas desde la protección perimetral de la subestación para su acceso hasta las protecciones que se deben adoptar para proteger los equipos primarios y equipos en las

casetas de la subestación y de igual manera el acceso a los mismos únicamente para personal debidamente autenticado y autorizado.

Una parte esencial de las Subestaciones es el Nivel que comprende equipos muy importantes que son los IED's (Intelligent Electronic Devices), cuya función es esencial para la protección y control de todos los equipos de patio de contenidos en las bahías de la subestación. Todo lo relacionado específicamente para que estos equipos cuenten con ciberseguridad se puede encontrar en la norma IEEE 1686. Se utiliza también como una guía para detectar vulnerabilidades y realizar recomendaciones para implementar buenas prácticas de ciberseguridad para gestión de puertos, contraseñas de acceso y configuración de los dispositivos.

Es importante considerar la importancia de la ciberseguridad en los protocolos de comunicación de la subestación debido a que estos protocolos pueden transportar información acerca de los eventos o bien, señales analógicas que influyen directamente en los IEDs, una guía recomendable es la norma IEC 62351.

La ciberseguridad para el bus de Estación en Subestaciones, el nivel 2, es sumamente importante para la operabilidad de todos los equipos primarios de maniobra y de todos los IEDs dentro de la subestación, debido a que es posible realizar control y monitoreo aguas abajo y al mismo tiempo, es el límite de la zona segura que se puede implementar dentro de la subestación, es por esta razón que es importante implementar medidas de ciberseguridad, como lo es la buena configuración del *firewall* y la implementación de una DMZ de manera que toda la información y datos que son enviados al Centro de Control se realice a través de canales seguros, garantizando que todo el control y monitoreo que se realice desde el sistema SCADA se realice también de manera segura.

Al mismo tiempo, considerando las normas aplicables, se realiza un análisis de las vulnerabilidades y con esto se realizan recomendaciones de buenas prácticas de Ciberseguridad en el Centro de Control en el nivel 3.

1. GENERALIDADES DE CIBERSEGURIDAD EN SUBESTACIONES

La ciberseguridad es el área de la ingeniería informática encargada del desarrollo y la implementación de los mecanismos de protección de elementos de la tecnología de la información y de los dispositivos del área tecnológica, desde el punto de vista de la informática se enfoca para tener sistemas seguros que garanticen la confidencialidad, integridad, seguridad y disponibilidad de los datos de una red corporativa, tiene diversas aplicaciones que en un inicio se enfocaron a las tecnologías de la información y que con el paso del tiempo y la actualización de la tecnología, su aplicación se ha extendido a diversos campos y que para el caso del campo de la electricidad de potencia se traduce en las medidas implementadas para prevenir las intrusiones cibernéticas en las tecnologías de operación y de la información de los sistemas eléctricos.

Para realizar una completa implementación de ciberseguridad en los sistemas de potencia, se debe tener presente que no se deben preparar únicamente el sistema y los equipos, sino que se debe preparar y capacitar a todo el personal que está a cargo del control de la subestación, la gestión de los de la seguridad en los equipos y la comunicación entre subestaciones, por tal motivo, se necesita contar con una buena política de ciberseguridad en las empresas propietarias de estos sistemas, que es un primer paso para mantener la seguridad de la operación en las redes de transmisión eléctrica.

La seguridad cibernética no se basa únicamente en protección para ataques desde el exterior, también busca evitar que se produzcan vulnerabilidades

generadas desde el interior de las mismas subestaciones provocados por el mal uso de la información y datos.

Dada la importancia del buen funcionamiento de los sistemas de potencia, una prioridad debe ser mejorar las defensas digitales para abordar el riesgo creciente y la posibilidad de ataques contra la infraestructura, los riesgos cibernéticos comienzan a ser considerados como riesgos empresariales fundamentales, considerando importante para el campo objeto del presente estudio, que las empresas transmisoras de energía evalúen e implementen una sólida base para resistir ante riesgos que amenazan la continuidad del servicio.

Las políticas y buenas prácticas de Ciberseguridad pasan a ser una necesidad para mantener la confiabilidad y la seguridad de las operaciones en una subestación eléctrica, sin dejar de tomar en cuenta que conforme las circunstancias y potenciales amenazas cambian, existe la probabilidad que las políticas de ciberseguridad y la estructura de los sistemas requieran actualizaciones frecuentes para abarcar los correspondientes cambios.

Para evitar tener un programa de ciberseguridad insuficiente, es importante saber diferenciar entre riesgos, vulnerabilidades y amenazas. Desde el punto de vista del medio informático, un riesgo es la probabilidad que ocurra un incidente que cause la pérdida o daño de un activo de información, una vulnerabilidad podría reconocerse como una debilidad que puede aprovecharse para causar daño a un activo y una amenaza es un peligro inminente para un activo, que surge de un hecho o acontecimiento que aún no ha sucedido.

El sistema de energía eléctrica puede estar expuesto a una variedad de amenazas de seguridad diferentes, que pueden llegar a generarse por navegar, descargar aplicaciones o archivos de páginas infestadas con *malware*

informático, aceptación de correos phishing por parte de empleados no capacitados, estos pueden traducirse en ataques DoS (*Denial of Service*), robo de información o inhabilitación de funciones en aplicaciones de sistemas operativos.

Los ataques DoS consisten en dejar sin capacidad de respuesta al servicio, esto se logra enviando una cantidad masiva de peticiones al servicio desde una sola IP, a diferencia de un ataque DDoS es más fácil detectarlo, debido a que en un ataque DoS se envía al mismo servicio la cantidad masiva de peticiones todas al mismo tiempo desde múltiples direcciones IP.

Los incidentes de seguridad cibernética en su mayoría se originan por causas accidentales, algunas vulnerabilidades como la falta de autenticación en los sistemas de las subestaciones, falta de encriptación de la información, cambio periódico de contraseñas de acceso a los distintos dispositivos son los motivos más comunes y frecuentes que dejan vulnerable a un sistema de seguridad en todos los niveles de la subestación.

Diversos estudios han identificado dos tipos predominantes de amenazas, las amenazas no intencionales, son las que se generan en los equipos y derivado de acciones de empleados y las amenazas intencionales son las que se producen a causa de intentos de intrusión directa en la red, claro ejemplo un ataque DoS, y otra amenaza reconocida son los virus.

Algunas medidas generales de Ciberseguridad que pueden tomarse en cuenta en las Subestaciones son:

- Mantener una buena gestión para la actualización de contraseñas en todos los dispositivos de IT y OT.

- Segmentación de la red en varias zonas, al momento de un ataque los intrusos puede que logren ingresar a la primera zona, pero, lograr pasar a la siguiente será muy difícil, esto evitará que desde un acceso remoto tengan control directo a los IEDs.
- Mantener el control de autenticación para el acceso físico a la subestación, cifrar toda la información y eventos que se transmite en la red de comunicación desde lo recibido desde las señales que se reciben del equipo de patio hasta lo que se envía al Centro de Control.
- Contar con un plan de resiliencia que conozca todo el personal de la compañía para en caso de un ataque seguir lo establecido en el plan dependiendo el grado de daño que se logre generar generando acciones correctivas.

1.1. Implementación de seguridad cibernética en una subestación

Proteger una subestación requiere de un enfoque de defensa en profundidad (*Defense in Depth*), y que se apoye de una evaluación de los riesgos cibernéticos y operaciones que sean seguras de ejecutar a través de los dispositivos instalados en todos los niveles de la subestación.

Los principios de defensa en profundidad se aplican en zonas fundamentales de la arquitectura de la subestación como los *firewall* y medidas de *hardening* del sistema.

Según IEC 62443-3-3 Para proporcionar una defensa en profundidad, las medidas de seguridad se colocan en diferentes zonas, componentes, interfaces

y conexiones de red del sistema, y se debe cumplir con los objetivos de protección de confidencialidad, integridad y disponibilidad.

Como parte de una estrategia de defensa en profundidad, los sistemas de control deben dividirse en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red de conformidad con las políticas y procedimientos de seguridad y una evaluación de riesgos.

Normalmente no es posible lograr los objetivos de seguridad recurriendo a una única contramedida o técnica, un enfoque superior consiste en utilizar a fondo el concepto de defensa, lo que entraña la aplicación de múltiples contramedidas de forma escalonada o gradual. Por ejemplo, los sistemas de detección de intrusos se pueden utilizar para señalar la penetración de *firewall*.

Según IEC 62443-1-1, existen diversos niveles aceptables de seguridad dependiendo que los elementos que se requiere proteger ya sea información o la operabilidad de dispositivos, no es necesario aplicar el mismo nivel de seguridad a todos los componentes, para ello se implementan las zonas de seguridad. Una zona de seguridad está conformada por activos que comparten características de seguridad comunes, dentro de estos pueden encontrarse activos de aplicaciones, informáticos, operacionales y físicos.

La zona de seguridad puede contener sistemas y con base en esto es posible referir a los sistemas que están dentro de la zona de seguridad y los que se encuentran fuera de ésta en otra zona o totalmente sin zona de seguridad. También aplica el concepto de subzonas, están contenidas dentro de las zonas de seguridad, y que se caracterizan por tener una seguridad estratificada. Pudiendo así implementar una defensa en profundidad otorgando diferentes propiedades a las zonas de seguridad.

Puede definirse a una zona segura desde un punto de vista físico como “zona física” o de un sentido lógico “zona virtual”, es importante tener en cuenta que una zona física se conforma agrupando los activos según su ubicación física en la subestación, mientras que las zonas virtuales se conforman agrupando elementos según su funcionalidad.

Para determinar los requisitos de seguridad que debe cumplir una zona, cada compañía debe evaluar la ubicación de cada activo dentro de una zona determinada como el acceso a la comunicación y el acceso físico y proximidad, siendo estas zonas denominadas como zonas de confianza.

Para el acceso físico, básicamente se debe crear una zona de confianza física, es decir tener un control del acceso de personal a las diversas áreas de la subestación, como lo son todos los puntos de acceso posibles al equipo de patio y los accesos posibles a otros puntos como son oficinas y caseta de control.

Para crear una zona de confianza en la red de la subestación, implica incluir equipos de protección, control y medida, *switches* de comunicación de la red LAN de capa de enlace, equipos de monitoreo y control como son HMIs y RTUs y *routers* para incluir la capa de red y al mismo tiempo incluir equipos *firewall*, para incluir la capa de transporte, todos estos dispositivos se pueden incluir dentro de la zona de confianza de la subestación.

Otro factor importante a considerar es la utilización del método de nivel de seguridad en las empresas, debido a que ayuda a definir lo que representa cada nivel y cómo medir el nivel de seguridad de la zona. Se recomienda tener un mínimo de tres niveles de seguridad como se muestra:

Tabla I. **Niveles de seguridad**

Nivel de seguridad	Descripción
1	Bajo
2	Medio
3	Alto

Fuente: elaboración propia.

Este método puede utilizarse para determinar una estrategia global de defensa en profundidad por capas superpuestas para contramedidas como es el caso de equipos y programas informáticos junto con contramedidas de tipo administrativo, un ejemplo es como el que se muestra:

Cuando el enfoque principal es proteger los datos, la implementación del método en redes corporativas puede incluir la creación y aplicación de políticas y procedimientos, así como la seguridad física, de red, informática y de dispositivos.

Desde el punto de vista de Tecnologías de la Información, se indican ciertas capas, pero se debe tomar en cuenta que la implementación de éstas dependerá del diseño de la red e infraestructura con la que cuente la compañía:

- En la primera capa se determinan las políticas a implementar y los procedimientos que los usuarios de la red deben seguir en forma obligatoria.
- En una segunda capa se deben asegurar los equipos con contraseñas e implementación de autenticación y auditoría para tener control de los usuarios que tienen acceso a los dispositivos y a la red.

- La tercera capa consiste en asegurar el perímetro de la red y este perímetro se delimita por la instalación de *firewall*, cuya función principal será permitir o rechazar los paquetes de datos que entran a la red, mientras que dependiendo de la función que se quiera otorgar también puede seleccionar la información que saldrá de la red, dependiendo de la topología con la que se cuente. Es importante que toda la comunicación de la red LAN pase a través del *firewall* debido a que este puede redirigir el tráfico de la red LAN hacia los servidores correspondientes para permitir accesos web, correos electrónicos o funciones DNS.
- En la cuarta capa es recomendable segmentar la red a través de direccionamiento lógico, se convierte en necesidad, reorganizando dicha red en secciones que dependiendo del alcance de la comunicación se puede tener la red LAN, la WAN y la sección para una zona desmilitarizada (DMZ); es punto importante de seguridad para el *firewall*.
- En la quinta capa para una mayor protección en los equipos de la red LAN, es posible aplicar un proceso de *hardening* al sistema operativo, esto con el objetivo de disminuir las vulnerabilidades en los clientes de la red como en los servidores. Buenas prácticas de *hardening* es establecer un bloqueo para el acceso de los dispositivos después de cierta cantidad de intentos fallidos para acceder y bloquear puertos que no estén en uso de la red.
- Y una sexta capa para dispositivos que tengan sistemas operativos vulnerables, es recomendable que, en los equipos utilizados como clientes, se implementa el uso de un antivirus, para ayudar a impedir la ejecución de código malicioso, evitando la intrusión de cualquier usuario no autorizado.

Para la defensa en profundidad, resumiendo, se puede basar en tres conceptos:

- Se pueden implementar múltiples capas de defensa con diversas soluciones de seguridad se obtiene la ventaja que, si se logra atravesar una, otra capa actuará como defensa.
- La implementación de capas de defensa diferenciadas, que se convierte en una estrategia de seguridad sólida cibernética, garantiza que cada una de las capas de seguridad sea ligeramente diferente.
- Realizar un diseño para la amenaza, creando distintas capas específicas con defensas creadas según su aplicación de manera específica del contexto y la amenaza.

1.1.1. Ciberseguridad en la red de comunicación en una subestación

Para implementar ciberseguridad en las redes de comunicación que forman parte de una subestación, la arquitectura de comunicación es el centro de estudio tomando en cuenta los elementos de la red, desde los IEDs hasta los protocolos, debido a que se puede tener acceso a IEDs a través de redes IP y tecnologías de internet y redes WAN.

Incluso si la red está completamente aislada y no hay ningún equipo remoto conectado, se deben aplicar mecanismos de seguridad como protocolo syslogs, pistas de auditoría de seguridad, contraseñas, control de acceso, seguridad de puertos y cifrado para aumentar la resistencia frente a errores de configuración e instalación.

Deben existir dos tipos de ciberseguridad puntualmente para las redes de comunicaciones de las subestaciones: seguridad física y seguridad de red.

Para obtener cierto grado de seguridad física es posible implementar ciertas medidas de acceso no autorizado a los dispositivos de comunicación, como mantener cerrado con llave el tablero y controlar el acceso a la caseta donde se encuentren estos tableros.

En cuanto a la seguridad de la red, uno de los factores más importantes es la implementación del mecanismo básico de seguridad es AAA.

AAA, es el acrónimo para *Authentication, Authorization & Accounting*, es un estándar que se puede adoptar para la autenticación, autorización y auditoría de usuarios en la red a proteger, las tres etapas tienen diversas formas de implementación y cuyo objetivo común es mantener el control de acceso a cada dispositivo haciendo uso de contraseñas e implementación de credenciales como PKI, llave magnética o *token* para la identificación de cada usuario definido en un control de acceso basado en roles en el sistema de seguridad aplicando de esta manera autenticación, y hacer posible el uso de un control del acceso de todos los usuarios, definiendo la cantidad de accesos de cada uno de ellos e incluso intentos de usuarios no autorizados, teniendo de esta manera una auditoría.

1.1.1.1. SNMP

SNMP son siglas para la definición de *Simple Network Management Protocol*, que significa Protocolo de Gestión de Redes Simple. Es un protocolo interoperable basado en estándares que permite el monitoreo y ajustes en la configuración de los dispositivos de forma remota, brindando seguridad a la información que se comparte entre dispositivos y que se implementa en la capa

de aplicación. En un principio se fabricó únicamente para gestionar *routers* y *switches* de comunicación, ahora bien, dada su valiosa utilidad en la actualidad el protocolo se puede utilizar para cualquier dispositivo que consiga conectarse a una red, pues se puede administrar de una manera común, todos los dispositivos de la red, independientemente del tipo y la marca.

Es un protocolo que utiliza UDP (*User Datagram Protocol*), para datagramas o el protocolo TCP/IP para transportar comandos y mensajes, entre el gestor o controlador y el agente o dispositivo controlado. Cualquiera de los dispositivos gestionados se comunica con el equipo gestor cuya función es almacenar toda la información recolectada de los agentes en una MIB (*Management Information Base*), la cual es una base de datos; es una manera jerárquica en estructura de árbol para organizar la información recolectada por parte de cualquier dispositivo con SNMP que se encuentre conectado a la red. Teniendo dos tipos de nodos de información, como son los nodos estructurales y los nodos con información. Los nodos estructurales únicamente tienen descrita su posición en el árbol, podrían describirse como las ramas del árbol y los nodos con información son los que asignan a cada nodo estructural, como analogía son como las hojas del árbol.

La información que se puede obtener el MIB es la siguiente:

- Como función de auditoría: puede describir la cantidad y el nombre de cada cuenta de usuario, es como una lista, es por esta razón que es posible saber sobre los grupos de usuarios y la creación de las cuentas de cada uno dentro de la red.
- Programas instalados: es viable obtener la lista de los programas de uno o más ordenadores, es por esta razón que es posible conocer las de los

sistemas operativos instalados, con la finalidad de detectar vulnerabilidades a través de versiones obsoletas.

- Probabilidad de contar con puertos abiertos: ante robo de información se puede realizar un escaneo que deje al atacante en evidencia ante los administradores de red.

Respecto a las versiones disponibles de SNMP todas se utilizan en la actualidad, y son las siguientes:

- SNMPv1: cuenta con un nivel de seguridad bajo. El esquema de autenticación es simple mediante texto plano, lo que implica que no se aplica ningún tipo de cifrado para el transporte de información.
- SNMPv2: tiene ligeras mejoras en relación con la versión 1, se introduce *GetBulk* para que el gestor pueda recuperar bloques de información, se introduce *Inform* para que el agente al recibir confirmación, de envío de información al gestor, y por último *Report* para que en caso el agente envíe errores de protocolo, éstos sean detectados. La protección de información en esta versión no fue mejorada significativamente.
- SNMPv3: es una versión donde la seguridad ya es reforzada, brindando mayor confiabilidad para configuraciones remotas, introdujo funciones de seguridad que incluyen el modelo de seguridad basado en el usuario (USM). Proporciona la autenticación e integridad por medio de cifrado, verifica que el mensaje recibido no haya sido alterado en el transcurso del envío y que en efecto haya sido enviado por el dispositivo registrado, lo que puede traducirse como una autenticación del dispositivo, también verifica la puntualidad de los mensajes. El SNMPv3 también está

respaldado por la seguridad de control de acceso basada en vistas VCAM (*Views-Based Access Control Model*), para proteger contra la manipulación de la información, la reproducción, la suplantación de identidad y el rastreo, permitiendo brindar diferentes niveles de acceso de los agentes a las MIB, de manera que un agente puede restringir el acceso de ciertos gestores a parte de su MIB, manteniendo de esta manera cierto grado de seguridad.

Los usuarios de empresas pueden recopilar de forma segura información de gestión de sus agentes SNMP en los IED.

1.1.1.2. RADIUS

RADIUS son las siglas de *Remote Authentication Dial in User Service*. Es un protocolo cliente / servidor con funciones de gestión como AAA. El servidor RADIUS suele ser un servicio cuya función principal es autenticar usuarios o dispositivos antes de otorgarles acceso a una red. El proceso principal de transmisión de mensajes RADIUS es que, al iniciar sesión en un dispositivo de red como un servidor de acceso, el proceso principal de transmisión de mensajes el usuario envía el nombre de usuario y la contraseña al dispositivo de red.

El cliente RADIUS, es un servidor de acceso a la Red (NAS), establece comunicación punto a punto a nivel de enlace, cuya función es verificar y autenticar con el servidor. Si la autenticación es válida, se permite que la información sea transferida al cliente. y envía la información de autorización requerida al cliente. En caso contrario, si la solicitud es denegada, se hace llegar un mensaje de error al cliente que solicita acceso.

La función RADIUS autoriza a los usuarios o dispositivos para ciertos servicios de red y cuentas para el uso de esos servicios. Todas las puertas de enlace que controlan el acceso a la red tienen un cliente RADIUS IEEE 802.1x.

RADIUS para mantener un control de las fases del proceso de AAA, hace posible contar con los tipos de mensaje:

- *Acces-Request*: es enviado por un cliente RADIUS para solicitar autenticación para el acceso en la red.
- *Access-Accept*: es el mensaje de autorización y autenticación que envía el servidor RADIUS para dar respuesta al *Acces-Request*.
- *Access-Reject*: es un mensaje tipo respuesta que explica la causa por la cual ha sido negado el acceso a un cliente, este es enviado por el servidor RADIUS.
- *Access-Challenge*: es enviado por el servidor RADIUS a un cliente para que dé respuesta a una consulta.

1.1.1.3. TACACS

El protocolo TACACS consiste en autenticación de manera remota muy aplicado en comunicaciones útil para redes donde se requiere la autenticación para autorizar el acceso a un servidor remoto. La finalidad de la autenticación radica en proteger la información del servidor y las herramientas de acceso al medio es utilizar *token*, tarjeta inteligente, entre otros. Para proporcionar autenticación de dos factores.

La aplicación en subestaciones consiste en que el servidor de acceso remoto puede comunicarse con un servidor de autenticación con TACACS para determinar si el usuario tiene acceso a la red.

1.1.1.4. SSH

SSH son las siglas de *Secure Shell*, es un protocolo de administración remota que le permite a los usuarios controlar sus servidores a través de internet implementando un mecanismo de autenticación. SSH se puede utilizar para iniciar sesión en IEDs, para una comunicación de datos segura, servicios remotos o ejecución de comandos y otros servicios de red seguros entre dos ordenadores. SSH utiliza criptografía de clave pública para autenticar el servidor remoto y permitirle autenticar al usuario, el protocolo también impide que se realicen ataques MITM (*Man in the middle*), cuyo objetivo es interceptar la información que se transporta entre dos dispositivos, pudiendo suplantar la identidad de algún usuario autorizado, el protocolo SSH impide que la información pueda ser interpretada.

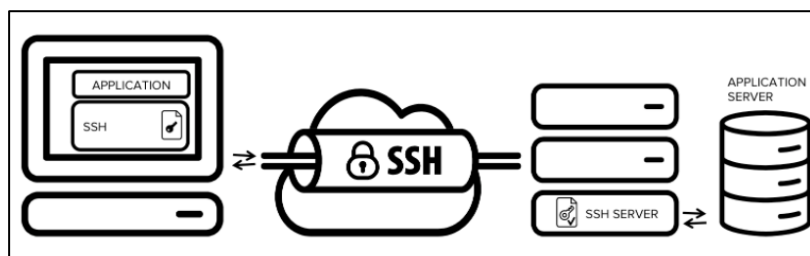
Para aprovechar la protección que brinda el protocolo, se encuentran tres tipos de cifrado con los que se pueden escribir los comandos.

- Cifrado simétrico: para hacer seguro el envío de información entre un host y cliente, es necesario crear una clave privada, característica común para una sesión de SSH, donde por medio de una clave compartida se sigue el método para acordar una clave confidencial creada mediante un algoritmo que se comparte y es brindado por el intercambio de claves, que nunca es compartida entre dicho cliente y el host.

- Cifrado asimétrico: se diferencia porque emplea dos claves auténticas y diversas para cifrar información, para ello se crean dos clases de clave, una pública y otra privada. Trabajan de manera conjunta de tal manera que la información cifrada por la clave pública únicamente puede ser descifrada por la clave privada que se creó en conjunto con su clave pública.
- *Hashing*: no es un método de cifrado, es un método unidireccional, por medio de un algoritmo utilizado por el protocolo SSH para la verificación de mensajes que son transmitidos con HMACs basados en hash obteniendo la autenticidad de los mimos, pues se puede garantizar la seguridad de los mensajes.

SSH solo verifica si la misma persona que ofrece la clave pública también es propietaria de la clave privada correspondiente.

Figura 1. **Diseño de SSH**



Fuente: Digital Guide IONOS. *Qué es SSH todo sobre el protocolo de cifrado.*
<https://www.ionos.mx/digitalguide/servidores/herramientas/protocolo-ssh/>. Consulta: 10 de octubre de 2021.

Aparte de los protocolos mencionados, existen métodos que se pueden implementar en los dispositivos de comunicación periféricos, siendo estos:

1.1.1.5. Seguridad por medio de *switch* de comunicación

Las redes de subestaciones se construyen principalmente con *switches* de comunicación. Se pueden construir segmentos de red de subestaciones lógicamente aislados mediante la creación de LAN virtuales dentro de una LAN física, las VLANs por configuración de puertos garantizan la integridad de los datos y apoyan a liberar el tráfico que se puede generar en una red LAN principalmente cuando se utiliza el transporte del tipo Multicast para mensajes. Los dispositivos conectados a diferentes *switches* físicos pueden comunicarse entre sí siempre que estén en la misma VLAN. Los dispositivos que se encuentran en diferentes VLAN no pueden comunicarse entre sí, y esto crea una serie de capas para la seguridad.

1.1.1.6. Seguridad con *router* (enrutador)

En términos generales un *router* es un dispositivo que administra de rutas que envía datos en paquetes entre redes de comunicación dentro de la red segmentada de una subestación, entre subestaciones o desde subestaciones a los Centros de Control.

El *router* indica el destino final de los paquetes de datos enviados por la red, y si este es intervenido por un usuario no autorizado, puede desviarse la información a destinos fuera de la subestación, logrando interferir directamente la comunicación entre dispositivos que se encuentren en redes separadas. El control de acceso de los usuarios a la red debe ser controlado y monitoreado en todo momento, esto se logra por medio de Listas de control de acceso ACL (*Control Access List*), incluso se pueden utilizar para filtrar paquetes de información que no cumplan con requisitos de ciberseguridad.

1.1.1.7. Seguridad por medio de *firewall*

Un *firewall* es un dispositivo cuya función principal es monitorear el tráfico existente en la red. Es un equipo de las tecnologías IT que determina el límite de una zona de red segura y con este puede implementarse como una capa de una defensa en profundidad, pues este además de monitorear el tráfico de la red puede dar o negar el acceso de información y datos entre diversas redes, esto es permitido debido a la función de las Listas de control de Acceso (ACL), conocidas como *Access Control List*. Algunos *routers* tienen incluida la funcionalidad de *firewall*.

Los *firewalls* pueden realizar funciones de gestión y detección el acceso a la red para crear alertas durante ataques y fallas. Existen diferentes tipos de *firewall* cuyas funciones están destinadas al tipo de red que se desea implementar. Los *firewalls* más comunes son:

- *Firewall* de filtrado de paquetes: la función de este tipo de filtro es rutear de manera selectiva, paquetes entre host internos y externos, utilizando el tipo de ruteo conocido como *screening router*. Se puede permitir o denegar el tráfico que entra a la red interna de acuerdo con reglas definidas por un administrador, por consiguiente, el uso de las ACL es fundamental en este tipo de *firewall*, de manera cuando un paquete llega al puerto del dispositivo, los encabezados de los paquetes a nivel de red se analizan siendo del tipo IP, TCP o UDP, para tomar una decisión y otorgar o no el paso a la red interna a proteger.
- *Firewall* SPI: estos elementos son los que se conocen como *firewall Stateful Packet Inspection* o filtrado dinámico, y la función principal es que realizan una inspección del estado de las conexiones de red que pasan

por el dispositivo protegiendo a la red interna que defiende de los riesgos de una red externa insegura de internet y de posibles ataques DoS. Esto se logra pues la lista de control de acceso tiene la posibilidad de añadir más reglas de manera dinámica considerando la conexión a nivel de transporte, por consiguiente, le permite comprobar si el paquete examinado pertenece a alguna sesión que este abierta en ese momento.

- *Firewall DPI*: estos elementos son los que se conocen como *firewall* Deep Packet Inspection o inspección a fondo de los paquetes, realizando una inspección minuciosa de los paquetes que atraviesan el *firewall* analizando los datos a nivel de aplicación pudiendo detectar troyanos, *malware* y cualquier amenaza de este tipo.
- *Firewall proxy*: también son conocidos como *dual homed*, brindan seguridad y almacenamiento de contenido, son equipos intermediarios entre la red interna y externa, analiza y registra todo el tráfico de entrada y salida, por consiguiente para acceder a cualquier servicio, se tiene que pedir por regla, el acceso al Proxy, pues éste gestiona la solicitud de información a la red externa insegura y únicamente deja pasar la información segura a la red interna, esto hace posible que se tenga un registro y que se puedan bloquear ciertas acciones o accesos a páginas de riesgo. La aplicación se puede hacer a nivel aplicación y ayuda a que se infiltren posibles amenazas. El inconveniente más notorio es que se puede formar un cuello de botella para solicitar los servicios de la red externa, pues todo el tráfico tiene que pasar a través del *firewall*.
- *Firewall* de próxima generación: tienen las características de los *firewalls* tradicionales, pero son fabricados de manera que tengan un mayor soporte

para necesidades, la organización, contra amenazas, y los sistemas que tienen incluidos son:

- Sistema de prevención de intrusiones (IPS): realiza un análisis profundo del tráfico de la red, identificando amenazas y bloqueándolas.
- Inspección profunda de paquetes (DPI): mejora el filtrado de paquetes al analizar el cuerpo y el encabezado.
- Conocimiento y control de aplicaciones, identifica y bloquea el tráfico en función de las aplicaciones a las que se dirige el tráfico.
- Fuentes de inteligencia de amenazas: incorpora flujos de inteligencia de amenazas que se actualiza constantemente para brindar una mejor protección.

1.1.1.8. Seguridad de Gateway

Cuando la red de la subestación está conectada a una WAN o se accede de forma remota, se deben aplicar *Gateway* para lograr la seguridad cibernética contra una variedad de ataques cibernéticos. Una puerta de enlace recopila datos de informes de medición, estado, eventos y fallas de los IED y RTU y crea una interfaz entre los sistemas de automatización de subestaciones y las conexiones externas, como un navegador web. Puede administrar, filtrar y controlar el tráfico de datos y proteger los IED y otros dispositivos contra el acceso externo. Las puertas de enlace normales se pueden lograr mediante VPN y cifrado.

1.1.1.9. VPN

La aplicación de una red privada virtual cuenta con los beneficios de establecer una conexión cifrada entre dos puntos a través de una red insegura. Una VPN utiliza un "túnel" seguro entre dos redes. La información se envía mediante tunelización, que es la práctica de cifrar y encapsular paquetes IP.

Dentro de las VPN se tienen dos arquitecturas principales: VPN de acceso remoto y las VPN de Sitio a sitio, cada arquitectura es utilizada dependiendo las necesidades de acceso que se presenten en la red.

- VPN de acceso remoto, es una arquitectura diseñada para que varios usuarios se conecten a un servidor de VPN desde una ubicación fuera de la subestación, utilizando una red de internet como vínculo de acceso, ahora, para volver segura la conexión, es necesario implementar protocolos de seguridad como la autenticación para poder acceder a la red empresarial de la empresa.
- VPN de sitio a sitio son útiles para conectar redes LAN entre sí, el *router* o *firewall* conectan todos los clientes para que la red se vea como una sola, aunque tráfico se transporte por diversos túneles de VPN.

Para implementar seguridad existen estos dos métodos:

1.1.1.9.1. Open VPN

Open VPN es un software de código abierto, es decir de libre uso, e implementa técnicas de VPN para crear conexiones seguras de punto a punto o

de sitio a sitio utilizando conexiones públicas de internet, teniendo acceso desde puntos remotos.

Cada usuario deberá tener un certificado único de Open VPN que lo identifique y en cualquier momento este podrá ser revocado. Este software también permite conectar dos redes locales de una misma compañía utilizando los canales de internet.

Una de las ventajas es que se puede utilizar desde diferentes sistemas operativos, como Windows y Linux.

1.1.1.9.2. IPSec

Significa *Internet Protocol Security* (IPSec), proporciona servicios de seguridad a la capa IP y a niveles superiores asegurando protocolos como TCP y UDP, en otras palabras, protege en la capa de red (capa 3 del modelo OSI), haciendo posible la comunicación de forma segura entre varios puntos de internet, manteniendo la información cifrada de los paquetes de IP, al mismo tiempo que implemente la autenticación del origen de los datos y protección para iniciar una defensa en profundidad contra ataques basados en la red o el robo de datos. IPSec admite las dos arquitecturas que existen de VPN, la de acceso remoto como VPN *site-to-site*.

1.2. Las demandas e implicaciones de la colaboración de IT y OT

Debido al tipo de funcionalidad de los dispositivos, normalmente las empresas de transmisión han implementado y respaldado la tecnología operativa o bien en su nombre en inglés *Operation Technology* (OT), por separado de la tecnología de la información, correspondiente a *Information Technology* (IT).

Dada la constante actualización de las OT sus software, funcionalidad, seguridad y migración a la utilización de protocolos de comunicación se están asimilando a los de IT.

Algunas diferencias más notorias son:

- IT abarca el concepto referido a la gestión de información; abarca un área de elementos que hacen posible el flujo de datos en una red, lo que implica la necesidad de incluir software, hardware y dispositivos y protocolos de comunicaciones. A diferencia de lo anterior, las OT son los elementos que hacen posible el control, protección, monitoreo y funcionalidad de sistemas implementados en las industrias para realizar diversos procesos estructurados garantizados por medio de la operabilidad de los dispositivos que lo conforman.
- El propósito de IT es la interacción de diversos factores para la distribución de información comercial, que está vinculado a generar, proteger, recuperar y procesar datos por medio de computadoras. Los términos anteriores utilizados para IT eran sistema de información de gestión (MIS); se encarga de medir el rendimiento de una empresa, y el sistema de información empresarial (BIS). Es posible utilizar para convertir los datos en productos de información para se pueda utilizar de apoyo en actividades de coordinación, planificación y toma de decisiones de una organización.
- OT abarca las tecnologías que se utilizan para la operación de activos físicos, y que para este caso es de suma importancia las aplicaciones que tienen los IEDs para la protección, control y monitoreo en la subestación y

donde el tiempo de envío de datos entre dispositivos es sumamente importante.

1.2.1. Tecnología operativa (OT)

Los sistemas y tecnologías OT incluyen IED, estos han tenido un desarrollo considerable desde su primer prototipo, actualmente cuentan con microprocesadores que les permite ser veloces para enviar datos y al mismo tiempo procesar datos que reciben de los dispositivos que estén monitoreando ya sea señales digitales o analógicas de voltaje o corriente. Para ello, dependiendo de su función cuentan con diversas entradas y salidas digitales y entradas analógicas dependiendo de la función para la que estén diseñados.

Al mismo tiempo han adquirido medios de comunicación con conexiones EIA que por sus siglas en inglés Electronic Industries Alliance. Es un estándar que en conjunto con TIA que por sus siglas en inglés Telecommunications Industry Association, publican estándares que abarcan el cableado estructurado de datos, teniendo mayor impacto en las comunicaciones seriales y que, los IEDs cuentan con conexión Ethernet, ambos son protocolos de comunicación utilizados en su mayoría para funcionar dentro de una red LAN.

En la actualidad para cumplir funciones mejoras en IEDs se han implementado el estándar IEC 61850, que por medio de multidifusión de paquetes Ethernet es posible enviar eventos generados entre los IEDs a través de mensajes genéricos GOOSE y mensajes con contenido de señales eléctricas de manera muestreada como son los Sampled Values, con los que se obtiene una mejor comunicación y agilidad del envío de datos entre dispositivos a diferencia de los métodos utilizados en elementos de IT.

El alcance de las redes OT no se limita únicamente a redes LAN, siendo equipos para protección, control y medición, y que, para el caso de sistemas de potencia, éstos pueden enviar datos a niveles superiores fuera de la subestación para el control y monitoreo desde sistemas SCADA, se encargan de la supervisión, control y adquisición de datos. Los SCADA pueden reunir datos de varias subestaciones y haciendo uso de redes de área amplia (WAN).

La introducción de estos sistemas hace necesaria la interacción entre redes de OT e IT para hacer efectivo el intercambio en tiempo real de datos, la comunicación entre elementos remotos como relevadores de protección de línea para protegerla entre subestaciones y en general para el funcionamiento del sistema eléctrico de potencia.

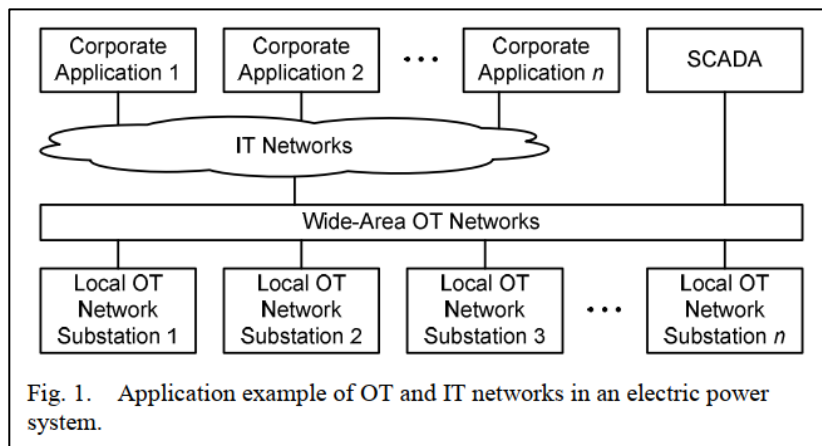
1.2.2. Tecnologías de la Información (IT)

Es necesario tener en cuenta que las IT conforman elementos de hardware, software y métodos para hacer posible el flujo y transporte de información y datos entre dispositivos y usuarios.

En la aplicación para sistemas eléctricos de potencia, la función de los elementos de IT es ser el medio de interconexión entre los equipos para que los elementos de protección puedan tomar decisiones de apertura y cierre de equipos de patio como lo son los interruptores de potencia y al mismo tiempo, las IT son el medio por el cual los elementos de OT envían los datos a los SCADA y también hacen posible que desde un Centro de Control Remoto se puedan realizar maniobras en los equipos primarios de las subestaciones, en la siguiente figura se muestra la interacción entre las diversas tecnologías y donde se incluyen las redes corporativas cuya función es la gestión de activos

desentendiendo de las decisiones que se tomen con la información que se recopila de las OT.

Figura 2. **Interacción entre IT y OT**



Fuente: MOUSSAMIR, Mohamed; DOLEZILEK, David. *The demands and implications of IT and OT collaboration*. p. 2.

Ejemplos de dispositivos de IT que son actualmente fundamentales en la interoperabilidad de equipos de OT son los *switches* de comunicación, *firewall*, *routers*, pues sin estos elementos no se podrían asignar tareas de seguridad, enlace de redes y transporte de información entre las redes de OT.

1.2.2.1. **Impacto de la IT en la infraestructura de la industria eléctrica**

Desde la creación de los dispositivos de OT no era viable implementar equipos de comunicación en las redes que se construían, pero tomando en cuenta la constante actualización tecnológica fue necesario implementar

tecnologías IT en las redes OT, lo que como todo cambio conlleva cierta serie de ventajas y desventajas.

Como ventajas existe la eficiencia que se tiene de comunicación entre diversos niveles de comunicación, se puede regular de mejor manera el tráfico de la red y se pueden incluir más IEDs dentro de una misma red o varias redes según sea necesario dependiendo de la funcionalidad de la subestación, empero, las mismas vulnerabilidades que se incluyen por defecto en las IT son incorporadas ahora en las redes OT, lo que conlleva a tener que implementar medidas de ciberseguridad en redes OT, expandiéndose a todos los elementos de la subestación.

1.2.3. Colaboración entre IT y OT

Las necesidades de los sistemas eléctricos de potencia actuales han generado diversos criterios de aceptación en las redes de comunicación para las tecnologías OT, el diferenciador más importante que distingue enormemente a OT de TI es la conectividad para la comunicación de dispositivo a dispositivo y la comunicación de cliente / servidor.

La funcionalidad más importante de los sistemas OT consiste en que deben decidir y actuar constantemente acciones de automatización y protección para mantener en correcto funcionamiento los elementos del sistema eléctrico de potencia y elementos como el SCADA son elementales para mantener el monitoreo y la recopilación de datos para ajustes de toda la red.

El primer elemento importante para crear una colaboración entre IT y OT es desarrollar una estrategia para que los equipos de ambas tecnologías puedan lograr diversos objetivos comunes, tomando en cuenta que las prioridades para

ambas tecnologías son distintas y que siempre existirán discrepancias y para ello se debe mantener siempre un equipo de trabajo especializados en ambas áreas para que respalde el funcionamiento del sistema en caso de contingencias.

El segundo elemento, es recomendable que ingenieros de tecnologías de OT sean los encargados de diseñar las redes OT exclusivamente para la subestación, puesto que ingenieros de IT son expertos para el diseño de la protección de información, en cambio, en redes OT la prioridad es la buena funcionalidad y parametrización de los equipos con base en estudios eléctricos para dimensionamiento de equipos y estudios de coordinación de protecciones y solución a otro tipo de problemas como son los de procedimiento, y luego de la buena operación de equipos, y después de toda la funcionalidad entra en juego la seguridad y es donde los ingenieros de IT pueden ser gran soporte para ingenieros de OT y para diseñar la intersección de las redes OT e IT en el Centro de Control y red corporativa.

El tercer elemento de colaboración es que los ingenieros de OT e IT trabajen juntos para evitar dejar espacios vulnerables en las redes que actualmente se diseñan, ya no es viable que los ingenieros para ambas tecnologías estén aislados entre sí.

Para dar seguimiento y aterrizar el proceso de colaboración, es necesario formar un equipo de colaboradores adecuado, con los conocimientos para ambas tecnologías y estar dispuestos a trabajar en equipo dado que al diseñar nuevas redes se tiende a correr nuevos retos de ingeniería dependiendo los requisitos de comunicación de red y poder generar las mejores soluciones. Lo recomendable es que se pueda crear un buen plan del proyecto, que tenga fechas clave para cumplir con los retos y no extender la solución más allá de las necesidades de las empresas.

1.2.4. IT y OT tienen criterios de aceptación muy diferentes

Los sistemas OT dependiendo de los diversos alcances que deban cubrir tienen diferentes requisitos de rendimiento y confiabilidad, implementando actualmente en su mayoría la multidifusión de GOOSE y Sampled Values del estándar IEC 61850, esto es muy importante para la efectividad de comunicación entre equipos de diversas marcas que forman parte de una misma red OT y el preámbulo para poder implementar bus de proceso, esta es una parte fundamental de las subestaciones digitales.

Se debe considerar que, al implementar ciberseguridad en la red, no se debe perder la eficiencia del sistema de manera que se evite algún tipo de conflicto. Las siguientes son algunas preocupaciones de los criterios de aceptación de IT y OT para varios requisitos de comunicaciones de red.

- **Desempeño:** para cumplir con la correcta funcionalidad de los sistemas de IT, éstos pueden tolerar cierto tiempo de demora para el envío de datos entre dispositivos y retardo a la variabilidad temporal durante el envío de señales digitales, es decir, fluctuación y aun así las IT pueden tener alto rendimiento. Por otra parte, las aplicaciones de OT para que cumplan con su funcionalidad son críticas en el tiempo de envío de eventos y datos, puesto que para los OT que son críticos en tiempo están los relevadores de protección, dependiendo de la función, estos se pueden parametrizar de manera que se requiera respuesta y latencia en un rango de menos de 3 milisegundo y no mayor a 20 milisegundos.
- **Rendimiento de mensajes:** en cuanto a tecnologías OT no es requisito fundamental que se cuenta con un nivel alto de rendimiento, es suficiente con que se obtenga un buen resultado. Independientemente de las

características de la red, lo importante es cumplir con el rango anterior establecido para la respuesta. En las tecnologías de IT no existe ningún requisito en tiempo de respuesta, tienen un margen superior para retardo de datos y su prioridad es el alto rendimiento.

- Latencia de entrega de mensajes: el estándar 60834-1 es aplicado a los sistemas de comando de teleprotección que se utilizan para transmitir comandos de información por medio de equipos de protección, y establece requisitos de rendimiento para teleprotección tipo comando, pudiendo transmitir información digital o analógica. La latencia permitida para un buen rendimiento es de 20 milisegundos para el disparo permisivo, tomando en cuenta también la función de teleprotección y latencia máxima de 30 milisegundos para disparo directo. No existe ningún requisito o medición similar para los sistemas de IT, puesto que es función propia de relevadores de protección.
- Confiabilidad en la entrega de mensajes: la confiabilidad definida por IEC 60834-1 indica los errores de bit que pueden perturbar un sistema de teleprotección, puesto que se rechazan los mensajes recibidos con errores detectados lo que provoca un retraso de la llegada de un comando al extremo de recepción, efecto que también puede provocar pérdida de sincronización. el número aceptable de mensajes no deseados porque pueden causar operaciones no deseadas. No existe ningún requisito o medición similar para los sistemas de IT puesto que tienen la facultad de almacenar y reenviar paquetes, lo que mejora la confiabilidad de IT, pero reduce la confiabilidad de OT.
- Seguridad en la entrega de mensajes: para tecnologías OT existen diversas normas que indican la seguridad que deben tener toda clase de

mensajes que transiten en la red de comunicación de la LAN de una subestación, como es el intercambio de GOOSE, Sampled Values en IEC 62351-6, y para MMS en IEC 62351-4, y otras como IEC 61850 donde indica el número aceptable de mensajes descartados para IED. No existe ningún requisito o medición similar para los sistemas de IT, de hecho, los sistemas de IT eliminan o retrasan de forma rutinaria los paquetes individuales, lo que mejora la seguridad de IT, pero reduce la seguridad de OT.

- Requisitos de disponibilidad: la disponibilidad de la red OT en todo momento es un elemento fundamental, puesto que las fallas en el sistema eléctrico de potencia pueden suceder en cualquier instante y los equipos de protección deben tener los medios disponibles para realizar las acciones de mitigación de fallas respectivas, de no hacerlo puede ser perjudicial para una buena parte del sistema eléctrico. Las estrategias de IT típicas, como reiniciar un componente, generalmente no son soluciones aceptables debido al impacto adverso en los requisitos de OT de alta disponibilidad y confiabilidad.
- Requisitos de gestión de riesgos: los riesgos en una red OT se identifican con base en la prevención de fallas, solución de contingencias técnicas, seguridad humana, cumplimiento normativo manteniendo un vínculo entre la seguridad y protección. En las redes IT la confidencialidad y la integridad de los datos son los factores más importantes.
- Enfoque de seguridad de la arquitectura: para los sistemas OT, los dispositivos de recepción de información como son los relevadores de protección y controladores de bahía deben protegerse cuidadosamente porque son los responsables de controlar los procesos finales, ahora bien,

es correcto considerar la protección del servidor central en un sistema OT porque el servidor central podría tener un impacto adverso en todos los dispositivos periféricos.

En un sistema de IT típico, el enfoque principal de la seguridad es proteger la operación de los activos centralizados y distribuidos de IT y toda la información transmitida entre estos activos, así como la información que se pueda llegar a almacenar en ellos.

Para fines de intersección de información, son los elementos periféricos de IT los encargados de realizar la interconexión entre redes OT e IT cuando se colocan en la intersección de las redes. Los que pueden ser los *routers*, *switches* y multiplexores puesto que utilizan enrutamiento para unir la información entre ambas tecnologías e incluso para unir varias redes dentro del direccionamiento de la capa de red para mensajes.

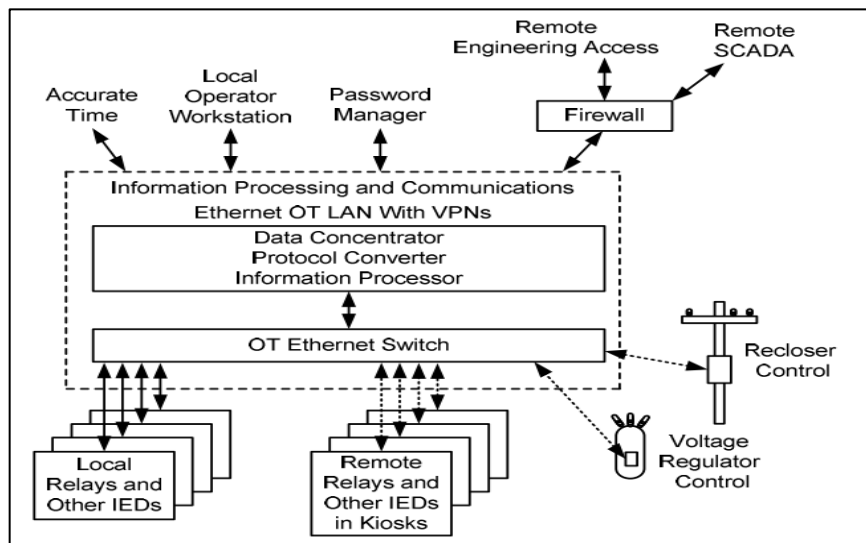
- Comunicaciones: los protocolos libres y de propietarios, y los medios de comunicación utilizados por los dispositivos de OT y la comunicación entre procesadores suelen ser diferentes de los del entorno de IT genérico.
- Gestión del cambio: una de las principales vulnerabilidades que presentan los IEDs en las redes OT es la gestión de actualizaciones de software o parches de seguridad para hardware y *firmware*. El mayor problema radica en que muchas veces los fabricantes de los equipos van actualizando tecnologías y los softwares utilizados en los equipos van quedando fuera de mercado, lo que eventualmente provoca que los equipos sean sustituidos por falta de soporte de los diversos fabricantes, más allá que la vida útil del equipo aún este vigente. En IT el software sin parches representa una de las mayores vulnerabilidades de un sistema,

generalmente las actualizaciones se aplican en periodos establecidos según las políticas y procedimientos de seguridad adecuados.

1.2.5. Intersecciones IT y OT

En el siguiente esquema simple se muestra la interacción entre las tecnologías de IT y OT.

Figura 3. Arquitectura entre IT y OT



Fuente: MOUSSAMIR, Mohamed; DOLEZILEK, David. *The demands and implications of IT and OT collaboration*. p. 9.

Como se observa son los IEDs los que tienen comunicación entre ellos por medio del *switch* de comunicación formando una red LAN propia de tecnología OT por medio de protocolo Ethernet. Luego se aprecia que en un nivel superior se encuentran los equipos que concentran los datos quienes pueden ser unidades terminales remotas (RTU), y *Gateways* los que se aprovechan para

convertir los protocolos de comunicación que se utilizan dentro de la subestación a protocolos adecuados para enviar la información fuera de la subestación, y donde también se aprecia que se generan VPNs; estas son redes privadas virtuales, que se crean para proteger los datos de la subestación creando redes privadas a la red no confiable y de esta manera poder enviar información de manera cifrada otorgando confidencialidad. El dispositivo límite como se aprecia es el *firewall*, selecciona la información que puede salir y entrar a la subestación.

Para posteriormente enviar la información hacia el Centro de Control que es donde se encuentran agrupados varios servicios como son accesos de ingeniería remotos, servidores de ciberseguridad y el envío de datos al SCADA.

1.3. Ataques a sistemas eléctricos

Para el caso de ciberataques a sistemas eléctricos se tienen varios casos, no obstante, al único que se le ha hecho un análisis exhaustivo es el siguiente:

1.3.1. Ataque a la red eléctrica de Ucrania

Retomando el tema y haciendo énfasis a los ataques a sistemas eléctricos se cuenta con el ataque cibernético que se realizó a la red eléctrica de Ucrania el 23 de diciembre de 2015, en Ivano Frankivsk; es uno de los primeros ataques registrado enfocado directamente a un sistema eléctrico, inhabilitando 100 MW de carga, de igual manera fueron víctimas del ataque tres empresas de distribución llamadas Kyivoblenerho, Prykarpattyaoblenerho y Chernivtsioblenerho.

Los intérpretes del ataque mostraron una precisa coordinación y planificación utilizaron *spear phishing* para plantar y suma capacidad para

ejecutar un *malware* llamado BlackEnergy3, que por medio de acceso remoto directo a los puntos ciegos del sistema deshabilitando las computadoras que controlaban el sistema de control, en consecuencia también algunas vías de comunicación ocasionando que la respuesta al ataque fuera un tanto más lenta para conocer la magnitud y restablecer el suministro de energía en las zonas afectadas. El éxito del ataque fue la vulnerabilidad que presentaba el personal para este tipo de casos.

El *spear phishing* es un correo electrónico dirigido a personas, organizaciones o empresas específicas, principalmente uno de los objetivos es el robo de información, su objetivo en ocasiones puede ser el robo de contraseñas por consiguiente en algún momento puede indicar que se ingrese la contraseña de algún acceso restringido para actualización, pero al mismo tiempo es un buen conducto para instalar *malware* en la computadora o sistema atacado.

Para llevar a cabo un ataque de este tipo los atacantes analizan al objetivo, recopilan todo tipo de información sobre cómo actúa la posible, los gustos, plataformas que utilizan la víctima de ataque.

También ejecutan un proceso de personalización, para que el correo incluya toda la información y datos que se recopilaron, luego corresponde a la preparación del ataque.

Debido al ataque a las empresas de distribución de energía eléctrica la consecuencia radicó en que 225 000 usuarios fueran afectados quedando sin el servicio. Los ataques a cada distribuidora ocurrieron dentro de 30 minutos de diferencia entre cada uno, la suspensión del servicio duró aproximadamente 6 horas.

El acceso remoto dio lugar a que la manipulación a los interruptores de potencia se llevase a cabo usando herramientas de administración remota a nivel de sistema operativo, esto derivado de acceder primeramente a la red IT y luego acceder a la red OT obteniendo el control.

El objetivo del ataque fue apagar la energía y hacer que fuese difícil volver a encenderla.

1.3.1.1. Descripción de las tácticas del ataque

Los ataques fueron elaborados de manera que fue evidente la experiencia que tenían los atacantes, desde la estrategia para ganar terreno con la manipulación de documentos de Microsoft Office que contenían el *malware* en las redes de tecnología de la información (IT), de las empresas eléctricas, fue una muestra de la habilidad para la recolección de información para acceder a la red de ICS.

Además, mostraron experiencia en conocer el funcionamiento de los ICS a través del sistema de control de supervisión; como la máquina humana Interfaz (HMI), y luego hacia los elementos de control y protección de las subestaciones, atacando por los elementos de comunicación como los convertidores de serial a Ethernet volviendo la red inoperable.

La manera incisiva de crear caos en la red eléctrica fue la capacidad de los atacantes para realizar acciones a largo plazo operaciones de reconocimiento necesarias para conocer el entorno y ejecutar un ataque que abarcara suficiente extensión territorial.

Desde el punto de vista técnico los elementos que se utilizaron para atacar al sistema fueron la utilización de los *spear phishing* para acceder a las redes empresariales, acciones como la implementación del BlackEnergy 3 en cada elemento que tuviera alcance permitió el robo de las credenciales de las redes comerciales con ello el *hackeo* e intrusión en las VPN ligadas al sistema facilitó el acceso a la red de los sistemas de control industrial (ICS); la disponibilidad de elementos similares a las HMI fue posible otorgar el acceso remoto pudiendo con esto afectar los elementos infectados de comunicación en las OT.

Sutilmente se utilizó un KillDisk para borrar el registro de arranque maestro de los sistemas, impidiendo reiniciar las acciones programadas para restablecer las funciones de los equipos que ejecutaron funciones de apertura de los elementos de bahía, el ataque abarcó diversos elementos hasta las líneas telefónicas para denegar el servicio de comunicación entre los Centros de Control de la red.

Figura 4. **Componentes necesarios para el ciberataque en Ucrania**



Fuente: LEE, Robert; ASSANTE, Michael; CONWAY Tim. *Analysis of the Cyber Attack on the Ukrainian power grid.* p. 2.

Es importante resaltar que los cortes fueron causados por el uso de sistemas de control de OT y su software a través de la interacción directa de los atacantes. Todas las demás herramientas y tecnología, como BlackEnergy 3 y KillDisk, se utilizaron para permitir el ataque o retrasar los esfuerzos de restauración.

1.3.1.2. Las vulnerabilidades del sistema

Los atacantes identificaron las vulnerabilidades del sistema y procedieron a aprovechar los recursos que tenían disponibles, entre ellos estaba el hecho que se contaba con fuentes de información de fuente abierta disponible, incluyendo una lista detallada de tipos de infraestructura, como los proveedores de unidades terminales remotas (RTU), y versiones publicadas en línea por los proveedores de ICS.

Las protecciones para acceder a las VPN (*Virtual Private Network*), son redes con acceso privado, no eran las mejores en efecto fue posible acceder al ICS desde la red empresarial, el *firewall* permitió a los atacantes salir del entorno de administración remota mediante la utilización de una capacidad de acceso directo a la red de los sistemas vulnerables.

A esto se debe agregar que no se contaba con ninguna rutina para monitorear continuamente la red del ICS y buscar anomalías y amenazas a través de medidas de defensa activas, como el monitoreo de la seguridad de la red.

Todas estas vulnerabilidades abrieron paso para que los atacantes para que los atacantes estudiaran el entorno del sistema durante un periodo de tiempo considerable y pudieran desarrollar de manera efectiva el ataque.

Es importante resaltar que los atacantes utilizaron tácticas consistentes en las subestaciones objetivos para impactar elementos controlables de campo dañando irreparablemente estos elementos de control y protección de las subestaciones tras el ataque.

Según los informes públicos del ataque, se desconoce si los objetivos se seleccionaron con base en las tecnologías implementadas en las subestaciones y que fueran comunes entre ellas o de las arquitecturas de sistemas. Las consideraciones basadas en oportunidades para seleccionar un objetivo específico pueden centrarse en la confianza y la capacidad de un atacante para causar un efecto ICS.

1.3.1.3. Uso de la cadena de Cyber Kill de ICS

La cadena Cyber Kill es un proceso de varios pasos dirigido contra una red, y prácticamente es modelo de análisis de intrusión en redes. Consiste en diversos pasos con continuidad y orden que al interrumpir cualquiera de éstos, conlleva a evitar el objetivo del ataque, y estudiando lo suficiente cada fase, es posible implementar las medidas de protección necesarias.

A finales del año 2015, SANS Institute realizó un informe donde se adaptó la Ciber Kill Chain a los sistemas de comunicación y control de sistemas eléctricos de potencia. El enfoque del estudio es dividir el proceso en dos etapas.

Para llevar a cabo un ataque exitoso se necesita conocer las características de los equipos que forman parte de los sistemas de control. Las condiciones típicas en el sistema y arquitectura de una subestación requieren que el atacante tenga que evitar la sobrepasar la seguridad de los equipos destinados al control

del sistema y que en múltiples ocasiones las dificultades intrínsecas que enfrenta el atacante son superadas por conexiones directas a internet.

Las dos etapas que propone la cadena de Cyber Kill son:

La primera parte, tiene relación directa con los conceptos de espionaje u operaciones de inteligencia. La estructura de ataque para la etapa 1 se muestra a continuación:

- Planificación: consiste en acciones de reconocimiento con la finalidad de recopilar información del objetivo de ataque, realizando investigación con herramientas libres basada principalmente en OSINT, para identificar debilidades.
- Preparación: consiste en definir la vía de intrusión, incluyendo un fichero para uso en las fases siguientes y la elección de un objetivo para el ataque, con esto, se eligen las herramientas a utilizar.
- Intrusión: consiste en cualquier intento de acceso a las redes o sistemas del objetivo de ataque. En el caso de un acceso exitoso, el atacante aprovechará la oportunidad de vulnerabilidad del sistema e implementará puntos de ruptura para aprovecharlos en accesos posteriores.
- Gestión y habilitación: al lograr la intrusión, el próximo paso es en sí misma la gestión, el atacante establece uno o varios sistemas de control y comando.
- Logística, desarrollo y ejecución: esta se caracteriza por la acción del atacante, donde es posible la detección de capacidades para realizar

accesos en diferentes puntos de tope en la red, entre otros. Esta tarea es crítica para el comienzo de la segunda etapa.

En la siguiente figura se muestra la estructura de la fase 1 incluyendo los pasos contenidos en cada acción, estos son: reconocimiento, preparación, distribución, explotación, instalación, comando, control y por último actuación.

Figura 5. **Estructura etapa 1**



Fuente: Incibe-cert. *Cyber Kill Chain en sistemas de control industrial*. <https://www.incibe-cert.es/blog/cyber-kill-chain-sistemas-control-industrial>. Consulta: 13 de noviembre de 2021.

Cuando el sistema objetivo es vulnerable y reconocido estratégicamente por el atacante se da por concluida la etapa 1. En ocasiones, la información acerca de la vulnerabilidad que se puede encontrar en el sistema a atacar, se consigue indirectamente de una fuente interna, lo que ahorra todos los pasos a seguir en la etapa 1. En estos casos, únicamente la segunda etapa, y se describe en la siguiente figura:

Figura 6. **Estructura etapa 2**



Fuente: Incibe-cert. *Cyber Kill Chain en sistemas de control industrial*. <https://www.incibe-cert.es/blog/cyber-kill-chain-sistemas-control-industrial>. Consulta: 13 de noviembre de 2021.

Para la etapa 2 se utiliza la información recopilada durante la primera etapa para elaborar un ataque dirigido, no necesariamente tienen que ser inmediatamente continuas. Las fases que normalmente se presentan para la cadena son las que se muestran a continuación:

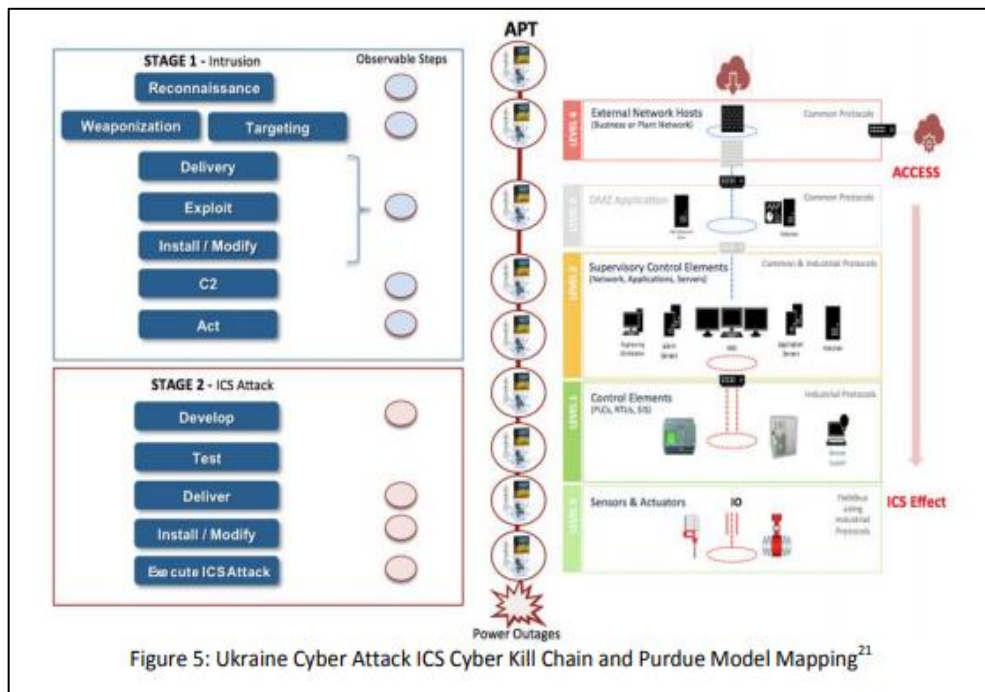
- Ajuste y desarrollo del ataque: en este paso el atacante tiene como objetivo crear un procedimiento o método que afecte específicamente a la infraestructura de control objetivo.
- Validación: esta acción tiene como objetivo confirmar que el procedimiento o método tendrá efectos esperados en un entorno similar o igual al que se pretende atacar, se realizan prácticas para simular los ataques en entornos industriales.

- Ataque: esta es la acción final donde el atacante tiene la posibilidad de aplicar el procedimiento a través de la capacidad desarrollada la ejecución. Normalmente las consecuencias generadas por un ataque es la extracción de información lo que conlleva la pérdida de datos, que el sistema colapse permitiendo denegar acceso a internos y la alteración de algoritmos y datos al ser manipulados.

La complejidad del ataque y tener éxito en ello siempre dependerá de las medidas de seguridad implementadas en el sistema objetivo.

Ahora bien, el ataque a la red eléctrica ucraniana siguió por completo los pasos y características de Cadena Cyber Kill Chain. El ataque obtuvo acceso a cada nivel de ICS, como se muestra en la figura, con la Cyber Kill Chain de ICS trazada junto con un modelo de segmentación / jerarquía (por ejemplo, modelo de Purdue modificado).

Figura 7. **Modelo del mapa del ciberataque con Cyber Kill**



Fuente: LEE, Robert; ASSANTE, Michael; CONWAY Tim. *Analysis of the Cyber Attack on the Ukrainian power grid*. p. 5.

1.3.1.4. **Ataque a Ucrania aplicado a etapa 1**

En la etapa 1, para la etapa de planeación, un análisis realizado a las estructuras muestra que las tres empresas atacadas fueron elegidas por las características del sistema de automatización y control del sistema de distribución, dado que mostraban vulnerabilidades similares. Dado el grado de coordinación que tuvo el ataque descarta que el ataque haya sido aleatorio y da indicios que en efecto existieron ciertas actividades de reconocimiento.

Para la fase de preparación, definiendo la vía de intrusión y selección de objetivos, para este ataque no fue necesario apuntar a una infraestructura

específica para obtener el acceso, puesto que los atacantes utilizaron documentos de sistema operativo de Windows y Microsoft Office, de Excel y Word, puntualmente, que incorporaban el BlackEnergy3.

En la fase de intrusión cibernética, se procedió a entregar los documentos maliciosos de Office vía correo electrónico a personal que ejercía labores específicamente en la red corporativa administrativa y aparentemente del área de informática de cada empresa distribuidora. El objetivo de los correos fue incentivar al personal a habilitar los macros en el documento abierto. Al habilitar macros se permitió la instalación del BlackEnergy3 en el sistema, permitiendo que el *malware* las funcionalidades de macros del office de la máquina atacada.

En la fase de gestión y habilitación, luego de que el *malware* fue instalado, éste se conectó a direcciones IP de control haciendo posible la comunicación entre el atacante con el *malware* y logrando así acceso a los sistemas infectados tras una recopilación de información del sistema. Con base en análisis se estima que la recopilación de información inició seis meses antes del ataque, donde el atacante recolectó credenciales que fueron punto de partida para estudiar los segmentos de la red donde existían las estaciones de trabajo y los servidores de despacho SCADA, otras acciones fueron escalar privilegios y moverse lateralmente por el entorno, logrando con esto, obtener un posible acceso persistente a los objetivos.

Teniendo los puntos de apoyo iniciales y las vulnerabilidades identificadas es muy probable que los atacantes se alejaran rápidamente de estos para integrarse en los sistemas como usuarios autorizados. Teniendo lograda esta posición ya es posible identificar conexiones VPN y avenidas desde la red empresarial hacia la red ICS realizando con esto la etapa de logística y

fortificación haciendo uso de conexiones y comandos nativos para extraer datos necesarios y pasar a la etapa 2.

1.3.1.5. Aplicado a etapa 2

En esta etapa los atacantes utilizaron al menos dos estrategias, la primera fue aprovechada por la información recopilada acerca de los dispositivos de campo que se encontraban en las subestaciones, tales como la conversión de protocolos de comunicación de la red del sistema de control al SCADA y con los tres entornos de los sistemas de administración de distribución (DMS), y utilizando los elementos de control del sistema. La segunda fue el desarrollo de *malware* para infectar los dispositivos Serie a Ethernet.

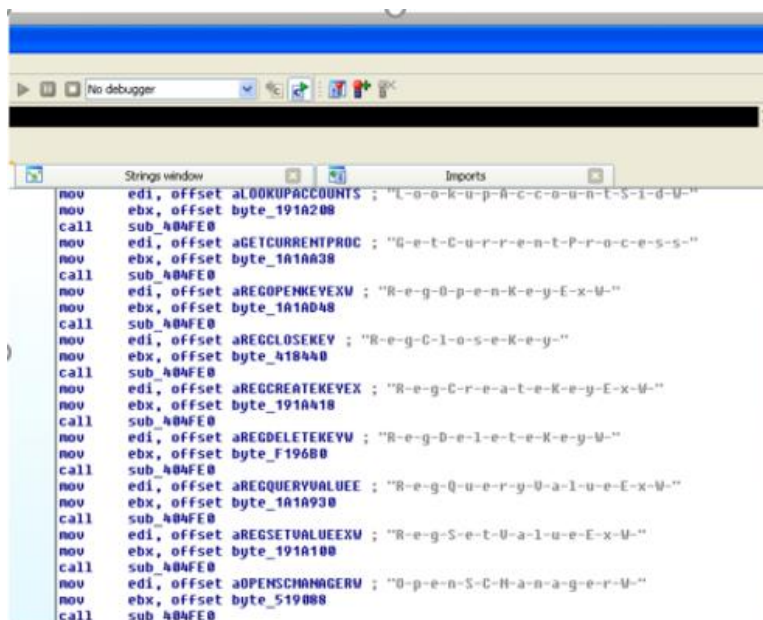
Como parte de la fase de validación es probable que los atacantes tuvieran un sistema para realizar pruebas de ejecución de su *malware* antes del ataque.

Para la fase de ataque para tomar el control de los elementos de ICS utilizaron acceso VPN en el entorno de IT, y reconfiguraron al menos una red conectada a un UPS para que cuando se provocara un corte de energía fuera seguido por un evento que también impactaría la energía en los edificios o datos del Centro de Control.

Como fase final para el ataque, los adversarios completaron la etapa Instalar el software malicioso identificado como un KillDisk. Es probable que los atacantes se aseguraran de que sus modificaciones al UPS estuvieran listas para el ataque, siendo el último acto de modificación el hecho que los atacantes tomaran el control de las estaciones de trabajo del operador y, es por esta razón que bloquearan a los operadores fuera de sus sistemas. La Figura muestra el análisis estático de las importaciones de la interfaz de programación de

aplicaciones (API), de KillDisk después del evento. Tomando en cuenta la fase final del ataque al ICS se tuvo acceso a las HMI desde el entorno del SCADA para dar señal de disparo de los interruptores.

Figura 8. **Análisis estático de API**



Fuente: LEE, Robert; ASSANTE, Michael; CONWAY Tim. *Analysis of the Cyber Attack on the Ukrainian power grid*. p. 8.

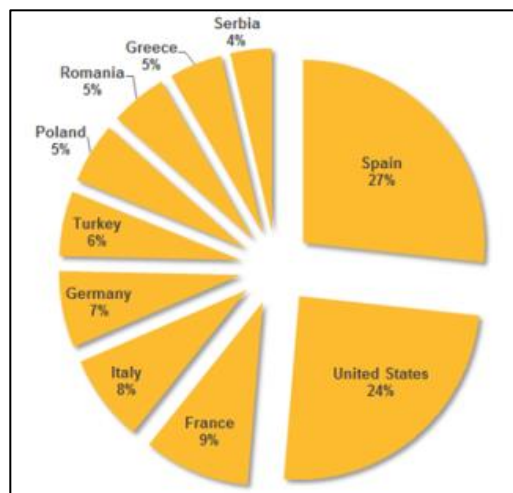
1.3.2. Otros ataques en el transcurso de la historia

En 2016 un Ciberataque masivo contra empresas energéticas de Estados Unidos consistió en atacar variedad de plantas de generación eléctrica. En Europa algunos países también fueron afectados por este ataque, siendo España el país más afectado concentrando un 27 % del total de equipos infectados por un *malware* espía.

El ataque tuvo gran alcance y por investigaciones realizadas se sostuvo que el ataque tuvo origen en Rusia. Los atacantes lograron infectar el software encargado del control mediante un virus troyano similar a Stuxnet, que pertenece a la familia de los malware, esto permitió acceso a los atacantes de manera remota.

Al suceso se le dio el nombre de Dragonfly, también conocido como Energetic Bear, este ataque se realizó con intenciones de espionaje, ahora bien, el ataque si tuvo la posibilidad y capacidad de realizar sabotaje en las redes eléctricas interrumpiendo el suministro de energía, pero no se llevó a cabo. Los países más perjudicados fueron Estados Unidos, Italia, Alemania, España, y el resto se aprecia en la siguiente figura:

Figura 9. Países afectados por Dragonfly



Fuente: Expansión.com. *Ciberataque masivo contra empresas energéticas de Europa y EEUU: España es el país más afectado.*

<https://www.expansion.com/2014/07/01/empresas/energia/1404200654.html>

Consulta: 13 de noviembre de 2021.

Los investigadores creen que el autor del ataque Dragonfly está respaldado por un estado nación que estaba reuniendo información y posiblemente preparaba el terreno para ejecutar ataques futuros.

Otro de los ataques al sector energético fue uno hacia un proveedor de servicios en la nube que afectó a los sectores de gas natural, petróleo y energía eléctrica, tuvo lugar en abril del 2018. El ejecutor se considera desconocido.

Los analistas determinaron un ataque por ransomware, es un *malware* que impide al usuario acceder a su sistema y a cualquier archivo, y en el ataque éste paralizó las computadoras de la empresa y exigieron a cambio un pago por la clave para descifrar los archivos.

El impacto que tuvo fue la interrupción de las comunicaciones electrónicas de al menos cinco empresas de gasoductos de gas natural, logrando que el seguimiento y la programación de los pasos de gas se demoraran, provocando que algunos grandes proveedores de energía cortaran los enlaces con la plataforma que les brinda información de precios y modelos de demanda para las transacciones de cobros de electricidad.

Un punto importante es que no se interrumpió el flujo de gas o electricidad, pero se expuso la interdependencia entre ambos sectores y cierta vulnerabilidad a través de un ataque en la cadena de suministro.

Otro ataque relevante es NotPet como dado que paralizó las operaciones en varios sectores, tuvo un costo de al menos USD 10 000 millones en daños en todo el mundo, este fue un suceso ocurrido en junio de 2017 y tuvo su origen en Ucrania. Los atacantes *hackearon* los servidores de un proveedor de software

contable y enviaron actualizaciones corruptas de software a los clientes de todo el mundo.

El ataque tuvo impacto en seis plantas eléctricas locales y saltó a sucursales tanto en Ucrania como el resto del mundo provocando la interrupción de operaciones en varios sectores de industria en general, transporte y salud.

Uno de los orígenes del problema aparentemente fue el software de contabilidad MeDoc que en su momento se usaba de forma masiva en empresas ucranianas.

Respecto al *malware* se reportó inicialmente como un brote de Peyta. Es un ransomware que cifra la información de las computadoras infectas y pide el pago de un rescate para descifrarlas y se centra en archivos con extensiones de lenguajes de programación como los de Python y Visual Basic, también hace uso de vectores de infección como el exploit EternalBlue. La versión tenía una sintomatología parecida al WannCry derivado de su manera de propagación en redes corporativas aprovechando las vulnerabilidades en sistemas Windows, y de otro exploit llamado EternalRomance que hace uso del puerto TCP 445 o de herramientas como psexec, por esos motivos, el ataque fue bautizado como NotPeyta, ExPetr o Nyetya. Los exploit son vulnerabilidades de seguridad que se aprovechan para un ataque.

1.4. Normas aplicables para ciberseguridad en subestaciones eléctricas

Los dos estándares que se presentan son los focos de estudio que se utilizan en el presente estudio para el análisis de seguridad implementada en las subestaciones del Sistema Nacional Interconectado de Guatemala.

1.4.1. IEEE C37.240

Se basa en detallar los requisitos de ciberseguridad, sistemas de automatización, protección y control para subestaciones.

Presenta prácticas de ingeniería, manteniendo una perspectiva para la viabilidad técnica, económica y operacional para implementar un programa de ciberseguridad, donde de manera que no se pierda la seguridad y confiabilidad de los sistemas, y donde la seguridad se puede dividir en dos tipos: la seguridad física y la ciberseguridad.

La seguridad física se enfoca en el perímetro físico, por ejemplo, proteger los puntos de acceso a la subestación, para que no se tenga acceso a los equipos de patio, tableros de control, protección y medición y dispositivos de comunicaciones. La ciberseguridad se enfoca en los datos en reposo y los datos en movimiento.

Los datos en reposo son los que se almacenan físicamente en los diversos formatos digitales, como son hojas de cálculo, archivos, oscilografías, parametrizaciones, reporte de fallas, incluso diagramas y listas de contraseñas. Los datos en movimiento son los que continuamente son procesados por los diversos IEDs instalados para que puedan tomar decisiones.

El estándar también recomienda organizar los accesos a la información de los distintos niveles de la subestación utilizando buenas prácticas de un control de acceso basado en roles, de manera que se pueda contar con una autenticación para cada usuario asignado por medio de credenciales recomendadas y al mismo tiempo contar con un plan de auditoría que lleve el registro de accesos exitosos e intentos fallidos a los diversos dispositivos y

sistemas realizados por los diversos usuarios autorizados y denegar cualquier tipo de acceso en todo el sistema a usuarios no autorizados.

También menciona buenas prácticas de seguridad física para los activos de la subestación, refiriéndose al estándar IEEE 1402; establece los diversos niveles de seguridad física que deben tener las instalaciones.

Establece los requerimientos mínimos de cifrado y gestión de contraseñas que tienen que tener los diversos IEDs instalados y requisitos mínimos de seguridad que deben tener los elementos de comunicación como son los *switches* de comunicación, *routers* y *firewall* para que protejan de manera correcta la red de comunicación propia de la subestación desde los relevadores de protección y controladores de habia hasta los equipos de control y monitoreo de la subestación como son los Gateway, unidades terminales remotas y HMI, estableciendo los requisitos que deben cumplir, como la seguridad en la red de comunicación que interconecte a todos los dispositivos.

1.4.2. IEEE 1686

Este estándar es una guía y define funciones características para la operación y configuración que deben proporcionarse en los dispositivos electrónicos inteligentes de la subestación para adaptarse a programas de ciberseguridad, de acuerdo con programas de protección de infraestructura crítica que por sus siglas en inglés CIP que sean aplicados en las empresas. Cada empresa debe evaluar las recomendaciones de seguridad que se recomiendan en este estándar, dependiendo de la configuración y operabilidad que tenga en sus subestaciones en particular.

Se indican todas las medidas de seguridad en la configuración de los equipos con el objetivo de evitar accesos de usuarios no autorizados a los IEDs y al mismo tiempo para que se generen alarmas por intentos de acceso fallidos e intrusión de usuarios no autorizados. Establece requerimientos mínimos para las contraseñas y la configuración y número de usuarios mínimos que debe tener cada IED independientemente de su función de control, protección o monitoreo.

Establece el uso de un control de acceso basado en roles para limitar acceso a la configuración evitando que cualquier usuario tenga acceso a realizar cualquier tipo de cambio no autorizado en la parametrización de los dispositivos. También se establecen requerimientos mínimos de acceso físico estableciendo un perímetro de seguridad.

La gestión de contraseñas también es un alcance fundamental de la norma, como dado que estas se deben gestionar con cierta frecuencia, al mismo tiempo el monitoreo en tiempo real del estado de los IEDs y revisión de alarmas habilitadas y deshabilitadas.

Determina las condiciones que se deben considerar para los diversos accesos que puede tener el equipo, físicamente por medio de cable, por medio de la HMI desde la misma subestación o bien, acceso remoto desde un SCADA.

La administración para la actualización de *firmware* es un factor importante, como las actualizaciones del software de configuración y los diversos controles que se pueden adoptar para mantener el dispositivo en óptimas condiciones.

Este estándar define una tabla de cumplimientos de requisitos donde se abarcan todas las medidas de seguridad recomendadas por el estándar, que por sus siglas en inglés se define como TOC (*Table of Compliance*), y donde para

cada subcláusula puede ser definida por cada usuario, pudiendo colocar el grado de cumplimiento que se presente en sus IEDs.

Otro estándar que no se aplica a fondo en el presente estudio, pero que es fundamental para la ciberseguridad en los protocolos de comunicación es la siguiente:

1.4.3. IEC 62351

Este estándar desarrolla diversas técnicas y recomendaciones para implementar una arquitectura de comunicación segura en una subestación, tomando en cuenta la ciberseguridad para cada protocolo que se pueda utilizar entre todos los IEDs, *switches* de comunicación, unidades terminales remotas y con el Centro de Control. El estándar tiene diversos alcances y se divide en las siguientes partes:

Tabla II. Partes que conforman el estándar IEC 62351

IEC 62351	Definición de servicios de seguridad para
Parte 1	Introducción y visión general
Parte 2	Glosario de términos
Parte 3	Perfiles que incluyen TCP/IP
Parte 4	Perfiles incluyendo MMS
Parte 5	Seguridad para protocolo IEC 60870-5 y derivados
Parte 6	Seguridad para perfiles con IEC 61850
Parte 7	Modelos de objetos de datos de gestión de redes y sistemas (NSM)
Parte 8	Control de acceso basado en roles para gestión de sistemas de potencia
Parte 9	Gestión de claves
Parte 10	Directrices de arquitectura de seguridad
Parte 11	Seguridad para archivos XML

Fuente: elaboración propia.

2. SUBESTACIONES ELÉCTRICAS

2.1. Subestaciones convencionales

La definición del concepto de subestación eléctrica desde un punto de vista conceptual es fundamentalmente lo que se encuentra en un circuito eléctrico, es un nodo que funciona como entrada de corrientes que circulan a través del circuito dependiendo de su configuración. Técnicamente una subestación es un nodo que forma parte del sistema de potencia y es en donde se logra abrir o cerrar el paso de una o varias ramas del sistema sin discriminar una función fundamental.

Entre las funciones que puede tener una subestación están elevar o reducir el voltaje que entra en dicha subestación y es en otras palabras transformar niveles de tensión y derivar circuitos de potencia y todos los circuitos se unen en un componente de la subestación; estas son las barras y el elemento principal para las maniobras de apertura y cierre son los interruptores de potencia, seguidamente por el transformador que es el principal componente para realizar cambios de niveles de tensión.

Las funciones de la subestación se logran a través de los elementos primarios como interruptores de potencia, secciones, transformadores de instrumentos y equipos secundarios como relevadores de protección, medidores, controladores de bahía en conjunto de otros equipos de monitoreo y comunicación. Los niveles de tensión que se le pueden asignar a una subestación se realizan bajo varios criterios:

- Si la estructura de la zona de la red a la que pertenece la subestación es radial, la tensión se puede fijar en función de la potencia de la misma.
- Si la alimentación proviene de una configuración del sistema de potencia que esté en anillo, la tensión de la subestación queda obligada a tener la tensión del anillo.
- En el caso que la tensión se tome de una línea de transmisión cercana, la tensión queda definida por el valor de tensión de la línea.

Los valores de tensión para un sistema de potencia están normalizados, dependiendo las funciones en las redes de potencia y las normas internas de las empresas propietarias de los componentes del sistema eléctrico, cada país define los niveles de tensión normalizados a utilizar.

Los niveles de tensión según la norma IEC 60038 y se indican en la siguiente tabla:

Tabla III. **Valores normales de tensiones entre fases**

Tensiones nominales del sistema kV		Tensión máxima para el equipo kV
66	69	72.5
110	115	123
132	138	145
150	161	170
220	230	245
275	287	300
330	345	362
380	400	420
500		525
700 a 750		765

Fuente: RAULL MARTÍN, José. *Diseño de subestaciones eléctricas*. p. 5.

Los niveles de tensión antes mencionados pueden agruparse en los siguientes rangos:

Alta tensión AT: $52 \text{ kV} \leq U_m < 300 \text{ kV}$

Extra alta tensión, EAT: $300 \text{ kV} \leq U_m \leq 550 \text{ kV}$

Ultra alta tensión, UAT: $U_m \geq 800 \text{ kV}$

Los niveles de tensión aplicados en subestaciones en el sistema eléctrico de Guatemala son los siguientes:

- 13,8 kV para distribución
- 34,5 kV para distribución
- 69 kV para Transmisión
- 230 kV para Transmisión
- 400 kV para la interconexión entre el sistema eléctrico entre México y Guatemala en Subestación Brillantes.

Luego de tener claros los niveles de tensión que se manejan en los sistemas de potencia, se pueden definir los tipos de subestaciones.

- Subestaciones variadoras de tensión
- Subestaciones de maniobra y seccionadoras de circuito
- Subestaciones mixtas (mezcla de las dos anteriores)

De las que se derivan las siguientes agrupaciones:

- Subestaciones de transmisión $>$. a 230 kV
- Subestaciones de subtransmisión. Son las que están entre 230 y 115 kV.

- Subestaciones de distribución primaria. Entre 23 y 115 kV.
- Subestaciones de distribución secundaria. Debajo de 23 kV

El medio de aislamiento para los elementos de las subestaciones de igual manera depende mucho de la densidad del medio y del nivel de voltaje que se maneje en la subestación, de manera que se tienen tres.

2.1.1. Subestaciones aisladas en aire (AIS)

Consiste en colocar la Aparamenta y otros equipos de alto voltaje donde el aislamiento a tierra y entre conductores de fase es proporcionado principalmente por aire a presión atmosférica y donde algunas partes activas no están encerradas (de IEC 6050-605-02-13).

Este tipo de subestación cuenta con la ventaja respecto a los elementos que la conforman, tienen precios relativamente accesibles siendo no tan costosos en comparación con otras soluciones, como dado que existen diversidad de marcas y dado que su medio de aislamiento es el aire, este tiene diversidad de valores de densidad conforme se aumente la altitud del terreno donde se instala la subestación y diferentes grados de contaminación del medio.

2.1.2. Subestaciones aisladas en gas (GIS)

La aparamenta se encuentra contenida en recipientes metálicos y otros equipos de alta tensión en los que el aislamiento se obtiene, al menos en parte, mediante un gas aislante distinto del aire a presión atmosférica (de IEC 62271-203, 3.102).

Este gas suele ser SF6 o una mezcla de SF6 con otros gases, por ejemplo, nitrógeno y otros tipos de gas que se encuentran en evaluación.

El equipo GIS suele ser la opción más costosa, tiene la mayor ventaja de ser solución compacta. Esto significa que la cantidad espacio físico requerido para la subestación será mucho menor que para una subestación AIS.

2.1.3. Aparamenta de tecnología mixta (MTS)

Equipo que se ha desarrollado a partir de AIS o GIS en una de las siguientes combinaciones:

- AIS en diseño compacto y / o combinado
- GIS en diseño combinado
- Aparamenta con aislamiento híbrido donde las bahías están hechas de una combinación de AIS y GIS, acá se encuentra la aplicación de subestaciones con diseños híbridos como DTC's donde prácticamente toda la bahía se encuentra encapsulada, interruptor, seccionadores, transformadores de potencial y corriente.

Las MTS tienen la ventaja de ser compactas, combinar múltiples funciones y bondades de las soluciones AIS y GIS. La solución ocupa relativamente menor espacio físico que una AIS y sin dejar de ser significativamente más barato que GIS.

Esto se puede utilizar cuando los costos de la tierra son moderados y se desea implementar una solución compacta y rentable para nuevas subestaciones.

Algunas características importantes con las que deben cumplir las subestaciones de todos los tipos son las siguientes:

- **Flexibilidad:** es una propiedad que tiene como finalidad la adaptación de las subestaciones a los cambios de infraestructura, integración de nuevas bahías, cambios operativos por contingencias generadas en el sistema de potencia. Un factor más a considerar es el mantenimiento que se tenga que brindar a los equipos y elementos de la subestación.
- **Confiabilidad:** es una propiedad que tiene como finalidad mantener y garantizar el suministro de energía en el sistema de potencia bajo cualquier contingencia y durante un periodo de tiempo determinado en caso el barraje o algún elemento de la subestación se encuentre fuera de servicio, es decir, la confiabilidad tiene como condición de que al menos un componente de la subestación no pueda repararse durante la operación.
- **Seguridad:** esta propiedad incluye a la confiabilidad dado que la finalidad es dar continuidad del suministro de energía, pero a diferencia de la confiabilidad, esta propiedad lo hace sin interrupción alguna durante fallas en los equipos fundamentales en la subestación como son los equipos de potencia y las barras en una subestación.

2.1.4. Tipos de subestaciones

Según el tipo de aplicación que se necesita, para cubrir necesidades del sistema eléctrico en donde se requiere instalar un nodo para la conexión de varios puntos para alimentador y sus derivaciones, se denominan como bahías, circuitos o campos.

2.1.4.1. Subestaciones de generación

Estas subestaciones son las que forman parte de una central generadora, la energía es generada y necesita una subestación elevadora para su respectivo transporte por medio de líneas de transmisión.

En cuanto a las consideraciones principales es necesario dar prioridad respecto a la aplicación de la subestación, dependiendo de esto se le puede dar un adecuado nivel de seguridad, dependiendo lo que la configuración requiera.

2.1.4.2. Subestaciones de maniobra

Estas subestaciones son las encargadas de realizar las conexiones o desconexiones de circuitos en el sistema de potencia, dependiendo de la estabilidad que se debe conservar para reducir los aportes de niveles de cortocircuito en algún sector, o para fines de regulación de voltaje.

Esta subestación no cuenta con transformador como dado que su función es meramente de *swicheo*. Este tipo de subestación requiere principalmente de flexibilidad.

2.1.4.3. Subestaciones de transformación

Estas subestaciones normalmente pertenecen al sistema de transmisión donde es necesario transformar los niveles de tensión de las líneas de transmisión que llevan la energía producida por las centrales generadoras hacia los centros de consumo, o bien para elevar los niveles de tensión nuevamente para llevar la energía a consumidores lejanos.

Este tipo de subestación requiere principalmente de confiabilidad, la seguridad también puede ser una importante necesidad.

2.1.5. Configuraciones de las subestaciones

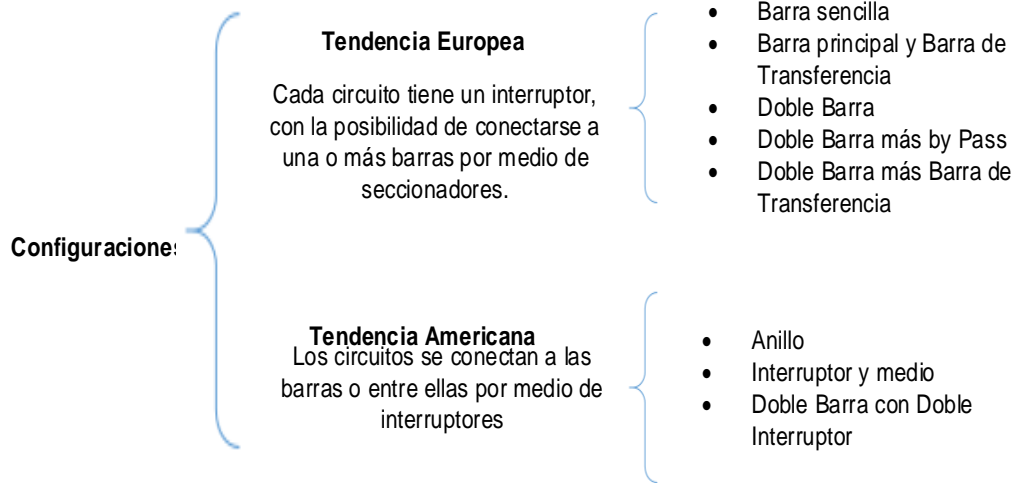
En una subestación es muy importante elegir la configuración de subestación correcta para la funcionalidad como valor agregado del sistema de potencia, el costo y las dimensiones de la misma; cada bahía de la subestación cuenta con un interruptor para abrir y cerrar la conexión y la utilidad de los seccionadores para conectarse a las barras.

La elección de la configuración o también conocido como arreglo de barras, requiere de un estudio previo donde se determinan aspectos relevantes como: los requerimientos de las demandas de la energía, las aplicaciones del sistema y las ventajas y desventajas desde el punto de vista para las compañías propietarias de las subestaciones, viabilidad para el mantenimiento, así como los costos de la compra de los equipos que conformarán la subestación.

Existen dos tipos de tendencias en las configuraciones de las subestaciones, estas son:

- La tendencia europea: cada circuito, campo o bahía tiene un interruptor, y estos equipos se conectan por medio de seccionadores a una o más barras.
- La tendencia americana: donde el principal elemento de conexión de cada circuito, campo o bahía son los interruptores y estos se conectan a las barras.

Figura 10. **Configuración de subestaciones según su tendencia**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

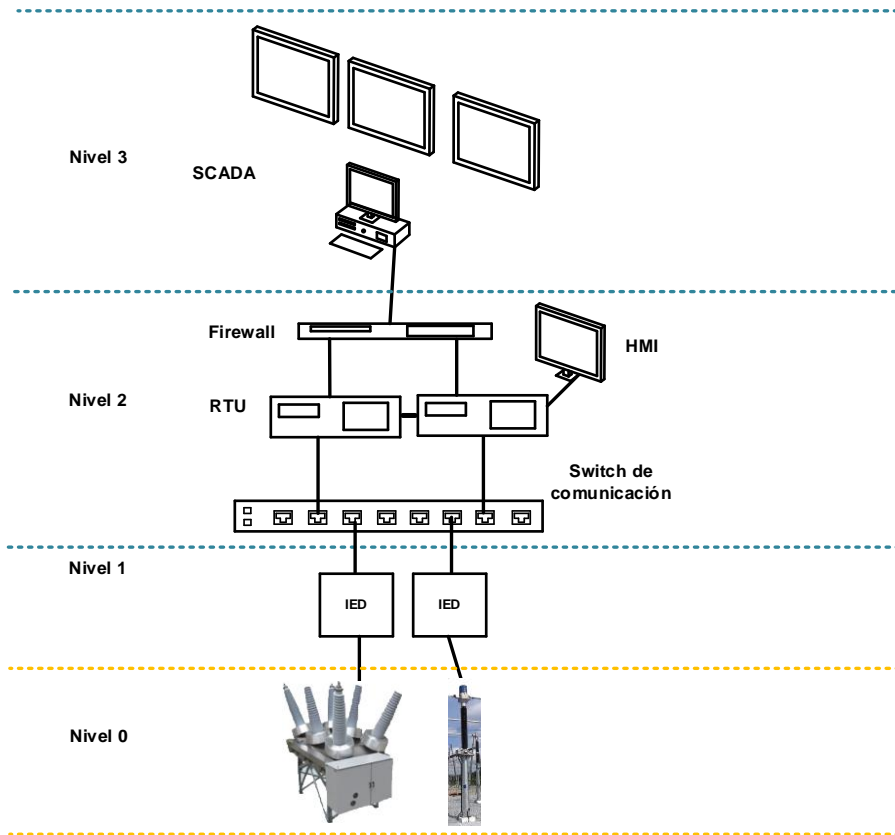
2.1.6. Niveles de control/operación de las subestaciones

Las subestaciones se dividen en diferentes niveles según las funciones que poseen los equipos que la conforman, cuyas funciones son de la automatización de toda la subestación.

El objetivo de dividirlos es poder clasificarlos según el tipo de operación que realizan ya sean de control, protección, comunicación o monitoreo.

Se pueden dividir en cuatro niveles, que se muestran en la siguiente figura.

Figura 11. Niveles de mando de subestaciones



Fuente: elaboración propia, empleando Microsoft Visio 2016.

A continuación, se detallan los diversos niveles:

2.1.6.1. Nivel de patio (nivel 0)

Está compuesto por los equipos primarios, su ubicación es el patio de maniobras, estos pueden tener diversas características dependiendo del medio de aislamiento, en el caso de las subestaciones aisladas en aire, los equipos son robustos con aisladores de porcelana o polímero ubicados a las distancias correctas en la parte de alta tensión.

Para realizar cualquier operación en este nivel de la subestación, es necesario ir a patio ejecutar la acción, por ejemplo, insertar la manivela en los seccionadores o colocar la posición de operación local en los interruptores de potencia.

Las maniobras correspondientes dependen del sistema de control de este nivel, que, reside en el propio mando y lógica de control implementados en los equipos de patio, pudiendo ser controlados de manera local, por ejemplo, los bloqueos de SF6 en los interruptores. La comunicación entre equipos por medio del cableado para una subestación convencional, de igual manera la comunicación puede llegar a los equipos primarios desde equipos de niveles superiores como pueden ser las protecciones o bien las HMI.

Para las maniobras es importante las funciones del control local remoto, donde se puede tener control de los equipos como interruptor, y según la posición que tenga puede tener cierto grado de protección para el personal que esté realizando algún trabajo de mantenimiento o inspección directamente en el interruptor, evitando que desde el Centro de Control se envíe una señal de disparo o por medio de los controladores de bahía que reportan los equipos de niveles superiores.

Características importantes para tomar en cuenta en los equipos de patio son:

- El valor de tensión asignada, corresponde al mayor nivel de tensión para el que se fabricó el equipo, según norma IEC 60694.
- El nivel de aislamiento asignado son los valores de tensión que son soportadas por los diversos aislamientos para equipos primarios para

evitar la generación de arcos eléctricos entre los polos de los equipos entre fases y a tierra, calculando la rigidez dieléctrica para brindar un aislamiento confiable, esta sobretensión se dimensiona con base en la resistencia para el impulso tipo rayo.

Las corrientes generadas en los elementos de las subestaciones no dejan de ser menos importantes.

- Corriente asignada en servicio continuo (I_r): esta magnitud es la que se reconoce como el valor eficaz que los equipos deben soportar en todo momento de su funcionamiento.
- Corriente de corta duración admisible asignada (I_k): es el valor eficaz de corriente que los equipos de maniobra como es el caso de los interruptores, pueden soportar antes de la apertura en un tiempo corto determinado por los fabricantes. Este valor de corta duración puede ser igual al valor de cortocircuito asignado.
- Valor pico de la corriente admisible asignada I_p : es el valor pico de corriente en el primer ciclo de la corriente de corta duración admisible, que un equipo puede soportar en posición cerrada.
- Duración asignada del cortocircuito I_k : es el intervalo de tiempo que el equipo debe soportar, en posición cerrada una corriente igual a la corriente de corta duración admisible asignada, el valor del tiempo normalmente es de 1 segundo, en su defecto es de 3 segundos.

Los elementos más comunes en este nivel de la subestación son los siguientes equipos:

- Interruptores de potencia
- Seccionadores, con o sin cuchilla de puesta a tierra
- Transformadores de instrumentos
- Transformadores de potencia
- Pararrayos.

Algunos equipos que son importantes en el nivel de campo de las subestaciones son los siguientes:

2.1.6.1.1. Interruptores de potencia

Son los equipos ubicados en las bahías de las subestaciones cuya funcionalidad principal es la apertura y cierre de la continuidad de potencia hacia un circuito energizado. Son equipos construidos con una cámara especialmente fabricada para la mitigación de arco eléctrico formado por la interrupción de un circuito conectado a carga.

Los interruptores de potencia también conocidos como *Circuit Breakers*, son los elementos ideales para en aislamiento de aire (AIS), y Aparamenta aislada en gas (GIS). El funcionamiento de estos equipos es mecánico, Los disyuntores de alto voltaje son mecánicos fabricados especialmente para funcionar en condiciones normales a corriente nominal en posición cerrada y poder abrirse sin dañar si mecanismo de interrupción durante el transcurso de una corriente de falla.

Estos equipos no poseen la capacidad de pensar por sí solos y abrirse para aislar y cortar el suministro de energía, es decir que carecen de inteligencia propia, en efecto las funciones ante fallas se hacen mediante los elementos de protección por medio de los transformadores de instrumentos; envían señales de

voltaje y corriente a dichos elementos enviando señales de disparo al mecanismo de apertura; estos están conformados por bobinas de disparo.

Figura 12. **Interruptores de potencia de tanque muerto**



Fuente: FINN, John; KRIEG, Terry. *Study Committee B3: Substations*. p. 262.

2.1.6.1.2. Seccionadores

Estos equipos son los encargados de seccionar las distintas bahías de una subestación, aislando los interruptores de las barras conductoras y al mismo tiempo aislando los interruptores de la parte de los circuitos que conducen hacia las cargas, para la necesidad de realizar mantenimiento o bien, por motivos de fallas, en otras palabras, cumple la función de aislar de manera segura dos partes de un circuito.

Es necesario hacer hincapié en el hecho de que la apertura de un seccionador se debe realizar sin carga o con los dos extremos del seccionador

bajo tensiones equipotenciales con el propósito de evitar la generación de arco eléctrico, como dado que, a diferencia de los interruptores, estos elementos no poseen una cámara interruptora adecuada para soportar los esfuerzos por generación de arco lo que proporciona grandes daños a los contactos del seccionador.

Figura 13. **Seccionadores de apertura central**



Fuente: FINN, John; KRIEG, Terry. *Study Committee B3: Substations*. p. 265.

2.1.6.1.3. Transformadores de instrumentos

Son elementos electromagnéticos cuya función principal es reducir a valores estándar las magnitudes de tensión y corriente que se utilizan en elementos que mantienen en correcto funcionamiento una subestación.

Es importante definir el concepto de burden, es la impedancia que se coloca en el secundario de un transformador de instrumento, su dimensional se expresa en voltio amperios, no obstante, también puede expresarse en Ohms.

2.1.6.1.4. Transformadores de corriente

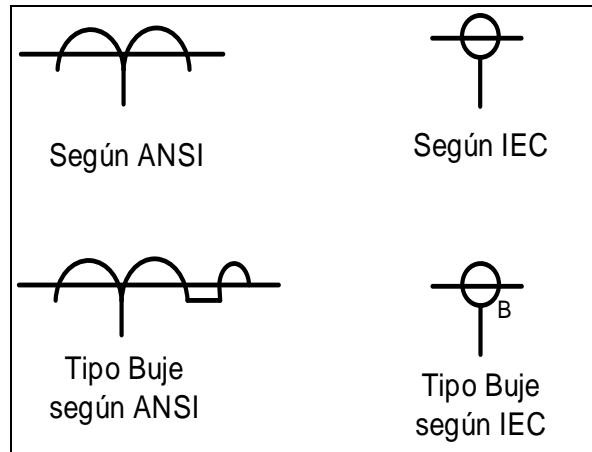
Estos elementos en las subestaciones son de suma importancia, principalmente porque cumplen la función de entregar magnitudes de corriente a los circuitos de protección, control y medida, que son los encargados de verificar que diversas funciones que dependen de la corriente, estén en correcto estado antes de enviar una señal de disparo o indicar una medida fuera del rango de operación aceptable respectivamente.

Los transformadores de corriente se instalan en serie con el elemento del circuito de alta tensión. Se denominan CT por su significado en inglés Current Transformers o TC por su abreviación en español.

Los TC Reducen los valores elevados de corriente a niveles medibles para equipos de protección, control y medida, los valores recomendados por la norma IEC son de un (1), Amperio, dos (2), o bien, de cinco (5) Amperios, dependiendo el valor de corriente depende de la aplicación que se quiera implementar, el valor normalizado por ANSI es de 5A.

La simbología para representar a los transformadores de corriente se muestra en la siguiente figura.

Figura 14. **Simbología para transformadores de corriente**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

En el aspecto constructivo, los transformadores de corriente pueden fabricarse con diversa cantidad de devanados para montarse en el núcleo secundario de manera que estos puedan ser independientes, de manera que todo el devanado primario enlaza todos los núcleos secundarios. El otro tipo es el secundario de relación múltiple o multi-relación, en estos elementos la relación de transformación del secundario se realiza por medio de *taps*.

Para TC's los valores comunes de operación se pueden definir de acuerdo con las siguientes normas:

- IEC 60044-1, los valores son: 10-12.5-15-20-25-30-40-50-60-75 Amperios y sus múltiplos decimales, los valores más comunes para elección son los subrayados.
- IEEE Std. C57.13, los valores son: 10-15-25-40-50-75-100-200-300-400-800-1200-1600-2000-3000-4000-5000-6000-8000-12000 Amperios.

Las guías actualizadas para la aplicación son la IEC TR 61869-100 y la C37.110, son para uso en protecciones.

En la siguiente tabla se muestran valores de la relación para una o dos relaciones según ANSI.

Tabla IV. **Valores de relaciones para transformadores de corriente según ANSI**

Relación sencilla	Doble relación en devanados primarios combinación serie-paralelo	Doble relación con derivaciones en el secundario
10:5	25x50:5	25/50:5
15:5	50x100:5	50/100:5
25:5	100x200:5	100/200:5
40:5	200x400:5	200/400:5
50:5	400x800:5	300/600:5
75:5	600x1200:5	400/800:5
100:5	1000x2000:5	600/1200:5
200:5	2000x4000:5	1000/2000:5
300:5		1500/3000:5
400:5		2000/4000:5
600:5		
800:5		
1200:5		
1500:5		
2000:5		
3000:5		
4000:5		
5000:5		
6000:5		
8000:5		
12000:5		

Fuente: RAMIREZ, Carlos Felipe. *Subestaciones de alta y extra alta tensión*. p. 281.

Las relaciones pueden variarse en el devanado primario o bien en el devanado secundario, y se expresan con el uso de los signos “x” o de la “/”, no obstante, el criterio de utilizar los signos queda a criterio de cada fabricante.

Con base en lo anterior, la relación del transformador (RTC), de corriente se define como:

$$RTC = \frac{I_p}{I_s}$$

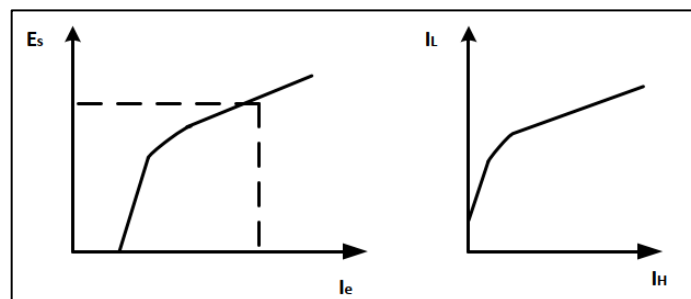
Donde:

I_p puede ser la corriente primaria, empero, no siempre lo es y dependerá del dimensionamiento del transformador de corriente.

I_s es la del secundario, el denominador es la corriente secundaria nominal, normalmente 1 A o 5 A.

Los transformadores de corriente cuentan con núcleo ferromagnético, en efecto se tendrá saturación y se presentan curvas de operación similares a las mostradas en la figura 15.

Figura 15. **Curva de saturación del transformador de corriente**

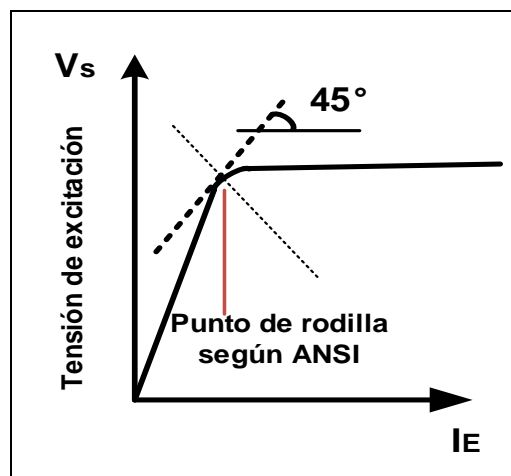


Fuente: elaboración propia, empleando Microsoft Visio 2016.

Donde se puede tener un punto de inflexión o punto de rodilla (Knee Point), que es punto de intersección entre dos rectas en un gráfico logarítmico, el valor de corriente de excitación se puede llevar hasta el máximo que va a depender del nivel de burden que se le instala.

Cuando más elevado es el valor del burden durante una falla, mucho más rápido se satura el CT.

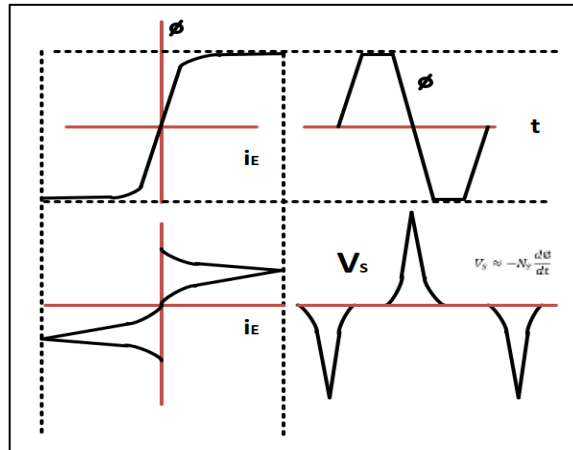
Figura 16. **Gráfica del punto rodilla según norma ANSI**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

El problema de la saturación en los transformadores, es que se crean picos en la corriente de excitación que generan picos en el voltaje de saturación dada la curva que se forma en la onda de flujo magnético (como se ve en la figura 17), y estos pueden causar problemas en el sistema de potencia.

Figura 17. **Forma de onda para el flujo magnético**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

La saturación también puede ocasionar problemas en los CT cuya principal función es la de exactitud para equipos de medición. Para efectos de protección la saturación puede ocasionar que los relevadores no actúen dada la saturación.

La clasificación de los transformadores de corriente se basa en los siguientes criterios:

- Transformadores de corriente de medición

En este tipo de CT se implementa en los diversos circuitos de las bahías de las subestaciones y su función principal será la medición de la magnitud de la corriente que pasa a través de dichos circuitos para que diversos dispositivos como son los medidores multifuncionales puedan tomar los valores de corriente y verificar la calidad de energía. La exactitud es el factor principal en este tipo de CT; es importante considerar la clase de exactitud como el máximo error de intensidad admisible para la clase de exactitud especificada a la corriente

nominal, este tipo requiere obtener de la manera más precisa la magnitud y ángulo de fase que corresponden directamente a la corriente. Sin embargo, la precisión no debe sobrepasar entre el 10 % al 20 % de la magnitud en valor nominal, considerando dentro de este valor cualquier exceso de corriente con el que sea posible percibirlo.

- Transformadores de corriente de protección

Para este tipo de CT, la función principal es proteger un circuito, por ello la exigencia de precisión no es tan notoria como el caso de los transformadores de medición, es necesario conservar un valor no mayor a veinte veces de lo que representa y abarca la magnitud de la corriente nominal.

2.1.6.1.5. Transformadores de tensión

Estos equipos tienen la finalidad de bajar el nivel de tensión y crear un aislamiento entre el circuito primario y secundario. La tensión secundaria, dentro de las condiciones normales de operación, es proporcional a la tensión primaria, aunque ligeramente desfasada.

Los tipos de transformadores pueden ser los siguientes: capacitivos, de tipo divisores capacitivos, inductivos, también del tipo divisores resistivos y divisores mixtos. Los más económicos por sus características constructivas son los transformadores capacitivos.

Para escoger la potencia nominal de un transformador, se suman las potencias que consumen las bobinas de todos los aparatos conectados en paralelo con el devanado secundario, más las pérdidas por efecto de las caídas de tensión que se producen en los cables de alimentación.

2.1.6.1.6. Clases de precisión para protección

Para el caso de los transformadores de protección, es importante tomar en cuenta la tensión asignada, que no debe superar el 5 %, para los devanados de protección es importante mencionar que la letra “P” para la nomenclatura representa el factor de tensión que se le asigna, y no debe sobrepasar la carga nominal.

Las clases normalizadas de acuerdo con norma IEC son 3 P y 6P, los que conllevan límites de error de tensión y desfase se presentan a continuación:

Tabla V. Clase de precisión para PT según norma IEC

Clases de precisión	Error en la relación de tensión (en porcentaje)	Desfase (min)
3P	± 3.0	± 120
6P	± 6.0	± 240

Fuente: RAMIREZ, Carlos Felipe. *Subestaciones de alta y extra alta tensión*. p. 276.

2.1.6.2. Nivel de automatización (nivel 1)

Esta parte de la arquitectura de las subestaciones está conformada por los IED, siendo todos los dispositivos de control y protección que interactúan con los equipos del nivel 0 o de patio. Es la parte inteligente y lógica de la subestación.

- Descripción de IED

En términos generales, IED por sus siglas en inglés Intelligent Electronic Device, se le denomina a cualquier dispositivo que incluye dentro de su estructura uno o varios microprocesadores capaces de recibir/enviar datos hacia o desde otro elemento, y los IED que se utilizan en las subestaciones son los siguientes:

2.1.6.2.1. Relevadores de protección

Uno de los elementos de mayor importancia, con respecto a la protección de los sistemas eléctricos.

- Relevadores funcionales

Los relevadores relés digitales, son elementos que se aceptan entradas y las procesan utilizando algoritmos lógicos para generar señales de salidas que van direccionadas para tomar decisiones respecto a disparos y así generar acciones en equipos primarios o bien, para generar diversos tipos de alarmas, cumpliendo así con funciones de protección para los elementos de la subestación respecto fallas generadas en el sistema eléctrico de potencia y evitando que el efecto de dichas fallas afecte a más elementos en la red eléctrica, estos elementos están basados en microprocesadores.

También se cumple con funciones de control y monitoreo, por tal motivo, son conocidos como relevadores multifuncionales, haciendo posible reducir costos totales de activos al momento de cuantificar elementos de la subestación.

Entre sus ventajas más relevantes se encuentran las siguientes:

- Multifuncionalidad, para este se agregan:
 - Protección y control
 - Medición
 - Registro de falas
 - Capacidad de comunicación
 - Compatibilidad con los sistemas digitales integrados
 - Alta confiabilidad
 - Auto verificación

- Diseño de los relevadores de protección

El sistema de protección conformado por relevadores consta de varios elementos que con su aporte proporcionan la protección a cierta zona de la subestación y dicho sistema se compone de los siguientes equipos:

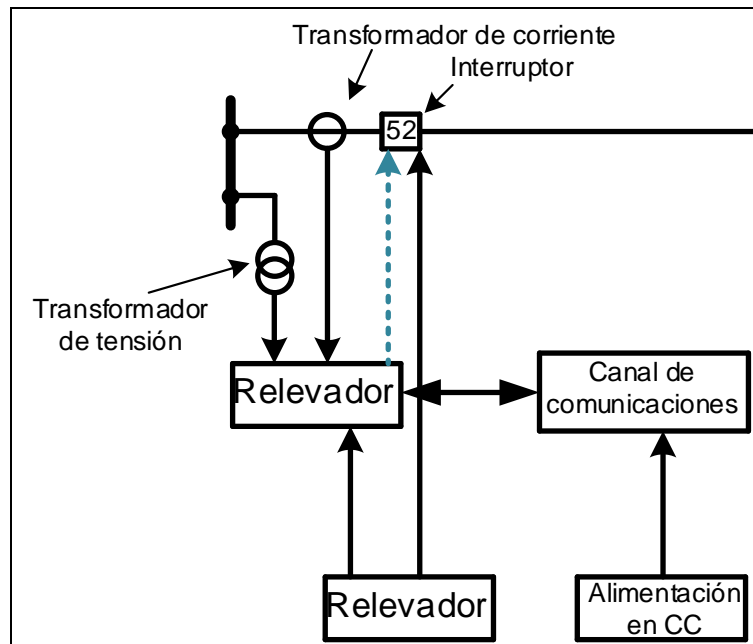
- Los transformadores de instrumentos

- El interruptor de potencia

- Los servicios auxiliares cumplen una función esencial al suministrar la alimentación en VDC a los equipos de protección y a muchos equipos de control y medición en la subestación.

- El canal de comunicación es importante para que los equipos de protección se comuniquen entre sí y también puedan reportar estampa de tiempo para diversos eventos que ocurran en el sistema o bien, enviar cualquier tipo de información a los controladores de bahía o enviar directamente hacia la RTU.

Figura 18. **Esquema de funcionalidades de los relevadores de protección**



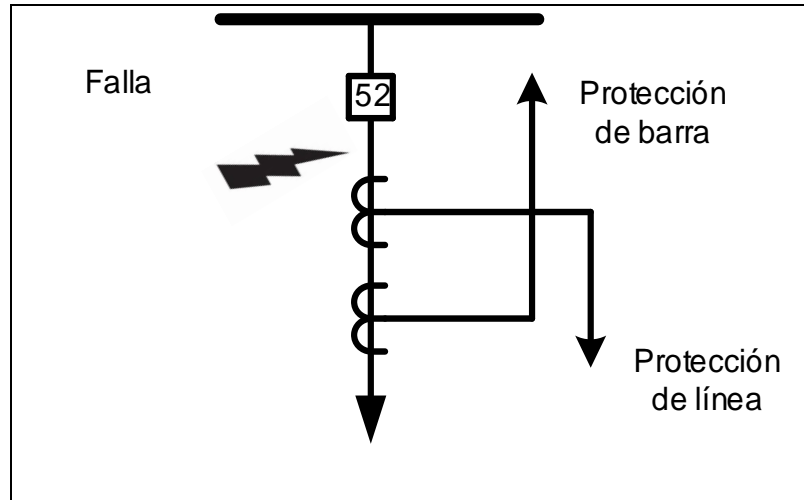
Fuente: elaboración propia, empleando Microsoft Visio 2016.

A partir de la función de cada elemento es necesario definir la importancia de las zonas de protección:

- Zonas de protección

Las zonas de protección son definidas por los transformadores de corriente. Idealmente las zonas de protección deben superponerse, de manera que ningún área del sistema de potencia quede desprotegida o como bien se conoce “zonas muertas”. Idealmente esto se logra colocar dos transformadores de corriente por cada interruptor, ahora bien, por temas de costos la implementación de ambos CTs no siempre se realiza.

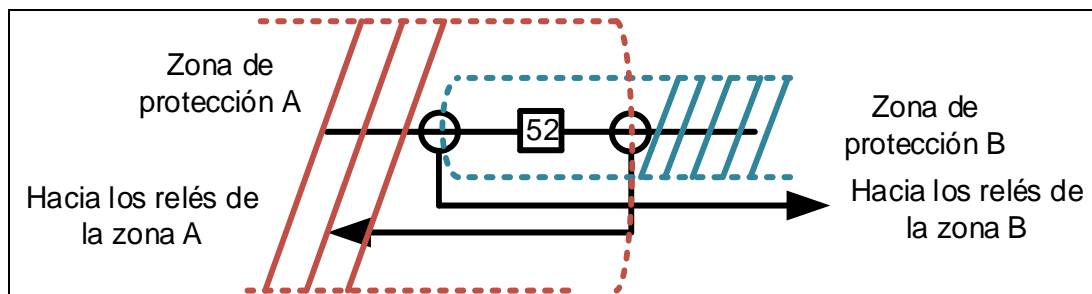
Figura 19. **Zonas de protección de una subestación**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Para esta implementación es necesario contar con transformadores de corriente de varios núcleos, el núcleo más alejado se utiliza para proteger la barra y el más cercano es para proteger una línea de transmisión según lo que aplique.

Figura 20. **Zonas de protección definidas por los CTs**



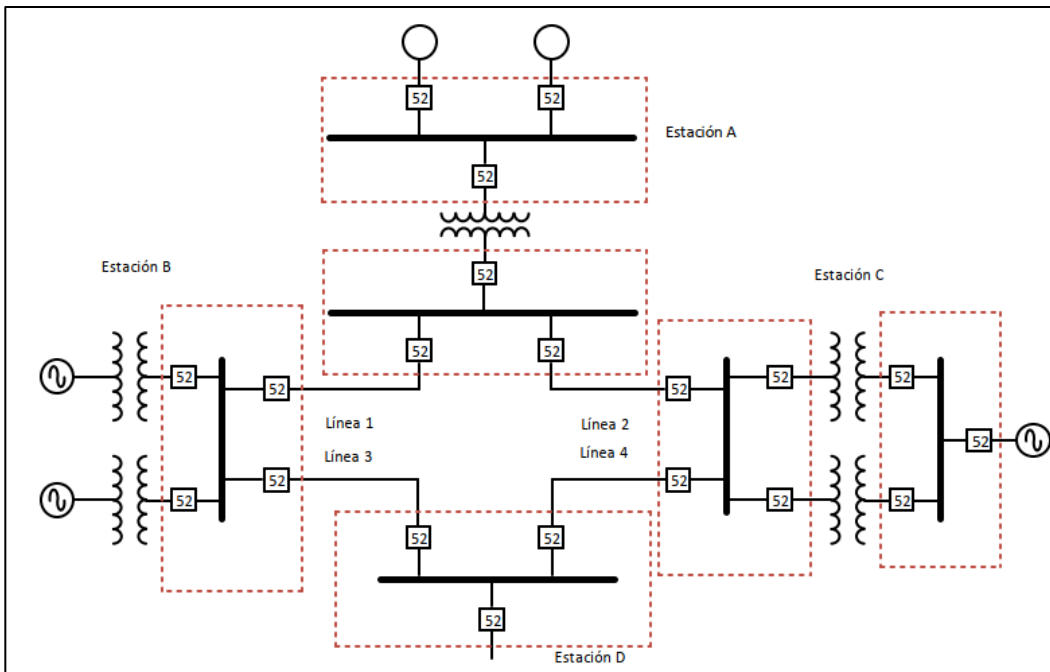
Fuente: elaboración propia, empleando Microsoft Visio 2016.

Las zonas de protección se pueden implementar para los siguientes elementos:

- Barras colectoras
- Líneas de transmisión
- Elementos independientes como: transformadores, generadores, motores

Como se muestra en la siguiente figura:

Figura 21. **Zonas de protección definidas para un sistema completo**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Los relevadores de protección son instalados en tableros que se fabrican para la protección, control y medida, los cuales son instalados dentro de la caseta de control de la subestación.

Las principales marcas en el mercado para los relevadores de protección son: SIEMENS, SEL, ABB y GE.

Figura 22. Relevadores marca SIEMENS y SEL



Fuente: SEL-411L. *Instruction manual*. p. 1.

- Arquitectura de los relevadores digitales

Se conforma de los siguientes elementos:

- Subsistema de entrada analógica: se convierten de señales de voltaje y corriente continuas a señales de voltaje y corriente con valores discretos por medio de filtros, que pasan a trabajar con base en 0 y 1.
- Subsistema de entrada discreta: son las entradas digitales; pueden tener únicamente dos valores, 0 o 1 (activas o inactivas), algunos ejemplos de estas son; la posición de interruptor, funciones de protección como 50 BF, funciones y señales de control como la posición de seccionadores, alarmas, posiciones de MCBs.

- Subsistema de salida discreta: son salidas digitales que se utilizan para disparos y alarmas.
- Puertos de comunicación: son los encargados de transmitir información por medio de protocolos de comunicación que puede manejar el relevador, estos protocolos de comunicación tienen diferentes niveles de seguridad para el acceso a la información, que se analizarán posteriormente.
 - Memorias que contienen los relevadores
 - Memoria de acceso aleatorio (RAM): es la que almacena toda la información que entra al equipo.
 - Memorias de lectura (ROM/PROM): tienen todos los algoritmos de protección.
 - Memorias de lectura/escritura (EPROM): es la que da los parámetros de ajustes de protección, guardan todos los ajustes que se realizan.
- Algoritmo de los relevadores de protección

Los algoritmos como el conjunto de operaciones que representan un procedimiento para realizar un cálculo y darle solución a un problema, son adaptados en los relevadores de protección para resolver problemas asociados a sobrecorrientes, fallas de impedancia en las líneas de transmisión, valores incrementales, onda viajera, entre otros.

- Funciones de protección

Los relevadores como equipos de protección tienen diversas funciones, estas se mencionan y se colocan el número; este se identifica con la norma ANSI/IEEE C37.2-2008.

Los diferentes tipos de relevadores son los siguientes:

- Relevadores diferenciales, pueden ser de línea o de barra
- Relevadores que trabajan con impedancia, son los de distancia
- Relevadores de sobrecorriente

2.1.6.2.2. Registrador de fallas

El registrador de fallas forma parte de las funciones propias de los relevadores de protección, incluyendo una memoria para guardar los eventos de forma segura y con ello garantizar el registro de las fallas que ocurren en los elementos del sistema protegidos (pueden ser líneas de transmisión, barras, transformador) y también se registra la acción de los relevadores ante las fallas.

Información que almacena un registro:

- Valores de las muestras que se generan de las señales analógicas.
- Valores que se calculan internamente en el dispositivo a partir de los valores medidos.
- Señales binarias, que se envían para realizar disparos a equipos primarios.

2.1.6.2.3. Controlador de bahía

El controlador de bahía, es un IED, las características principales es contener una pantalla para la visualización (también llamado unidad de control de bahía o computadora de bahía) está conformado por un hardware (módulo electrónico); también contiene para las funciones inteligentes un software (programación y bases de datos) configurado para permitir la implementación de varias funciones de control, como:

- Control y seguimiento de los equipos de patio de *switches*
- Gestionar lógicas de enclavamiento
- Mostrar señales de alarma
- Registro y visualización de información de eventos
- Interfaz con relés de protección
- Comprobación de sincronismo para el funcionamiento del disyuntor
- Funciones de medición
- Interfaz con instalaciones de control aguas arriba

Actualmente los fabricantes de estos equipos incluyen dentro de sus características, la facultada de tener algunas funciones de protección.

Se traslada lo que se tiene en el nivel de patio y se traslada al nivel 1, todos los controladores de bahía cuentan con su mímico, se cuenta con enclavamientos, que dependiendo de la configuración que se le otorgue al controlador, se puede realizar mandos desde el dispositivo, eso significa que se tiene control sobre los equipos de maniobra, y por este motivo es tema de interés para la ciberseguridad.

Como desde el controlador de bahía podría producirse un disparo no deseado de interruptor, es decir controlando a este IED se tienen control sobre una bahía completa. Es importante mencionar que muchos relevadores de protección tienen implementado por los fabricantes la opción de controlador de bahía, en efecto es común encontrar en una subestación un relevador que además de sus funciones de protección específicas, actúe con su interfaz como controlador de bahía.

2.1.6.2.4. Equipos de medición

Es un IED importante en la subestación como dado que se utiliza en los puntos de frontera que son importante para las empresas les permite facturar.

Los medidores de energía cada vez toman más importancia en los sistemas eléctricos de potencia, es importante como dado que de estos dependen los ingresos económicos de toda la empresa eléctrica.

Actualmente tienen mucha influencia los equipos de medida fasorial, que se utilizan en generadores y bahías; estos visualizan a futuro el comportamiento del sistema.

Por lo general, el equipo de medición digital consta de un transductor digital trifásico que acepta señales de los secundarios VT y CT y es capaz de calcular digitalmente voltios trifásicos, corrientes trifásicas, vatios sumados trifásicos y vars y frecuencia sumados trifásicos.

La salida del equipo de medición digital se realiza normalmente a través de un puerto de comunicación, como RS232 o Ethernet.

2.1.6.2.5. Equipos de monitoreo

La gestión de activos es un aspecto importante, siempre se ha requerido el monitoreo de la subestación tanto para la operación.

Actualmente es necesario un equipo de monitoreo conformado por dispositivos cuya funcionalidad es ser herramientas para prevenir fallas en el sistema, desde aspectos físicos como seguridad, deterioro de equipos y el correcto estado de los equipos que protegen la funcionalidad en la subestación. Ejemplos abarcan desde varios ámbitos, como son las cámaras de video vigilancia, monitores de descargas parciales en GIS, entre otros.

2.1.6.3. Nivel de control de la subestación (nivel 2)

En este nivel se realizan las labores de operación y monitoreo de las bahías de la subestación a través de los operadores quienes se encargan de ordenar las maniobras.

2.1.6.3.1. *Switch* de comunicación

Estos elementos son los que permiten la comunicación entre los dispositivos que conforman una red de área local por sus siglas en inglés LAN. Permite interconectar los IEDs que se tengan en la subestación, permitiendo su comunicación, y este intercambio de datos entre equipos lo hace dentro de la misma red sin afectar a ningún elemento dentro de esta.

Figura 23. **Switch de comunicación**



Fuente: SIEMENS. *RUGGEDCOM rack-mount switches*.

<https://new.siemens.com/global/en/products/automation/industrial-communication/rugged-communications/ruggedcom-portfolio/ethernet-layer2-switches/rack-switches.html>. Consulta: 29 de septiembre de 2021.

En la 802.3 es posible encontrar información importante para la finalidad de los *switches* respecto al buen funcionamiento y características para el dimensionamiento de los mismos, siendo uno de los principales objetivos determinar la velocidad de los puertos, y el medio por el cual se transmitirán los datos, los más importantes son el estándar 802.3 y el 802.3u, para Ethernet de cobre y la 802.3z/ab para fibra óptica.

Los *switch* para una red LAN operan en la capa de enlace o capa 2 del modelo OSI; se encuentra entre la capa física y la capa de red que corresponde al enrutamiento y direccionamiento lógico, es por ello que La capa 2 mediante la dirección MAC correspondiente a cada equipo permite el direccionamiento de los paquetes.

Los *switches* son muy versátiles dada su estructura de hardware y se encuentran de diferentes cantidades de puertos necesarios para cumplir diversas funciones, existen de cuatro puertos con funciones básicas, pero también se pueden encontrar *switches* con cientos de puertos que pueden incluir diversos

tipos de protocolos de comunicación y tipo de puerto. El medio de transmisión para los datos se da en cobre y en fibra óptica.

Es importante aclarar que un *switch* no es capaz de tener la particularidad de conectar redes entre sí y tampoco brindar una conexión a internet, estas funciones son exclusivas del *router*, en el caso estos dos equipos se integran en el mismo dispositivo conocido como *switch* de capa 3, cuyas bondades ofrecen funciones centralizadas.

Tipos de *switches*:

- *Switch* no administrables

Son un tipo de *switch* de Ethernet Plug and Play, los usuarios los conectan y esperan a que funcione por cuanto estos dispositivos no requieren de configuración manual, en efecto son menos sofisticados que los *switch* administrables, incluso este tipo de equipo se utiliza para aplicaciones rápidas en campo, tomando en cuenta que tienen algunas funciones simplificadas como:

- Solo pueden utilizarse en redes simples
 - No poseen la opción de configuración de usuario
 - Envía los datos deseados al dispositivo deseado
 - Utilizados en grupos de trabajo dentro de una red
- *Switch* administrables

Es el tipo de *switch* capaz de brindar las capacidades más completas para la red, estos se utilizan en la capa central de la red, principalmente para

centros de datos complejos, brindan mejor control y funciones avanzadas sobre el tráfico de LAN.

La configuración disponible para los dispositivos administrables es:

- El protocolo simple de administración de red (SNMP), permite el registro de eventos a través de bases de información de administración (MIB).
- Configuración a través de la interfaz de línea de comandos, Telnet o interfaz web.
- Puerto habilitado, monitorización de puertos (por *Mirroring*).
- Filtrado de direcciones MAC, *Spanning Tree Protocol*.
- Configuración de redes de área local virtual (VLAN) IEEE 802.1Q y priorización de tráfico IEEE 802.1p.
- Gestión de direcciones IP (enrutamiento).
- Enrutamiento QoS.
- Calidad de servicio, lo que quiere decir que da prioridad a mensajes GOOSE por cuanto puede ser una señal de disparo.
- Seguridad IEEE 802.1X.
- Entrega de datos Ethernet determinístico y predecible.

- Automatización utilizando estándar IEC 61850.

Para la configuración de los *switches* son necesarios dos métodos los cuales es contar con un puerto para la misma configuración, o bien, por un acceso desde la red como servicio web, ambos son características propias que debe tener el dispositivo. Por el puerto es necesario conectarse mediante una computadora desde un cable con el tipo de conector adecuado y que tenga instalado el software propio del *switch*.

Para hacer uso del servicio web, es necesario utilizar un puerto Ethernet para poder realizar alguna configuración haciendo uso de la dirección IP.

El *switch* administrable se divide en los siguientes tipos:

- *Switch* inteligente: es un *switch* administrable cuyas capacidades de administración son limitadas. Sus características hacen posible ingresar al campo administrativo y no administrativo. En cuanto a costos, en el mercado se encuentran con precios mucho más accesibles que cualquier otro tipo, en este caso se tiene un acceso a interfaz web limitado desde el punto de vista de seguridad, sus configuraciones básicas incluyen el uso de VLAN, ancho de banda de puerto y dúplex.

Switches empresariales: este tipo se enfoca en tener otro tipo de funciones como son las personalizadas en comparación con los del tipo inteligente. Su aplicación se dirige a las capacidades de administración y este dispositivo puede centralizar la información proveniente de distintos concentradores de datos y conexiones. Algunas funciones incluyen la lista de control de acceso, interfaz web y protocolos de seguridad como el

SNMP y características de operación abierta con capacidad de restaurar configuraciones anteriores.

- *Switches* de nivel 3

Un *switch* de nivel correspondiente a la capa 3 es diseñado para poseer todas las funciones y características de un *switch* de capa 2 pero también proporciona funciones de enrutamiento IP contenidas en la capa 3. Esta función particular para operar en diferentes VLAN derivadas de diversos *switches* de capa 2 y que requieran comunicar algunas de sus redes LAN virtuales, adicional a que tienen funciones básicas de enrutamiento para direccionar las VLANs. Es compatible con todas las funciones de conmutación y son más rápidos que los *routers*, un *switch* de capa 3 puede considerarse como un *router* con múltiples puertos Ethernet más la función de conmutación y se puede configurar para soportar protocolos de enrutamiento como RIP e EIGRP, pero carecen de algunas funcionalidades sofisticadas de los *routers*.

La elección de implementación entre un *switch* y un *router* eventualmente puede ser un dilema, dada la demanda de comunicación dentro de manera segura entre redes, donde existe un tráfico considerable y diversas direcciones para múltiples dispositivos y por ello es necesario gestionar funciones de administración de direcciones MAC en todas las redes. Por lo tanto, la aplicación del dispositivo para la tercera capa del modelo OSI, se aplica en las siguientes condiciones:

- Para la implementación en zonas las cuales deben tener sus dominios de difusión por separado.

- En caso se requiera sustituir un *router* y agregar conexiones del tipo Ethernet donde su aplicación sea funcionar como interfaces a un servidor.
- Para la interconexión de diversas zonas a través de los circuitos en la capa 2, proporciona la facilidad de configurar enrutamiento y enlace con la capa 3 del modelo OSI.
- Para tener un alto porcentaje de la correcta transferencia de datos y la interacción entre VLANs.
- Para una red con muchas emisiones que necesitan VLANs de mejor rendimiento.
- Alcances de una red local.

La existencia de la red local permite:

- Para archivos y datos, todos los equipos pueden acceder a la información que al menos un equipo haya enviado en la red, haciendo posible que se compartan entre todos los dispositivos conectados.
- Compartir interconexión con periféricos como impresoras, monitores, cámaras y proyectores. Todos los equipos de la red pueden utilizar los mismos periféricos. Para dar una definición de los periféricos, son los dispositivos que cuentan con interface para tener interconexión con un puerto del CPU, haciendo posible agregar funciones adicionales al sistema, formando parte del

hardware para toda la operación que hace posible el conjunto de equipos.

- Es posible compartir conexión por varias vías a internet. Esto es posible a través de *router*, que distribuye señal a todo dispositivo que se conecte por conexión de cobre o inalámbrica.
- Características básicas de los *switches*
 - Puertos de comunicación

La parte de hardware más importante de estos equipos que logran la interoperabilidad entre dispositivos son los puertos o sea toda interfaz capaz de conectar ambos por un medio. La cantidad de puertos que se pueden admitir varía entre *switches* con un mínimo de cuatro puertos hasta *switches* del tipo troncal cuya característica es tener capacidad para cientos de puertos.

El tipo de puerto es una característica a tomar en cuenta en la elección del dispositivo, por cuanto el tipo de conector para el cableado es importante, el cableado que acepta protocolo Ethernet es par trenzado y fibra óptica, para puertos de cable de par trenzado y para este caso el conector común es el RJ-45 y del que es propio para cable UTP trenzado de 4 pares y para *switches* de mayor dimensiones incluyen puertos de fibra óptica donde el conector más frecuente pero no los únicos son del tipo SC y LC, otros menos utilizados son ST, MTRJ y micro-D.

Ethernet como protocolo de comunicación tiene la particularidad de permitir varias velocidades, que para el caso de los puertos una característica a considerar es la velocidad a la que pueden enviar paquetes de datos en un medio

de transmisión, los puertos más comunes en cobre van desde 10/100; son los que funcionan bajo los estándares 10BASE-T y 100BASE-TX para 100 Mbps.

La solución de 10/100/1000, es el mismo que el anterior, pero con 1000BASE-T. Para puertos de fibra óptica pueden implementarse los puertos de 100BASE-FX y 1000BASE-X.

- Power Over Ethernet

La alimentación eléctrica por Ethernet, a la que se le conoce como PoE lo que significa Power Over Ethernet, es la tecnología que permite el envío de alimentación eléctrica en conjunto con los datos en el cableado de una red Ethernet a dispositivos conectados en la misma, lo que permite ahorrar la instalación de infraestructura de cableado para la alimentación de los mismos. Es una tecnología similar al USB permitiendo el envío de datos cliente-*switch* y la alimentación la realiza directamente por el cable UTP.

Se basa en los siguientes estándares:

- IEEE 802.3af: PoE con alimentación de hasta 15.4 W
- IEEE 802.3at: PoE+: aumenta la capacidad de potencia hasta 30W.
- 3bt: uPoE con un rango que llega hasta los 51W o 71W dependiendo de la aplicación.

La capacidad de alimentación es importante para crear puntos de acceso a la zona Wi-Fi y dispositivos con su respectiva IP en subestaciones.

- La conmutación

Uno de los temas esenciales para entender la funcionalidad de los *switches* de comunicación y sus puntos vulnerables y donde se debe reforzar el tema de ciberseguridad en este tipo de tecnología OT, es entender cómo se transfieren los datos entre todos los elementos conectados.

Si es necesario referir a un *switch* en español, se denomina conmutador, se le llama de esta manera dada la funcionalidad que posee sobre el estándar Ethernet, por cuanto la transmisión de datos se realiza a través de tramas que llevan en la red los datos con la conocida cabecera lo que hace posible identificar tanto emisor como receptor mediante la dirección MAC y esta dirección es contenida dentro de la cabecera.

La trama de Ethernet es la principal responsable de controlar transmisión correcta y exitosa de los paquetes de *data*.

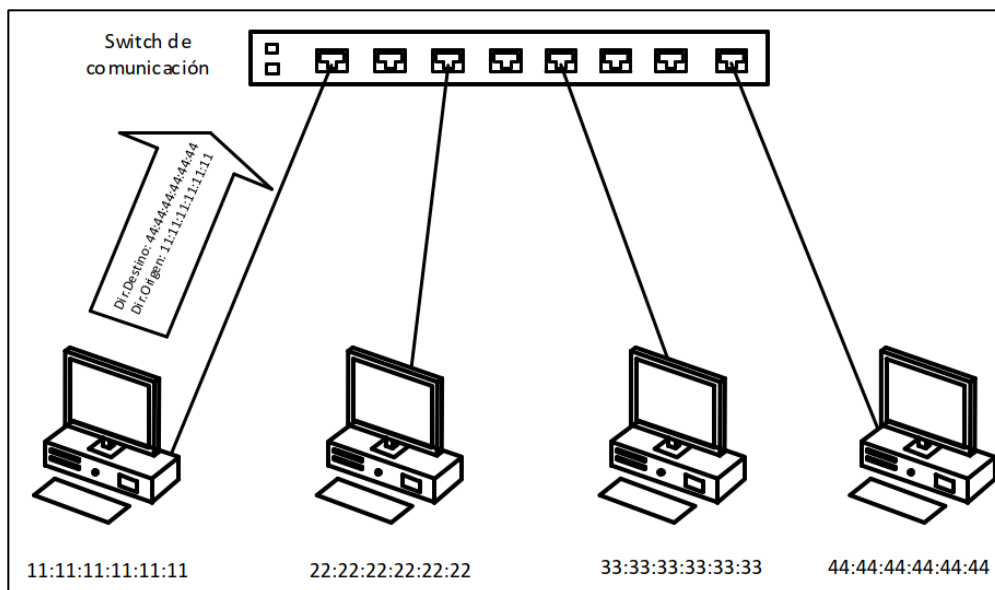
El paquete siempre comienza con un preámbulo, que controla la sincronización entre el transmisor y el receptor, y un Delimitador de trama de inicio (SFD), que define la trama. Las dos piezas de información son una secuencia de *bits* en el formato 10101010, la trama real tiene en el correspondiente formato MAC los datos de destino, y su origen, para ello también se cuenta con datos de control, seguido de toda la *data* a transmitir. Una secuencia de verificación de cuadros (FCS), cierra el cuadro completo (excepto el preámbulo y el SFD), como una suma de control. El paquete se termina con un momento de reposo conocido como Inter Frame Gap, estableciendo una pausa de transmisión de aproximadamente 9.6 μ s.

La dirección MAC como su denominación lo indica es la identificación asignada a la interfaz de red física que corresponde a cada dispositivo que se encuentra conectado desde cualquier punto de acceso a la red hasta el *router*.

La dirección MAC obedece cierta longitud de dígitos hexadecimales conformada por 48 *bits*.

Los *switches* guardan en memoria interna una tabla que contiene las direcciones MAC que interactúan en la red a la que se conectan colocando también como información importante los puertos que se habilitan, y cuando una trama se hace llegar al *switch*, se envía inmediatamente al puerto de destino. El IED envía la trama hacia el *switch* y dado que el *switch* no conoce el puerto de destino, la envía a todos los dispositivos conectados, pero aprende la dirección del puerto emisor, cuando el puerto receptor responde al puerto emisor, el *switch* conoce el puerto donde está y lo envía solo a ese puerto y aprende la dirección "MAC" del equipo receptor. De esta manera se completará la tabla.

Figura 24. **Conmutación en un *switch* de comunicación**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

- Importancia de *buffers*

Un elemento fundamental para que se realice la conmutación de manera efectiva son los *buffers*; son espacios de memoria que tienen como objetivo almacenar todas las tramas recibidas en el dispositivo para luego reenviarlas al puerto de destino, al mismo tiempo que la característica permite conectar puertos que trabajen a diferentes velocidades.

- Técnicas de conmutación

La transferencia de datos dentro de los diversos puertos de un mismo *switch* puede darse de la siguiente manera:

- Reenvío directo (cut-through). Consiste en que en un puerto al momento de recibir datos no se tiene tiempo de espera para leer la trama en su totalidad y la reenvía al puerto destino, siendo es una técnica que ayuda a optimizar tiempos para transmitir datos al puerto que corresponde.
- Almacenamiento y reenvío (Store and Forward). Su finalidad es verificar si es que existe error en el envío de los datos al puerto correcto de destino y funciona de manera que la trama es almacenada de manera total en el buffer.

2.1.6.3.2. Gateway

Un Gateway o puerta de enlace es el dispositivo encargado de transmitir toda la información proveniente de los dispositivos inteligentes de protección, control y medida del nivel 1 de la subestación. Las principales características de

estos dispositivos es que pueden manejar los protocolos serial RS232 y RS485 y Ethernet IEC 61850, Modbus.

Tienen punto de autenticación de seguridad los siguientes:

- Protocolo ligero de acceso a directorios (LDAP)
- Autenticación remota del servicio de usuario de marcación de entrada (RADIUS).
- *Whitelist* o *Blacklist*.
- Encriptación.

Es el elemento dentro de la comunicación de la subestación encargado de ser el enlace entre dos redes, estando dentro de una red permite el acceso hacia otra, ambas redes con protocolos y arquitecturas distintas, donde se traduce la información del protocolo en ejecución de una red al protocolo que se utiliza en la red de destino.

En términos de operaciones, un *Gateway* tiene la función de dar acceso en una sola conexión a dispositivos que forman parte de una red LAN, y se crea una sola dirección IP externa derivado de la capacidad de conversión de formato IP a NAT, esto permite crear un enmascaramiento de IP.

Un ordenador puede configurarse como Gateway desde una red LAN hacia una red exterior, pero para ello se debe contar con dos tarjetas configuradas. A los dispositivos de una red con la finalidad de direccionar de manera predeterminada paquetes de datos cuyo puerto de destino sea desconocido, es posible utilizar la puerta de enlace estableciendo una ruta por defecto.

Dadas las características del *Gateway* es posible obtener una capa adicional de seguridad en los puertos del equipo, porque cualquier puerto que reciba o envíe información como característica que es posible configurar, guarda toda la información como un registrador de eventos.

Para recopilar la información de los dispositivos esclavos en la red y garantizar la comunicación entre los equipos de nivel 1 y con el *Gateway* en el nivel 2 de la subestación y al mismo tiempo, permitir la comunicación entre nivel 2 y nivel 3 de SCADA, con frecuencia el *Gateway* se encarga de la traducción entre diversos protocolos como es el Ethernet, TCP/IP, DNP3.0, entre otros.

2.1.6.3.3. Unidad Terminal Remota (RTU)

Las unidades terminales remotas pueden efectuar las funciones de enlace y registro de eventos entre la subestación y el Centro de Control Remoto. Generalmente las RTU incluyen las siguientes funciones:

- Recolección de información de señales para la configuración de enclavamientos y funciones de automatización en equipos primarios de maniobra en las subestaciones.
- Diversidad de protocolos normalizados con diferentes IEDs para minimizar el cableado de control convencional y reducir costos para la comunicación. Normalmente en subestaciones con una arquitectura de comunicación sofisticada donde se encuentran muchas redes LAN, son los *switches* de comunicación quienes envían toda la información de los IEDs hacia la RTU.

- Factibilidad para la instalación de HMIs de trabajo que facilitan y mejoran la operación, visualización de eventos y medidas de la subestación.

Para obtener una HMI funcional el equipo debe tener como mínimo lo siguiente:

- Módulo de diversas entradas, estas son entradas binarias y analógicas
- Módulo de diversas salidas, estas son salidas binarias y analógicas
- Módulo de control como interfaz para los equipos de control dentro de la subestación.
- Módulo de unidad de procesamiento de información centralizada (CPU).
- Módulo de comunicaciones.
- Módulo de sincronización de tiempo (GPS).

Este es normalmente el hardware para las RTU, también existen software con las funcionalidades de las RTU para obtener todos los protocolos de comunicación y su configuración, y estas son vendidas como licencias que al final dicho software sea adaptado en computadoras industriales (CPUs), y se le puede agregar funcionalidades de HMI con otro tipo de licencia complementándola con una pantalla LCD.

Otras características son:

- Fácil configuración con el software
- Puertos adicionales y modularidad
- Seguridad programable-Niveles de acceso
- Fabricadas para funcionar como una RTU concentrada o una RTU distribuida.

Abarcan la funcionalidad de los *Gateway*, por cuanto las RTU han evolucionado y ampliando sus alcances de funciones con el mejoramiento de diversas tecnologías, en efecto al referirse a las RTU de subestaciones en alta tensión también se les conoce como concentradores de datos o *Gateway*.

Una unidad terminal remota tiene la capacidad de monitorear un número de entradas/salidas (I/O), relacionadas con un proceso, analizar y mantener datos en tiempo real, ejecutar algoritmos de control programados por el usuario, comunicarse con la estación maestra y en algunos casos, con otras remotas.

Contienen todos los elementos de la red supervisada, transmitiendo los datos necesarios de cada subestación a su Centro de Control y para la dirección inversa transmite comandos desde dicho Centro de Control de área hacia las subestaciones.

La RTU aprovecha la información y el cableado existente, posición de equipos, alarmas, medidas y comandos remotos, se minimiza la modificación de los sistemas de protección y control convencional existentes y se simplifica la instalación.

Para configuración del software algunas marcas utilizan Codesys o Phyton.

La RTU procesa toda la información proveniente de los dispositivos esclavos y mediante protocolo realiza el envío de la información hacia un centro de control remoto o también conocido como estación maestra, donde se encuentra el SCADA con su sala de control central. El medio por el cual es posible trasladar la información es diverso y puede ser por fibra óptica utilizando conmutación de etiquetas multiprotocolo conocido como MPLS, otro medio es por satélite, o también microondas.

El protocolo de comunicación utilizado se basa en las necesidades de seguridad y medios disponibles, tanto técnicos y económicos, y de esta manera establecer la estructura del mensaje que se define por los distintos fabricantes.

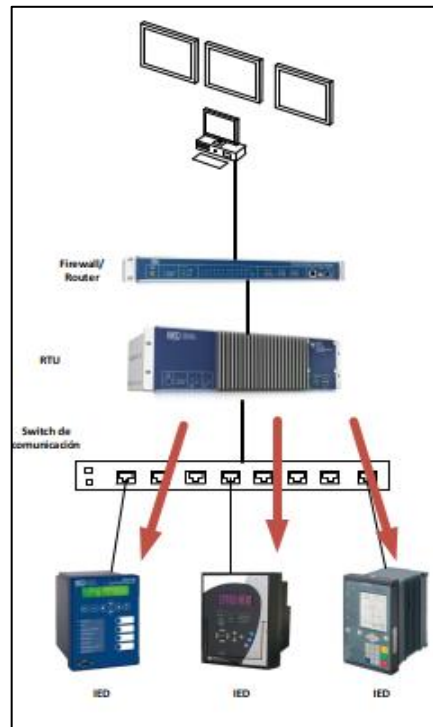
Entre la lógica de ingeniería para cumplir con las funcionalidades de las RTU se encuentran las siguientes:

- Protocolos para funcionar como servidor
- Protocolos como maestro
- Protocolos de comunicación punto a punto y entre pares
- Lógica de diagnóstico de ajustes
 - Para Web Browser
 - Para base de datos externa

- Protocolos de comunicación en RTU
- Protocolos como “cliente” necesarios en una RTU
- IEC 60870-5-104/103/101
- DNP3 serial /TCP
- Modbus serial/TCP
- Sincrofasores IEEE C37.118
- MMS del estándar 61850
- SNMP permite integrar *switch* de comunicación a la RTU y realizar gestión del mismo.

Donde les pide información a todos *switches* de comunicación, IEDS, transductores, medidores y todos los equipos conectados aguas abajo, como se muestra en la figura 25.

Figura 25. **Funcionalidad de la RTU aguas abajo**



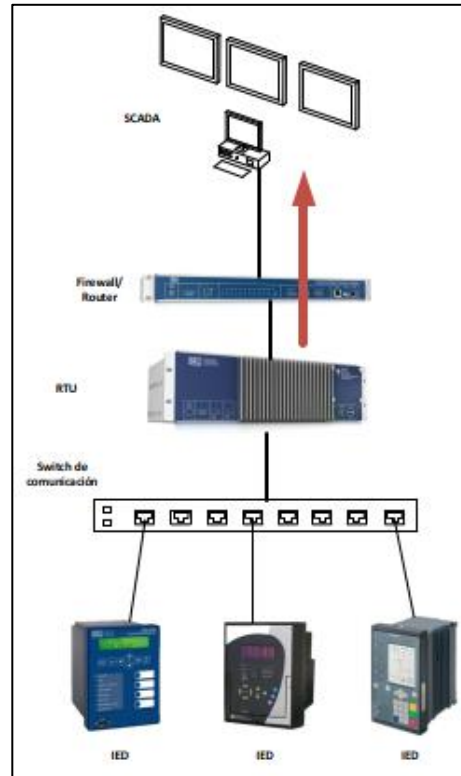
Fuente: elaboración propia, empleando Microsoft Visio 2016.

Protocolos como “servidor” necesarios en una RTU:

- IEC 60870-5-104/103/101
- DNP3 serial /TCP
- Modbus serial/TCP
- Sincrofasores IEEE C37.118
- MMS del estándar 61850

La RTU reporta toda la información que le es requerida por el equipo aguas arriba en la jerarquía de la comunicación, como se muestra en la figura 26.

Figura 26. **Funcionalidad de la RTU aguas arriba**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Otras funcionalidades:

En otras aplicaciones de RTU se puede configurar para que no funcione como cliente o servidor, y que posea una función de comunicación horizontal cuya función principal es que pueda apoyar en él la interacción con mensajes GOOSE, incluyendo para funcionalidades de protección y control, con funcionalidades específicas entre equipos de comunicaciones digitales con procesamiento rápido.

Otras aplicaciones que se le puede otorgar a estos equipos son la función de Port Server (Conversión de Serial a Ethernet), para la comunicación a grandes distancias, en donde se encuentran muchos IEDs que estén comunicándose por protocolo serial se conecten y reporten hacia la RTU de manera que ésta reúna toda la información y la envíe por medio de protocolo Ethernet hacia un equipo ubicado a gran distancia como puede ser un *switch* de comunicación.

Las RTU también son conversores de protocolos, por cuanto convierte todos los protocolos de los equipos aguas abajo, entiéndase IEDs y *switches* estos pueden ser DNP3, Modbus, IEEE 61850 y el resto ya mencionado anteriormente y enviar toda la información al Centro de Control en protocolo propicio para la comunicación entre niveles 2 y 3, es decir IEC-104 o DNP3.

También puede funcionar como procesador de sincrofasores; actualmente es una nueva funcionalidad para estos equipos.

Las RTU pueden funcionar como un mini SCADA con la implementación de una HMI donde se pueden realizar funciones de control y monitoreo de la subestación que se encuentre en supervisión.

Con el avance inminente de la tecnología, dado que las RTUs son dispositivos que funcionan a partir de hardware con dispositivos de micro procesamiento, es posible utilizar diversos tipos de memoria como es la EEPROM y RAM, ambas con su correspondiente aplicación como memoria de solo lectura y como memoria de acceso directo respectivamente, haciendo posible velocidades de procesamiento de 16 o 32 GB, así como discos para almacenamiento de información de hasta 1 TB, permitiendo también hacer el uso de arreglos de discos redundantes para asegurar la información almacenada. Para resguardar las memorias también es posible el uso de batería de litio, o bien

la opción más recomendada es la implementación de memoria no volátil en estos equipos.

La CPU es la unidad controladora de todas las funciones de la unidad terminal remota, por cuanto dirige todas las transferencias de *data* entre los registros y las localidades de memoria, y controla las interrupciones de la interfaz de comunicación quien envía la *data* de la RTU a la MTU. EL microprocesador de la RTU contiene una serie de registros destinados a almacenamiento temporal de instrucciones, direcciones de memoria y resultados de ciertas operaciones.

El procesamiento y aplicación de las funciones de la RTU, se realiza por el software aplicable al dispositivo, este utiliza algoritmos e información contenidas en las memorias RAM y ROM, apoyadas por un reloj en tiempo real.

2.1.6.3.4. Human Machine Interface – HMI-

Una HMI consiste en un conjunto de piezas de hardware más un paquete de software de aplicaciones.

El hardware generalmente incluye:

- Monitores a color para pantallas de visualización que muestran los circuitos de energía de la subestación, así como los recursos de control y monitoreo.
- Teclado alfanumérico o con teclas de función para la interacción con las pantallas mostradas y un *mouse* o *trackball*.

- Impresora para producir copias en papel bajo demanda.
- Registrador de datos para la impresión continua de textos de eventos en orden cronológico.

En cuanto al software de la HMI, normalmente se emplean interfaces gráficas completas y programas de edición.

Las pantallas, que deben ser comprendidas fácilmente por el operador de la subestación y se desarrollan en estrecha cooperación entre el diseñador de SAS y el personal del propietario de la subestación, comprenden varias etapas clave, como las de las siguientes secciones:

- Pantalla de inicio

Es común que un cuadro de diálogo de entrada, solicite a los posibles usuarios que ingresen un nombre de usuario y una contraseña para evitar el acceso no autorizado a la operación del tablero.

- Pantalla de la caja principal

Esta es la primera pantalla que aparece después de iniciar sesión a través del cuadro de diálogo de entrada. Los botones que aparecen en esta pantalla incluyen los siguientes:

- Campos para información de datos y tiempo
- Ingreso a la lista de eventos
- Ingreso a la lista de alarmas
- Tecla de salida

- Pantalla de administrador de usuarios

Al hacer clic en el botón "Opciones" que se muestra en la pantalla del cuadro principal, aparecen varios botones secundarios que dan la opción de elegir otras pantallas requeridas, incluido un cuadro de "administrador de usuarios".

- Pantalla de circuito primario (pantalla de proceso)

Esta pantalla aparece como resultado de hacer clic en el botón respectivo en la pantalla del cuadro principal. Aparte del diagrama unifilar, los códigos de identificación de los aparatos primarios y los nombres de los alimentadores conectados, indica lo siguiente:

- Posiciones de selectores locales / remotos instalados en tableros de aparamenta y IED de control.
- Estado de toda la aparamenta instalada (abierta / cerrada).
- Valores de medidas en puntos relevantes del circuito primario.
- Medios para abrir cuadros de diálogo complementarios para funciones de control particulares, como el control del cambiador de tomas.

Características operativas:

El proceso de ingeniería a nivel HMI también cubre la definición y establecimiento de varios aspectos operativos, como:

- Supervisión del sistema: Se refiere a la definición de mecanismos adecuados para obtener un sistema autocontrolado, de modo que las

fallas sean avisadas inmediatamente al operador de la subestación antes de que se conviertan en situaciones graves.

- Servicios de copia de seguridad: se deben tomar las medidas necesarias para crear una copia de seguridad de los directorios de archivos contenidos en el sistema.

2.1.6.4. Nivel 3, nivel de estación (Centro de Control)

El Centro de Control está conformado por diversos elementos que permiten concentrar la información que es enviada de diversas subestaciones remotas, por lo que es posible el monitoreo y control remoto de diversas funcionalidades habilitadas para realizarse desde este punto, como son los disparos a interruptores de potencia, estos son posibles de realizar desde el Centro de Control siempre y cuando se cumpla con los requisitos de los niveles inferiores de mando.

En un Centro de Control se cuenta con diversas HMI que son monitoreadas por diversos operadores cuya función es verificar que diversas magnitudes del sistema, como la frecuencia, la tensión y la carga sean estables y estén en los rangos aceptables para la buena operación del sistema.

Composición de Centros de Control:

- Operadores de demanda: supervisan cargas y demandas de subestaciones.
- Operadores de transmisión: operan y coordinan las operaciones en líneas de transmisión.

- Operadores de generación e intercambio de áreas: operan despachos y garantizan intercambios de energía controlando el flujo que cada generador conectado puede proporcionar al sistema de potencia.
- Operadores de Control del Sistema: control y manejo de Centro de Control.

En los Centros de Control incluye diversas funcionalidades críticas operacionales y otras que son corporativas. Para implementar ciberseguridad lo más recomendable es que se definan correctamente las diversas zonas conformadas por hardware, principalmente servidores, que son destinados para cumplir con diversas funciones de ingeniería, accesos a sitios web de una red insegura, almacenamiento de gran cantidad de información, un control de acceso basado en roles para establecer límites de acceso a funciones operativas y de confidencialidad de información dependiendo las características que se configuren para los diversos usuarios.

Incluso debe analizarse la funcionalidad que se otorga a servidores cuyo objetivo será realizar funciones de autenticación remota de usuarios. Los *firewalls* son muy importantes para controlar toda la información que entrará al Centro de Control, previniendo cualquier tipo de *malware* que pretenda realizar perturbaciones al sistema del Centro de Control de manera que al momento de una contingencia no sea posible reaccionar para mitigar la falla y ocurran daños severos a elementos del sistema eléctrico de potencia a proteger.

Las VPNs de igual manera juegan un papel fundamental en las entradas de los Centros de Control para llegar a los sistemas de funciones periféricas del mismo, por cuanto son canales seguros donde se pueden utilizar protocolos de cifrado para que la información llegue segura desde las subestaciones remotas.

- SCADA

El elemento principal de este nivel de operación es el SCADA, una definición muy general es la siguiente:

El control de supervisión y la adquisición de datos (SCADA), es un tipo de ICS que recopila datos y monitorea la automatización en áreas geográficas que pueden estar a miles de kilómetros de distancia.

Y cuya función es monitorear y recopilar información de RTUs e IEDs, ubicados en subestaciones remotas, manteniendo el control y supervisión de datos de varias subestaciones del sistema eléctrico de potencia.

Las principales funciones de un SCADA son:

- Supervisión, control y adquisición de datos
- Procesamiento de datos
- Recopilación de secuencial de eventos
- Recopilación de oscilografías
- Sistema de información de históricos

La adquisición de datos se centra en lo siguiente:

- Analógicos, por ejemplo, valores de voltaje, corriente, potencia P y Q y factor de potencia.
- Digitales por ejemplo medición en BCD de la posición de *taps* en transformadores.

- Control de supervisión: agrupados mandos y enclavamientos de control.
- Etiquetado (Tagging).
- Trabajos de mantenimiento / alarmas y notificaciones.
- Procesamiento de topología (coloreo de feeder, Trazado de circuitos, Malla detección).
- Deslastre de carga por SCADA.
- Por prioridad o Round Robin.
- Capacidad Multi-Site: modificación temporal de administración y mandos y enclavamientos de control.
- Comandos de disparo, aperturas y cierres.
- Edición de Point & Click.
- Ejecución automática o paso a paso.

Las ventajas del sistema SCADA son:

- La procesadora puede almacenar múltiple tipo de información y capacidad amplificada para almacenar datos.

- Versatilidad para mostrar los datos en diversos formatos, dependiendo la necesidad de uso.
 - Se pueden conectar al sistema múltiples RTU, dependiendo de la capacidad del software y hardware instalados para el sistema.
 - El operador puede incorporar simulaciones de datos reales en el sistema.
- Hardware del SCADA

Un sistema SCADA consiste en una serie de unidades terminales remotas (o RTU), que recopilan datos de campo y envían esos datos a una estación maestra conformada por servidores a través de un sistema de comunicación hacia el Centro de Control.

La estación maestra muestra los datos adquiridos y también permite al operador realizar tareas de control remoto, los datos precisos y oportunos permiten optimizar la operación de la planta y proceso. Un beneficio adicional son operaciones más eficientes, confiables y, lo que es más importante, más seguras. Todo esto da como resultado un menor costo de operación en comparación con los sistemas anteriores, no automatizados.

En un sistema SCADA sofisticado, hay esencialmente cinco niveles o jerarquías:

- Dispositivos de control e instrumentación a nivel de campo
- Marshalling, o conversión de datos, de las RTU
- Sistema de comunicaciones

- La estación maestra
- El departamento de tecnología de la información comercial (TI), o procesamiento de datos del sistema informático.

Las RTU son equipos propios de las subestaciones, a pesar de ello, son las interfaces entre la subestación y el Centro de Control remoto donde se encuentra la estación remota, para implementar la comunicación de estos elementos, el sistema puede realizarse por cable, fibra óptica, radio, línea telefónica, microondas y posiblemente incluso satélite, utilizando protocolos específicos como son DNP 3.0 o IEC 60870-5-104 y filosofías de detección de errores para una transferencia de datos eficiente y óptima.

Los datos recopilados por la estación maestra son proyectados en una interfaz de operador para realizar acciones de monitoreo y control remoto.

- **Software del SCADA**

Software SCADA El software SCADA se puede dividir en dos tipos, propietario o abierto. Los diversos fabricantes han implementado software propietario para comunicarse con su hardware, el principal inconveniente de este tipo de software es que es necesario instalar equipos que sean totalmente compatibles. Por otra parte, la viabilidad de utilizar software abierto es necesaria para la interoperabilidad de equipos de diferentes fabricantes en el mismo sistema.

2.1.6.5. Generalidades Estándar IEC 61850

Este estándar es una serie de diversas publicaciones cuyo objetivo es establecer requisitos para establecer una estructura para la buena funcionalidad

del sistema de comunicación de una subestación de manera que todos los equipos de protección, control y medición puedan comunicarse entre sí, manejen un tiempo de respuesta para cada servicio de una manera estandarizada y que se normalice la estructura de datos dentro de la red LAN de la subestación y se asegure la interoperabilidad entre equipos.

Se implementa el concepto de nodo lógico para identificar todas las partes de la subestación para hacer las especificaciones mínimas que debe tener cada fabricante de manera que se establezca la comunicación entre equipos de diversos niveles de mando, por ejemplo, entre primarios y equipos de protección para cubrir los diversos servicios, un servicio es el método de comunicación que se utiliza entre los diversos nodos lógicos.

Luego de cubrir los servicios se necesita mapear la información; permite llevar todos los servicios y nodos lógicos a la LAN de la subestación por medio de protocolo Ethernet, donde ya se utilizan los diferentes tipos de mensajes GOOSE, SV y MMS, y son los que se definen en las siguientes viñetas:

- Mensajería GOOSE, cuyo significado es evento de subestación orientado a objetos genérico, este método de comunicación puede distribuir eventos en un tiempo crítico en milisegundos entre varios IEDs simultáneamente y se basa el mecanismo de editor y suscriptor. Estos mensajes son enviados de manera horizontal a toda la red LAN dedicada a los IEDs y no se realiza por medio de cables dedicados, entra en juego el papel importante del Multicast.
- SV (Sampled Values), se utilizan para transmitir los datos provenientes de los transformadores de instrumentos en patio, de manera que sea posible distribuirlos en la red LAN de los IEDs para que estos datos puedan ser

analizados, para la comunicación utiliza el principio de editor y suscriptor, de aquí que el dispositivo editor registra el valor medido y equipo suscriptor lee dicho valor y lo interpreta.

- MMS (especificación de mensajes de fabricación), se utiliza para transmitir comunicación de manera vertical y puede intercambiar información entre nodos lógicos en la red de comunicación. Este método de comunicación funciona bajo el concepto cliente / servidor y es muy útil para transmitir información entre la red LAN de los IEDs hacia el bus de estación de la subestación.

Por otro lado, la compatibilidad entre los diversos fabricantes se logra con los archivos de configuración SCL (Lenguaje de descripción de configuración de subestación), donde se transforma a un archivo XML que es compartido a los dispositivos de los diversos fabricantes para poder ser interpretados e implementando compatibilidad entre todos los dispositivos, esta parte es contenida dentro de la parte IEC61850-6.

- Servicios de comunicación

Ofrece tres tipos de modelo de comunicación:

- Tipo Cliente/Servidor
- Distribución rápida y confiable de datos basado en el modelo de editor y suscriptor; incluye mensajes GOOSE para Multicast de mensajes analógicos y digitales, y adicional, GSSE intercambio de datos digitales a través de Multicast.

- *Sample Values (SMV)*, para valores medidos de Multicast.

Tabla VI. **Partes del Estándar 61850**

Número	Título	Edición	Fecha de publicación
61850-1	Introducción y sinopsis	2.0	Marzo 2013
61850-2	Glosario	1.0	Agosto 2003
61850-3	Requerimientos generales	2.0	Diciembre 2013
61850-4	Sistema y gestión de proyectos.	2.0	Abril 2011
61850-5	Requisitos de comunicación para las funciones y modelos de dispositivos.	2.0	Enero 2013
61850-6	Lenguaje de descripción de configuración para la comunicación en subestaciones eléctricas relacionadas con los IEDs.	2.0	Diciembre 2009
61850-7-1	Estructura básica de comunicaciones – principios y modelos.	2.0	Septiembre 2011
61850-7-2	Información básica y estructura de comunicación – Abstract Communication Service Interface (ACSI).	2.0	Agosto 2010
61850-7-3	Estructura básica de comunicación – Clases de datos comunes.	2.0	Diciembre 2010
61850-7-4	Estructura de comunicación básica – clases de nodos lógicos compatibles y clases de objetos de datos.	2.0	Marzo 2010
61850-7-410	Estructura de comunicación básica – clases de nodos lógicos compatibles y clases de objetos de datos.	2.0	Octubre 2012

Continuación de la tabla VI.

61850-7-420	Estructura básica de comunicación – Recursos energéticos distribuidos nodos lógicos.	1.0	Mayo 2009
61850-7-510	Estructura básica de comunicación – Centrales hidroeléctricas – Modelos de conceptos y directrices.	1.0	Marzo 2012
61850-8-1	Servicio de Mapeo de comunicación específico – (SCSM) – Mapeo a MMS (ISO 9506-1 e ISO 9506-2) y a ISO /IEC 8802-3.	2.0	Junio 2011
61850-9-2	Servicio de mapeo específico (SCSM) - Sampled Values sobre ISO/IEC 8802-3.	2.0	Septiembre 2011
61850-10	Ensayos de conformación	2.0	Diciembre 2012
61850-80-1	Guía para el intercambio de información del modelo basado en CDC utilizando IEC 60870-101 o 60870-104.	1.0	Diciembre 2008
61850-90-1	Comunicación entre subestaciones.	1.0	Marzo 2010
61850-90-4	Guía para ingeniería de redes.	1.0	Agosto 2013
61850-90-5	Uso de IEC 61850 para transferencia de información por sincrofasores de acuerdo con IEEE C37.118.	1.0	Mayo 2012
61850-90-7	Modelos de objetos para convertidores de potencia en sistemas de recursos energéticos distribuidos (DER).	1.0	Febrero 2013

Fuente: PADILLA, Evelio. *Substation automation systems design and implementation*. p. 20.

- Impacto en la filosofía de implementación del sistema

La norma IEC 61850 brinda a los propietarios de subestaciones la oportunidad de rediseñar algunas de sus vistas tradicionales para implementar funciones SAS (control, protección, monitoreo, entre otros), esto conlleva a obtener ventajas económicas a mediano plazo y la posibilidad de mejorar la confiabilidad del sistema secundario tanto para la operabilidad como para la seguridad.

2.1.6.6. Clasificación de redes

Creadas para la conexión de múltiples dispositivos electrónicos inteligentes (IED), para compartir recursos y se clasifican según su extensión.

2.1.6.6.1. Redes de Área Local (LANs)

La red de área local conocida como LAN derivado de su significado en inglés *Local Area Network*, es una red cuyo alcance físico se concentra en una zona donde los equipos conectados a la red tienen conexión hacia uno o varios *switches* de comunicación que forman una red simple o redundante.

Características importantes a tener en cuenta en una red LAN:

- Cuenta con el método de difusión de mensajes o conocida como Broadcast, los cuales son repartidos en los equipos que forman la LAN.
- Por medio de protocolo Ethernet es posible contar con transmisión de datos en un rango de 1 Mbps hasta 1 Gbps.

- Como característica normalmente es de un radio no superior a 3 km, pero es permitido el uso de estándar FDDI, para crear líneas de fibra óptica logrando extender una LAN hasta un radio máximo de 200 km.
- Para la comunicación es partido el uso de protocolo privado.
- El medio de transmisión de datos a todos los dispositivos de la LAN es utilizando cable de cobre de par trenzado UTP, o fibra óptica.
- Ofrece versatilidad para sustituir algún equipo sea reemplazado en la red por alguna falla, dado que existen dispositivos con las mismas características técnicas y de diferentes marcas.
- La cantidad de dispositivos conectados depende de la capacidad de los *switches* de comunicación que conformen la LAN.
- Capacidad de comunicación con otras LAN por medio de *Router*.
- La limitante del alcance depende de la longitud máxima del cable de cobre o de la fibra, es posible utilizar repetidores para amplificar alcance.

2.1.6.6.2. Redes de área metropolitana (MANs)

El componente principal de este tipo de red es el *router*, la comunicación entre ellos se puede realizar por fibra óptica o microondas que aplique a la capa 3 del modelo OSI.

La principal aplicación de una red MAN es establecer comunicación entre dos o más nodos remotos como parte de una misma red, realizando conexión en un medio físico entre varias redes LAN para compartir información por medio de la velocidad que permita el protocolo utilizado.

Tiene la particularidad de implementarse como una red pública o bien, para gestionar redes de una empresa de manera que sea privada.

Un ejemplo de aplicación de red MAN en un sistema eléctrico de potencia es una red privada que transporte datos administrativos y de operación de dos subestaciones que se ubiquen a no más de cincuenta kilómetros y que utilicen operadores del centro de control que une más subestaciones conformado por varias MAN.

2.1.6.6.3. Redes de área amplia (WANs)

Este tipo de red de comunicación se aplica en la capa de aplicación del modelo OSI, y se aplica a funciones de software para interactuar con usuarios, y permite establecer conexión en un área de mayor extensión llegando a cientos de kilómetros a diferencia de las redes LAN y MAN.

En este tipo de red se cuenta con equipos terminales para la comunicación que se convierten nodos que por medio de protocolo pueden hacer posible la comunicación a grandes distancias entre los *hosts* convirtiendo la red donde se ubican en subredes de la WAN lo que hace posible incrementar el alcance de la red, haciendo llegar la red al nivel de expansión de internet.

Cuando varios *hosts* envían datos para comunicarse remotamente, se puede utilizar los medios que se encuentran en las redes LAN y el uso de *routers*, se puede aprovechar su utilidad para almacenar y enviar a la línea de transmisión para enviarlo al próximo *router* que forme parte de la WAN, y para hacerlo llegar al destino el *router* puede esperar a estar libre de tráfico para reenviar las tramas.

Las redes de área extensa con el objetivo de brindar diferentes funcionalidades es posible distribuir los elementos de la red de la siguiente manera:

- Red punto a punto

- Red en anillo
- Red en intersección de anillos
- Red en árbol
- Red completa
- Red en estrella
- Red irregular

2.1.6.6.4. Redes Virtuales Privadas (VPNs)

Una red privada virtual es aplicada principalmente en la capa 2 de enlace de datos, es aplicada en los *switches* de comunicación para redes LAN para crear conexiones seguras a internet.

Siempre y cuando se apliquen las medidas y protocolos de seguridad necesarias, por medio de Internet es posible tener conexión a una red corporativa, porque una vez se tiene acceso a la conexión enmascarada es importante que existan ciertas medidas de políticas de gestión de red, autenticación y niveles de acceso a funciones críticas y de información confidencial. Esto es posible porque se establece una conexión punto a punto que brinda un medio de comunicación específico para la VPN y se le puede agregar aún mayor seguridad utilizando protocolo con capacidad de cifrado.

Al realizar la conexión VPN a través de Internet se aplica una red WAN, entre los extremos remotos, pero para el usuario se visualiza como una VPN.

Ejemplos comunes en subestaciones es la posibilidad de conectar dos o más concentradores de subestación a la red empresarial en el centro de control

de nivel 3, utilizando como medio de conexión Internet, o que un empleado pueda acceder a la red de la empresa desde un sitio remoto desde su computadora.

- Usos de una VPN
 - Para acceder a la red de una empresa para realizar ciertas funciones de operación y monitoreo, mientras un operador se encuentra de vacaciones. Es importante que para funciones de monitoreo de los elementos de la subestación, se cuente con un sistema de autenticación y con nivel mínimo de acceso de contraseña como lo determina el estándar IEEE 1686, de ser posible es prudente que cualquier operación directa a los equipos de patio o cualquier tipo de disparo a los IEDs esté completamente prohibida desde un dispositivo que se conecte a través de una VPN. De ser necesario debería implementarse un nivel alto de seguridad para poder realizar este tipo de acciones.

2.1.6.7. Topologías de red de comunicaciones

Las topologías de red de comunicación que pueden encontrarse en las subestaciones son:

2.1.6.7.1. Bus

Para fines de una adecuada comunicación de los elementos de una subestación, la configuración de bus es aplicada en la red LAN especialmente cuando se trabaja con estándar IEC 61850 y específicamente para implementar bus de proceso, lo cual es parte de las subestaciones digitales.

La topología trabaja a un nivel de comunicación horizontal, es decir que todos los datos como eventos, disparos contenidos en GOOSE y valores analógicos transportados por medio de Sample Values, son llevados a todos los IEDs que formen parte de la topología de bus por medio de la facultad de Multicast o Multidifusión.

- Ventajas:
 - Tiene gran capacidad de redundancia en caso de falla de un equipo perteneciente al bus.
 - El sistema está más centralizado en el bus.

- Desventajas:
 - Existe un límite de equipos que se pueden conectar a la red
 - Dependiendo la cantidad de equipos conectados en el bus, puede producirse demasiado tráfico.
 - Para aislar una falla es más difícil la sanar la contingencia.
 - Dependiendo el medio físico de comunicación se tiene límite de distancias.
 - Se debe cerrar en anillo la conexión hacia los *switches*.
 - Posible saturación de mensajes en la red, provocando colisiones.

2.1.6.7.2. Cascada

Para subestaciones esta topología no es frecuentemente utilizada, y no es posible tener un nivel aceptable de redundancia, ya que los equipos no están conectados en anillo entre ellos y hacia todos los *switches* de comunicación, y se

debe tomar en cuenta que al fallar un *switch* se pierde la comunicación de los IEDs conectados a este.

2.1.6.7.3. Estrella

En el caso de aplicarse en una subestación, todos los IEDs en la red deben tener una conexión directa a un punto central por lo que toda la comunicación enviada por los equipos pasa a través de este, por ejemplo, un *switch* de comunicación.

El nodo central activo de la red en estrella, debe contar con medidas para evitar tráfico y eco. La conexión en estrella es utilizada en su mayoría en una red local, donde el nodo central puede contar un *switch* de comunicación, un *router* y un concentrador de datos.

- Ventajas
 - Si un IED se desconecta o se daña el cable solo queda fuera de la red ese IED.
 - Práctico de implementar.
 - Es viable para anticipar daños.
 - Fácil implementación de comunicación entre nodos.
 - Por su estructura, el mantenimiento se puede realizar de una manera cómoda y más económica.

- Desventajas
 - Si el nodo central falla, toda la red se desconecta, no hay posibilidad de redundancia.

- La implementación es costosa, y requiere más cable que las topologías bus o anillo.

2.1.6.7.4. Anillo

Topología de red en la que cada IED está conectado al siguiente en cada tablero, y el último elemento al primero, de manera que también se implemente un anillo entre los *switches* que forman parte de la LAN. Cada tablero que se integre en la red debe tener un equipo receptor y otro transmisor.

Se debe tomar en cuenta que no todos los IEDs están fabricados para implementarse en este tipo de topología, por diversos factores, como la falta de puertos o bien, la posibilidad de configuración en ellos. Es posible crear redundancia implementando anillo doble.

- Ventajas:
 - Ofrece una conexión de red simple
 - La configuración de equipos se torna relativamente fácil.
 - Los datos se reparten a todos los equipos de la red
- Desventajas:
 - La longitud de la red se limita a la capacidad de longitud del canal
 - Posible deterioro del canal para la comunicación cuanto mayor es la cantidad de quipos conectados en la red.
 - Posible lentitud en la transferencia de datos.

2.1.6.7.5. Malla

Todos los dispositivos tienen conexión entre sí, por tal motivo los datos en la red tienen diversos caminos para llegar al dispositivo de destino, lo que hace mucho menos probable que ocurra una posible interrupción de comunicación en toda la red porque el tráfico tiene diversos caminos.

La particularidad de esta configuración es que por medio de cables separados los equipos se conectan todos entre sí, de manera que el concepto de redundancia es aplicado en toda la red. Por lo que una red mallada obtiene un grado de confiabilidad sumamente importante ya que se cuenta con la garantía que nunca se perderá la comunicación en la red.

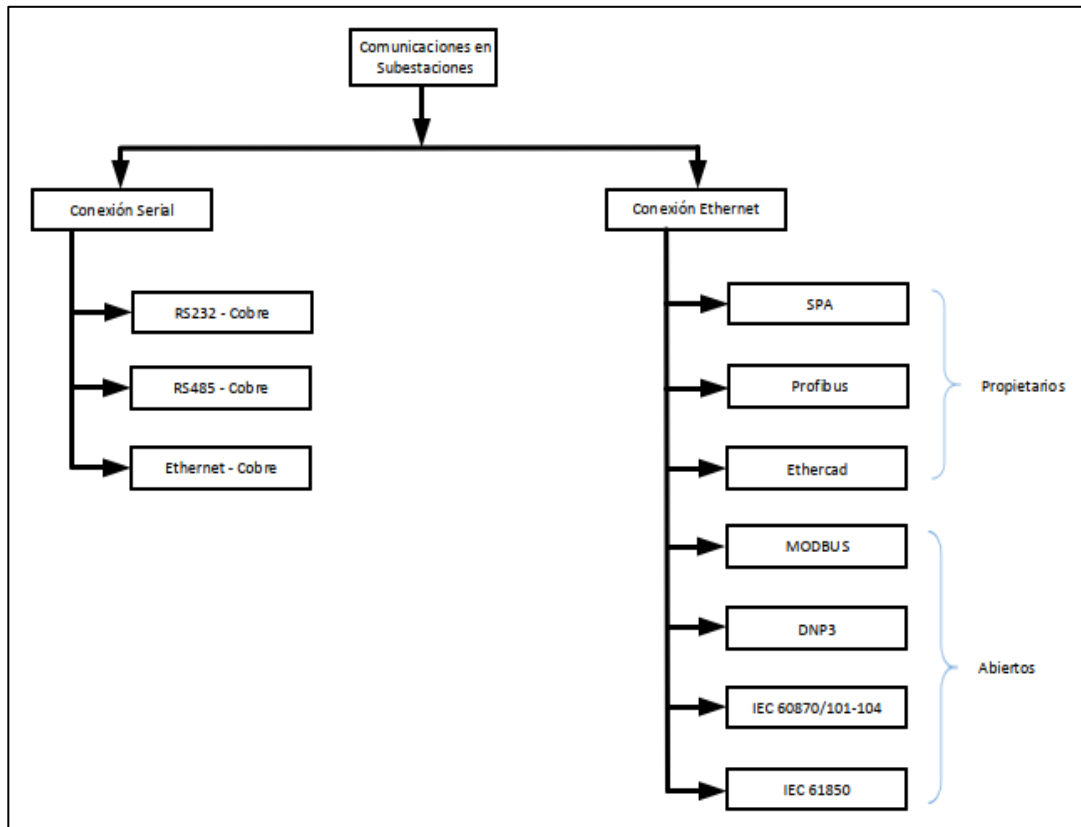
Con la finalidad de hacer posible implementar este tipo de red desde el punto de vista económico, es necesario no utilizar medios de conexión físico, cable, y emplear la conexión inalámbrica, porque este tipo de red inalámbrica es más viable de implementar.

Es posible aplicar redes híbridas con el motivo de mejorar la confiabilidad de redes con otro tipo de topología.

2.1.6.8. Comunicaciones en la subestación

La comunicación en las subestaciones depende de varios estándares y protocolos de comunicación para poder realizar de manera efectiva todas las funciones importantes de control, protección y medida, en la figura 27 se muestra cómo se distribuye.

Figura 27. Clasificación de protocolos de comunicación



Fuente: elaboración propia, empleando Microsoft Visio 2016.

2.1.6.8.1. Conexión serial

Es el tipo de conexión que utiliza un medio de cobre para su comunicación.

Un estándar de interfaz define los detalles eléctricos y mecánicos que permiten equipos de comunicaciones de diferentes fabricantes para que se conecten entre sí y funcionen de manera eficiente. Cabe destacar que RS-232 y otros relacionados.

Los estándares EIA, definen solo los detalles eléctricos y mecánicos de la interfaz y no definen un protocolo. Estos estándares fueron diseñados principalmente para transportar datos digitales de un punto a otro. El estándar RS-232 se diseñó inicialmente para conectar equipos informáticos digitales a un módem donde los datos se convertirían luego a una forma analógica adecuada para la transmisión a mayores distancias. RS-485 tiene la capacidad de transferir datos digitales a través de distancias superiores a 1 200 m.

El más popular (pero probablemente técnicamente el más inferior) de los estándares RS es el estándar RS-232C. Esto se discutirá primero. La representación correcta de RS-232E y RS-485 es en realidad EIA-232E y EIA-485.

- Estándar RS 232

Es un estándar recomendado por donde dos dispositivos se comunican y está revisado por la asociación de Industriales Eléctricas (EIA), y es una conexión punto a punto. La práctica recomienda distancias no mayores a 15 metros sobre medios de cobre, el estándar no define el protocolo, pero si la funcionalidad de la interfaz física.

El estándar RS-232 consta de 3 partes principales, que definen:

- La señal eléctrica y el nivel de voltaje
- Las características mecánicas del hardware, son básicamente: DTE y DCE.
- La descripción funcional de los circuitos de intercambio.

En cuanto a la señal eléctrica, el RS-232 es diseñado para la conexión de dispositivos:

- DTE

Por sus siglas "DTE" Equipo terminal de datos, pueden ser: computadoras, relevadores, Dispositivos Electrónicos Inteligentes (IEDs). En sus inicios un dispositivo DTE se comunicaba con un dispositivo DCE y transmitía datos en el pin 2 y recibía datos en el pin 3 en un conector tipo D de 25 pines, actualmente se realiza por medio de un conector tipo DB-9 de nueve pines.

- DCE

Equipo de Comunicación de Datos (DCE): equipos de comunicación como transceivers, convertidores de medio. Un dispositivo DCE transmite datos entre el DTE y un enlace de comunicaciones de datos físico.

El transmisor RS-232 tiene que producir un nivel de voltaje ligeramente más alto en el rango de +5 voltios a +25 voltios y de -5 voltios a -25 voltios para superar la caída de voltaje a lo largo de la línea.

En la práctica, la mayoría de los transmisores funcionan con voltajes entre 5 y 12 voltios, las líneas de datos se utilizan para la transferencia de datos. Los pines 2 y 3 se utilizan para este propósito. El flujo de datos se designa desde la perspectiva de la interfaz DTE, el DTE transmite (y el DCE recibe), está asociada con la patilla 2 en el extremo DTE y la patilla 2 en el extremo DCE.

La "línea de recepción", en la que el DTE recibe (y el DCE transmite), está asociada con la patilla 3 en el extremo DTE y la patilla 3 en el extremo DCE. El

pin 7 es la línea de retorno común para las líneas de transmisión y recepción de datos.

Las líneas de control se utilizan para el control de dispositivos interactivos, comúnmente conocido como "hardware" y regular la forma en que los datos fluyen a través de la interfaz. Las cuatro líneas de control más utilizadas son:

- RTS
- CTS
- DSR
- DTR

Los pines de los conectores y la función que ejercen en la comunicación son:

Tabla VII. **RS-232 DB-9 Pinout (DTE)**

DB-9	Función	Abreviación
Pin 1	Data Carrier Detect	CD
Pin 2	Received Data	RD, RX, or RXD
Pin 3	Transmitted Data	TD, TX, or TXD
Pin 4	Data Terminal Ready	DTR
Pin 5	Signal Ground	GND
Pin 6	Data Set Ready	DSR
Pin 7	Request to Send	RTS
Pin 8	Clear to Send	CTS
Pin 9	Ring Indicator	RI

Fuente: WEIS, Olga. *Interfaz de comunicación serie. Pinout RS232*. <https://www.virtual-serial-port.org/es/article/what-is-serial-port/rs232-pinout/>. Consulta: 25 de septiembre de 2021.

Tabla VIII. **RS-232 DB-9 Pinout (DCE)**

DB-9	Función	Abreviación
Pin 1	Data Carrier Detect	CD
Pin 2	Transmitted Data	TD, TX, or TXD
Pin 3	Received Data	RD, RX, or RXD
Pin 4	Data Terminal Ready	DTR
Pin 5	Signal Ground	GND
Pin 6	Data Set Ready	DSR
Pin 7	Clear to Send	CTS
Pin 8	Request to Send	RTS
Pin 9	Ring Indicador	RI

Fuente: WEIS, Olga. *Interfaz de comunicación serie. Pinout RS232*. <https://www.virtual-serial-port.org/es/article/what-is-serial-port/rs232-pinout/>. Consulta: 25 de septiembre de 2021.

El rango de voltaje que se puede manejar es el siguiente:

Tabla IX. **Rango de voltaje para las lógicas en EIA-232**

	Rango
Lógica 0	+3V y +25V
Lógic 1	-3V y -25V
Indefinida	-3V y +3V

Fuente: elaboración propia.

La transmisión de datos funciona de la siguiente manera:

- La comunicación EIA-232 depende de una velocidad de sincronización establecida a la que ambas piezas de hardware se comunican.

- El hardware sabe cuánto tiempo debe ser alto o bajo un bit según la velocidad de datos.
- EIA-232 también especifica el uso de los *bits* de inicio, parada y paridad.

Una de las particularidades para que se pueda dar la comunicación ambos dispositivos deben tener la misma velocidad de datos para comunicarse, pero también deben saber para manejar problemas.

Es necesario saber que la velocidad de los *bits* es el número de dígitos binarios transmitidos en 1 segundo (*bits* por segundo, bps), de aquí que la velocidad de transmisión es el número de elementos de señalización por unidad de tiempo, y la velocidad de transmisión no es igual a bps a menos que la señalización sea de 1 *bit*.

Las limitaciones más notorias del RS-232 cuando se requiere una conexión punto multipunto son las siguientes:

- La limitación de distancia (normalmente 50 metros), es una limitación cuando las distancias de 1000 m son necesarias.
- La velocidad en baudios de 20 kbps es demasiado lenta para muchas aplicaciones.
- El estándar es un ejemplo de un estándar desequilibrado con alta susceptibilidad al ruido.
- Estándar RS-485.

Estándar de la capa física de comunicaciones es una interfaz del tipo serial que utiliza un proceso de señal equilibrada o diferencial para admitir aplicaciones punto a punto, punto a multipunto y multidrop. Actualmente es conocido como EIA/TIA-485, fue creado para ampliar las capacidades físicas de la interfaz RS-232.

El modo de operación es del tipo diferencial y la máxima cantidad de transmisores y receptores en una línea es de 32 transmisores (TX), y 32 receptores (RX), en una línea, tomando en cuenta que únicamente un transmisor puede estar activo a la vez.

El alcance de un cable de conexión puede ser de hasta 1 200 metros, de manera que se intercambian los datos a través de un cable de par trenzado de 22 o 24 hilos AWG. La función principal es transportar una señal por dos cables, mientras que un cable transporta la señal original, el otro transporta una señal inversa, lo que proporciona una alta resistencia al ruido.

Los voltajes de línea oscilan entre -1.5 V a -6 V para un "1" lógico y de $+1,5\text{ V}$ a $+6\text{ V}$ para un "0" lógico. Al igual que con RS-422, el controlador de línea para la interfaz RS-485 produce un voltaje diferencial en dos cables, y para los sistemas Full Duplex, se requieren cinco cables.

Para un sistema Half Duplex, solo se requieren tres cables. El cable adicional (5 en lugar de 4, 3 en lugar de 2), es para proporcionar un voltaje de referencia común para todos los dispositivos del sistema.

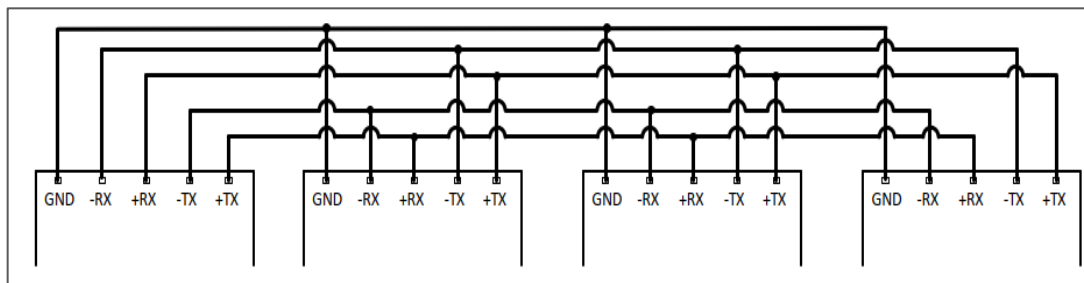
La principal mejora de RS-485 es que un controlador de línea puede operar en tres estados, siendo estos: "0" lógico, "1" lógico y "alta impedancia", donde prácticamente no consume corriente y parece no estar presente en la línea.

Este último estado se conoce como estado "deshabilitado" y puede iniciarse mediante una señal en un pin de control en el circuito integrado del controlador de línea. Esto permite el funcionamiento multipunto.

A cada terminal de un sistema multipunto se le debe asignar una dirección única para evitar conflicto con otros dispositivos del sistema. RS-485 incluye limitación de corriente en los casos donde ocurre la contención.

Para la configuración en *Full Duplex* todas las conexiones de dispositivos son consistentes y es requerido para aplicaciones punto a multipunto como IEC 60870-5-101/104 o DNP3 Modbus, es un estándar de cuatro hilos sin contar el de tierra.

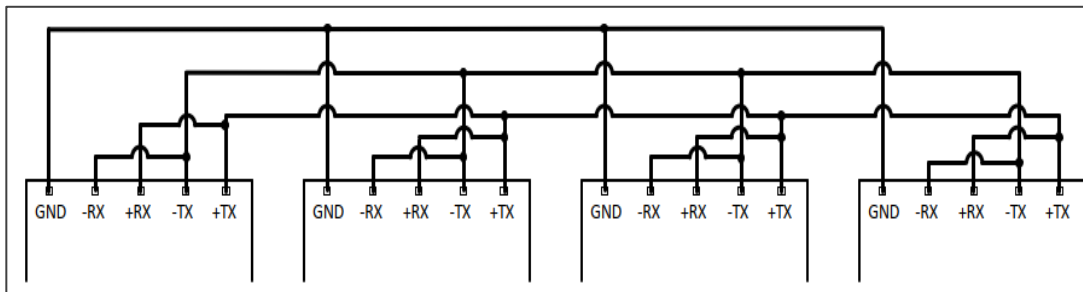
Figura 28. **Configuración *Full Duplex***



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Para la configuración de *Half Duplex*, solo un dispositivo puede transmitir a la vez, las polaridades coincidentes de RX y TX usan las mismas líneas de datos y esta configuración admite protocolos direccionales como DNP3 o Modbus, es un estándar de dos hilos sin contar el de tierra.

Figura 29. **Configuración *Half Duplex***



Fuente: elaboración propia, empleando Microsoft Visio 2016.

En esta configuración el flujo de datos serie puede ser transportado en una dirección, la transferencia de datos al otro lado requiere la utilización de un transceptor; es un dispositivo que genera una señal desde el transmisor.

En configuración Multiseñalador la línea de comunicación RS-485 puede trabajar con varios transceptores y receptores conectados, al mismo tiempo, un transmisor y varios receptores pueden conectarse a una línea de comunicación a la vez, el resto de transmisores que requieran conectarse esperan hasta que la línea de comunicación este libre para la transmisión de datos.

La comunicación por RS-485 sigue siendo la base de muchas redes de comunicación en la actualidad, las principales ventajas son:

- Transmiten datos a través de cobre de par trenzado, por lo que es posible tener bidireccionalidad para el tráfico de datos.
- Soporte para varios transceptores conectados a la misma línea, haciendo posible la capacidad de crear comunicación desde varios puntos en la red.

- Por medio de repetidores, es posible aumentar la longitud de la comunicación.
- Se mejora la velocidad de transmisión de datos. La máxima velocidad de datos de 12 a 1 200 metros en RS-485 es de 10 Mbps a 100 kbps.

2.1.6.8.2. Protocolo Ethernet

Es un protocolo de red que se utiliza comúnmente en redes de área local cableadas LAN, principalmente controla cómo se transmiten los datos a través de la red, para ello es necesario hacer mención de las capas del modelo OSI.

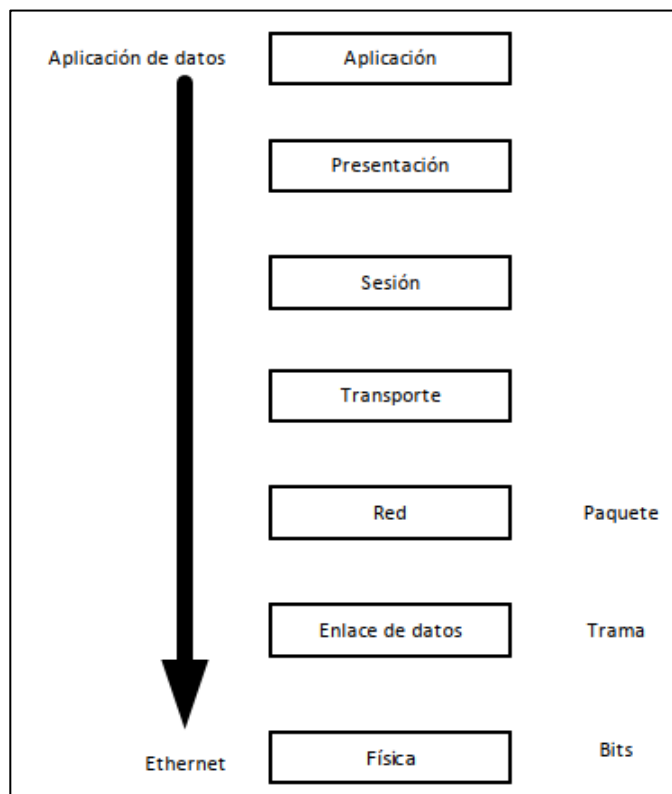
El modelo OSI es un método para describir cómo se pueden organizar los conjuntos entrelazados de hardware y software de red para trabajar juntos en la red.

El modelo OSI proporciona una manera de dividir arbitrariamente la tarea de especificar el comportamiento de la red en partes separadas, que luego se someten al proceso formal de estandarización.

Es importante recordar que el modelo OSI describe las funciones de una red, no es una arquitectura o un modelo para el diseño de la red como tal. El modelo de referencia OSI describe siete capas de funciones de red, como se ilustra en la figura. Las capas inferiores cubren los estándares que describen cómo un sistema LAN y las capas superiores tratan con nociones más abstractas, como la transmisión de datos y cómo se representan los datos al usuario.

El protocolo abarca su operación en las primeras dos capas del modelo OSI: la capa de enlace de datos y la capa física. En la figura 30 se muestran todas las capas.

Figura 30. **Capas del modelo OSI**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

En la capa física, Ethernet utiliza los medios para el transporte de tramas *bits* en todas las topologías de red.

Ethernet opera en la capa 2 específicamente en la subcapa de MAC que se encarga de determinar el medio de comunicación conocida también como

Control de Acceso al Medio. La subcapa MAC se ocupa de preparar los canales para el transporte de los datos.

Figura 31. Limitaciones de capa 1 y capa 2

Limitaciones de la capa 1	Funciones de la capa 2
<ul style="list-style-type: none"> • No es posible por sí mismas comunicar con capas superiores. 	<ul style="list-style-type: none"> • Se conecta con las capas superiores mediante control de enlace lógico (LLC).
<ul style="list-style-type: none"> • No es posible la identificación de elementos. 	<ul style="list-style-type: none"> • Utiliza esquemas de direccionamiento para identificar dispositivos.
<ul style="list-style-type: none"> • Únicamente son reconocidas las tramas de <i>bits</i>. 	<ul style="list-style-type: none"> • Utiliza tramas para organizar los <i>bits</i> en grupos.
<ul style="list-style-type: none"> • Cuando existe tráfico de datos por diversas fuentes, la fuente de origen no se detecta. 	<ul style="list-style-type: none"> • Utiliza control de acceso al medio (MAC) para identificar fuentes de transmisión.

Fuente: elaboración propia.

En resumen, el modelo de referencia OSI incluye las siguientes siete capas, comenzando en la parte inferior y avanzando hacia la capa superior.

- Capa física (capa 1)

Estandariza el control eléctrico, mecánico y funcional de los circuitos de datos que se conectan a los medios físicos.

- Capa de enlace de datos (capa 2)

Establece la comunicación de una estación a otra conectada a la misma red. Esta es la capa que transmite y recibe tramas y reconoce direcciones de enlace. Las partes del estándar Ethernet que describen el formato de trama y el protocolo de control de acceso a medios pertenecen a esta capa.

- Capa de red (capa 3)

Establece la comunicación de una estación a otra a través de una internetwork, que se compone de varios sistemas de red interconectados. Esta capa proporciona un nivel de independencia de las dos capas inferiores al establecer funciones y procedimientos de nivel superior para intercambiar datos entre computadoras a través de múltiples redes.

Los estándares en esta capa del modelo describen partes de los protocolos de red de alto nivel que se transportan en el campo de datos de la trama Ethernet. Los protocolos en y por encima de esta capa del modelo OSI son independientes del estándar Ethernet.

- Capa de transporte (capa 4)

Proporciona mecanismos confiables de recuperación de errores de extremo a extremo y control de flujo, ubicados en el software de red de nivel superior.

- Capa de sesión (capa 5)

Proporciona mecanismos para establecer comunicaciones confiables entre aplicaciones que se ejecutan en computadoras separadas.

- Capa de presentación (capa 6)

Proporciona mecanismos para tratar la representación de datos en aplicaciones.

- Capa de aplicación (capa 7)

Proporciona mecanismos para admitir aplicaciones de usuario final (por ejemplo, correo electrónico o navegadores web).

- Subcapas IEEE dentro del modelo OSI

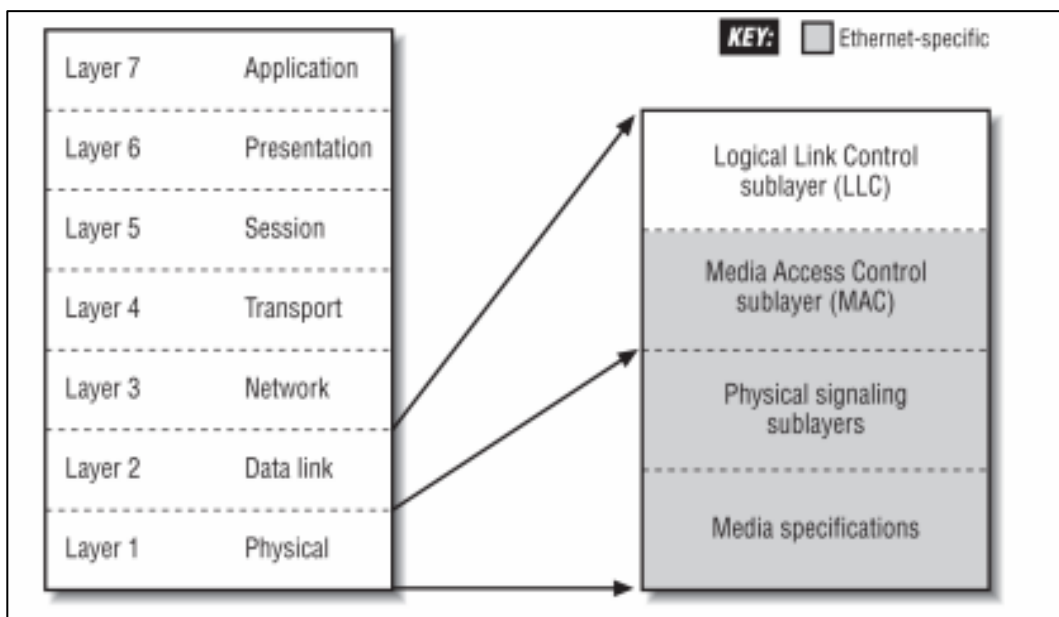
El estándar Ethernet se ocupa de los elementos descritos en la capa 2 (la capa de enlace de datos), y la capa 1 (la capa física) del modelo OSI. Para ayudar a organizar los detalles del desarrollo al optar por las especificaciones para Ethernet, el estándar IEEE define subcapas adicionales que encajan en las dos capas inferiores del modelo OSI, lo que simplemente significa que el estándar IEEE incluye algunas capas más finas que el modelo OSI.

En teoría las subcapas están fuera del modelo de referencia OSI, a pesar de ello, el modelo OSI no está destinado a dictar la estructura de los estándares o el diseño de productos de red, por tal motivo se pueden agregar capas para dar soporte a la finalidad y necesidades de ésta.

La figura muestra las dos capas inferiores del modelo de referencia OSI y muestra cómo se organizan varias de las subcapas específicas de IEEE. Dentro de las principales subcapas que se muestran, hay más subcapas definidas para funciones MAC adicionales.

En el nivel de enlace de datos OSI (Capa 2), existen subcapas de control de enlace lógico (LLC), y control de acceso a medios (MAC), IEEE, que son las mismas para todas las variedades y velocidades de Ethernet. La capa LLC es un mecanismo definido por IEEE para identificar los datos transportados en una trama de Ethernet. La capa MAC define los protocolos utilizados para arbitrar el acceso al sistema Ethernet.

Figura 32. **Subcapas IEEE mayores**



Fuente: SPURGEON, Charles; ZIMMERMAN, Joann. *Ethernet, the definitive guide: designing and managing Local Area Networks*. p. 19.

- Niveles de cumplimiento

Al desarrollar un estándar técnico, el IEEE incluye solo aquellos elementos cuyo comportamiento debe especificarse cuidadosamente para garantizar que el sistema funcione correctamente.

Todas las interfaces Ethernet deben cumplir completamente con las especificaciones del protocolo MAC en el estándar para realizar sus funciones de manera idéntica. De lo contrario, la red no funcionaría correctamente. Al mismo tiempo, el IEEE hace un esfuerzo por no restringir el mercado al estandarizar cosas como la apariencia de una interfaz Ethernet o cuántos conectores debería tener.

La intención es proporcionar las especificaciones de ingeniería suficientes para que el sistema funcione de manera confiable e interopere correctamente, sin inhibir la competencia y la inventiva del mercado. En general, el IEEE ha tenido bastante éxito en este objetivo. Es posible que algunos de estos dispositivos funcionen bien, pero normalmente no interactuarán con el equipo de otros proveedores porque no siguen los estándares.

Tabla X. **Estándares LAN basados en Ethernet**

Estándar	Data Rate	Descripción
IEEE 802.3	10 Mbps	10BASE-5 sobre coaxial cable, "Red Gruesa"
IEEE 802.3a	10 Mbps	10BASE-2 Sobre coaxial cable, "Red Delgada"
IEEE 802.3i	10/100 Mbps	10/100BASE-T Sobre cobre, "Par trenzado"
IEEE 802.3ab	1 Gbps	1000BASE-T Gigabit Par trenzado (cat 5e or cat 6)
IEEE 802.3j	10 Mbps	10BASE-F sobre fibra
IEEE 802.3u	100 Mbps	100BASE-TX/FX (Ethernet rápido cat 5e or 1,300 nm fiber)
IEEE 802.3z	1 Gbps	1000BASE-SX Gigabit Ethernet sobre 850 nm multimode fiber
IEEE 802.3z	1 Gbps	1000BASE-LX Gigabit Ethernet sobre 1,300 nm single-mode fiber

Fuente: elaboración propia.

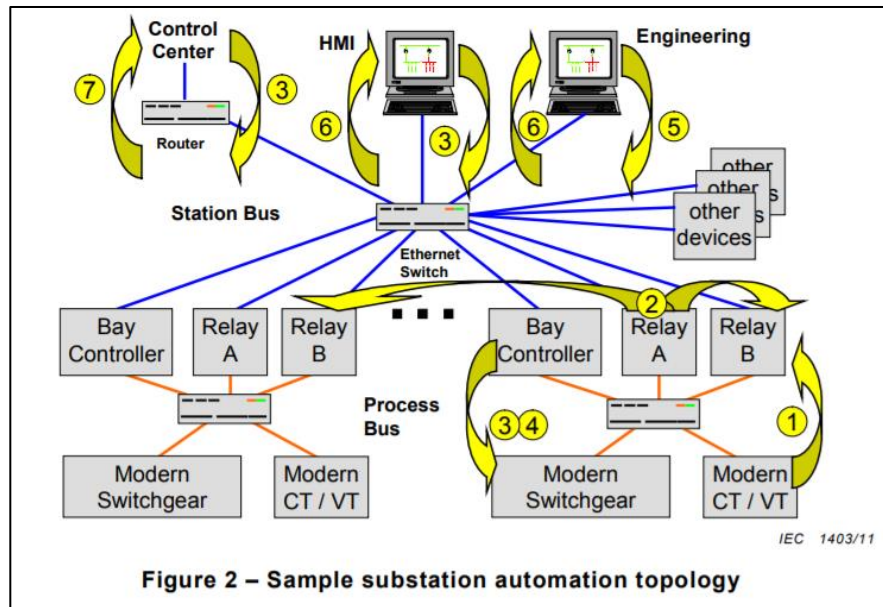
3. SUBESTACIONES DIGITALES

Las subestaciones digitales son la evolución tecnológica de las subestaciones convencionales producto de la digitalización de las funciones que se desarrollan en los equipos propios de la subestación, como las funciones de protección y control. En el presente capítulo se abarcan únicamente los elementos y características propias de las subestaciones digitales, y muchos elementos que forman parte de éstas son comunes para las subestaciones convencionales. La principal diferencia es la implementación del Bus de Proceso, en este se describe con mayor detalle en el presente capítulo.

La Funciones de topología y comunicación de los sistemas de automatización de subestaciones como se muestra en la topología de la Figura 33, un enfoque de la serie IEC 61850 es el soporte de funciones de automatización de la subestación mediante la comunicación de (los números entre paréntesis se refieren a la figura).

- Intercambio de valor muestreado para CT y VT (1)
- Intercambio rápido de datos de E / S para protección y control (2)
- Señales de control (3)
- Señales de disparo (4)
- Ingeniería y configuración (5)
- Seguimiento y supervisión (6)
- Comunicación del Centro de Control (7)
- Sincronización de tiempo

Figura 33. **Topología de los sistemas de automatización de subestaciones digitales**



Fuente: INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Communication networks and systems for power utility automation*. Standard IEC 61850-7-1. p. 16.

3.1. **Arquitectura de las subestaciones digitales**

A diferencia de las subestaciones convencionales, la arquitectura de la subestación digital tiene tres niveles.

- El primero es el nivel de patio, es el nivel que está conformado por los equipos primarios de la subestación.
- El segundo es la interfaz de proceso. Está formado por las *Mergin Unit*, por los distintos IEDs (equipos de control y medición), y los *switch* de comunicación conocido como bus de proceso.

- El tercero, el nivel de estación, se encarga de reunir la información de los elementos dentro de la subestación y también de enviarla a niveles superiores, coordina las funciones operativas de la subestación por medio del bus de estación donde se interconectan los equipos del nivel de bus y los equipos como RTUs, *Gateways*, Routes y HMIs, y todo este conjunto de equipos apoyan a nivel de estación.

Los datos en tiempo real se obtienen por medio de sensores y equipos que forman parte del sistema primario, que comunican con los equipos convertidores hacia el bus de proceso.

La importancia de los IEDs como enlace entre el bus de proceso y el bus de estación es fundamental, y estos equipos deben tener presente contar con un puerto para recibir toda la información proveniente del bus de estación y enviarla por medio del otro puerto hacia los equipos del bus de estación.

Las subestaciones digitales por sus características son capaces de monitorear los elementos de la red y de contar con la implementación adecuada, contar con acceso seguro desde cualquier punto de acceso.

Algunos beneficios de las subestaciones digitales son:

- Mejora la capacidad de transmisión de datos
- Pueden utilizarse funciones agrupadas para ejecutarse en equipos que estén disponibles para cumplir con funciones simultáneas, ahorrando equipos.
- Escalabilidad y facilidad de añadir funciones.

- Las redes de comunicación reemplazan diversos cableados de control.
- Problemas asociados a la interferencia en cables son eliminados.
- Se mejora la comunicación y automatización en la subestación.
- Aumenta la seguridad en la sala de control.
- Se obtiene reducción de inversión y costos por mantenimiento.

3.2. Equipos de subestaciones digitales

En los siguientes incisos se describen los diferentes equipos de subestaciones digitales.

3.2.1. Transformadores ópticos

Al igual que los transformadores de instrumentos convencionales, estos elementos son utilizados para medir voltajes y corrientes de lado de alta tensión de las subestaciones y convertirlos a voltajes aceptables dentro del rango de funcionamiento de los elementos de protección, medición, control y supervisión de la calidad de energía.

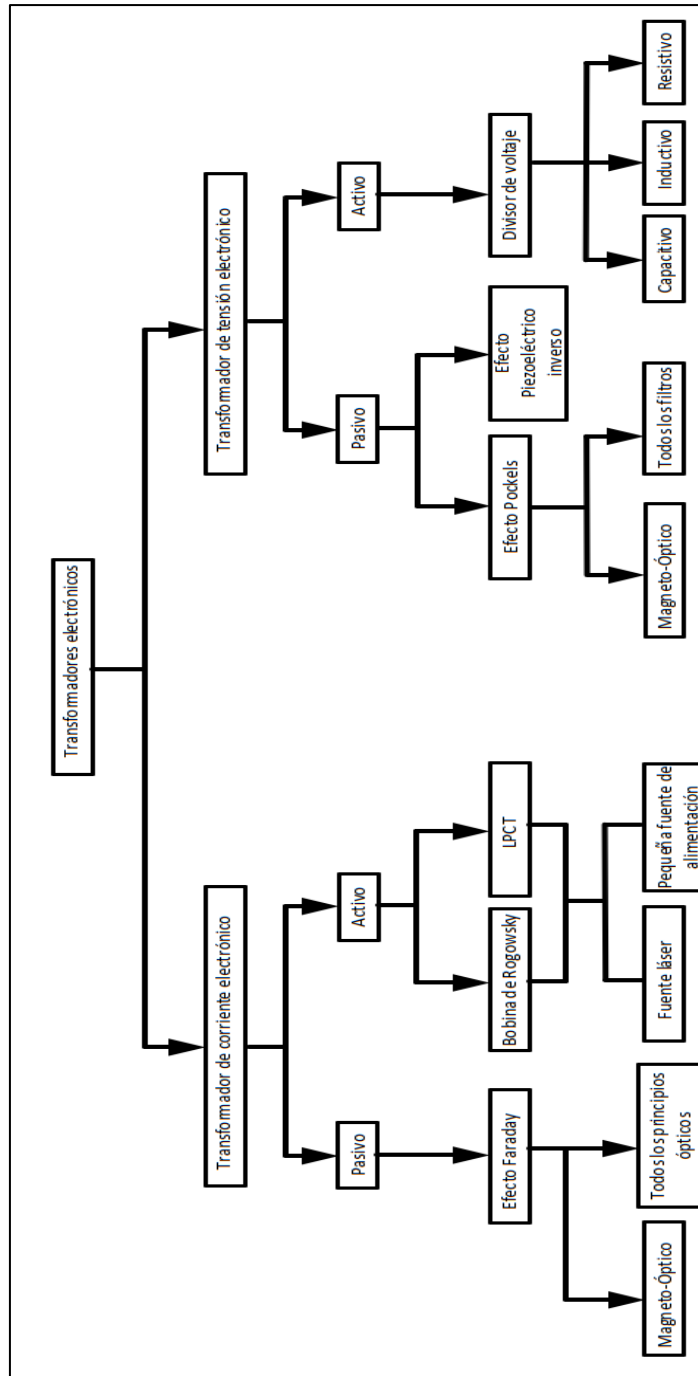
A diferencia de los transformadores convencionales, los ópticos se basan principalmente en efectos ópticos o electromagnéticos de muy baja potencia, teniendo circuitos electrónicos encargados de transformar las señales obtenidas directamente del elemento medido y transformarlas en datos digitales o señales analógicas de baja potencia, enviándolos a los equipos de protección, control y

medición, o en su defecto, hacia una *Mergin unit* encargada de funcionar como transductor entre los transformadores ópticos y los equipos PCyM.

Estos transformadores combinan técnicas tradicionales de medición conjuntamente con señales ópticas para transmisión, permitiendo, esto una conexión no conductiva entre el transductor en la subestación y la interface en el cuarto de control.

La clasificación de los transformadores según los elementos que lo conforman es la siguiente:

Figura 34. Clasificación de los transformadores ópticos



Fuente: elaboración propia, empleando Microsoft Visio 2016.

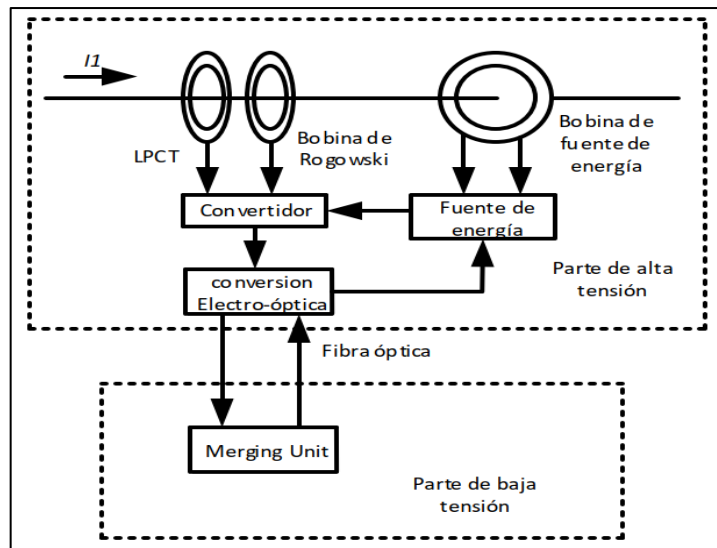
3.2.1.1. Transformadores ópticos de corriente

Los transformadores de corriente ópticos, están constituidos por elementos pasivos y activos.

- Elementos activos

Este tipo de transformador de corriente funciona por medio de cristales magneto-ópticos. Son dispositivos basados o contruidos con bobinas de Rogowsky y bobinas de baja potencia, las que necesitan una fuente para los transductores que forman parte del lado primario o de alta tensión propio del transformador. En la figura 35 se puede apreciar un esquema de la constitución.

Figura 35. Esquema de constitución de elementos de un transformador óptico



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Están constituidos por los siguientes elementos para la parte de alta tensión:

- Bobina de Rogowski

Una bobina de Rogowski es un arrollamiento de alambre en un toroide (núcleo no ferromagnético), a través de este pasa flujo magnético producido por la corriente que fluye por el conductor quien es el objeto de la medición, como es bien sabido, el flujo inducirá una F.E.M. debido a ley de inducción de Faraday, la forma de onda de la tensión inducida será la derivada de corriente a medir. Se torna como parte importante la implementación de un integrador con la finalidad de obtener una señal con forma de onda similar a la corriente medida. Ante estímulos de alta frecuencia se obtienen resultados lineales dado a la ausencia de materiales ferromagnéticos, evitando problemas de saturación como es el caso de los transformadores convencionales.

- Integrador

Se conoce como la etapa de integración y se toma la señal de la F.E.M. inducida directamente de la bobina de Rogowski, dado los elementos que conforman el integrador, la tensión será similar o igual a la corriente dependiendo de las características del amplificador operacional que se utilice. El integrador cuenta con divisores de voltaje, comparadores e impedancias, es uno de los métodos más utilizados para la construcción de transformadores ópticos. A las salidas de este, la señal de salida del integrador será en AC para ser enviada a los conversores de medio para convertir la señal AC en señal óptica.

- Convertidores

Estos elementos convierten señales de baja tensión que se generan y se transforma para transmitirse por medio óptico hacia una Merjin Unit para el caso

de una subestación que no esté totalmente digitalizada, o en caso de estar totalmente digitalizada, directamente a los equipos de medición.

- LPTC (*Low Power Current Transducer*)

Son sensores que funcionan por inducción, tienen un núcleo de hierro. La corriente inducida pasa a través de una resistencia en el devanado secundario y convierte la corriente en una salida de tensión.

Se realiza un divisor de tensión a la salida del LPTC, donde la resistencia R_{SH} juega el papel principal de conversión para ajustar el nivel de tensión y enviarlo hacia los convertidores de señales análogas a digitales.

- Elementos pasivos

Están basados en principios de medida óptica. No requieren fuentes adicionales de tensión para el lado primario.

Los transformadores ópticos de corriente funcionan de acuerdo con la ley de Ampere, a diferencia de los transformadores convencionales, los transformadores ópticos se basan en efectos magneto ópticos de Faraday, de aquí que entra en juego la ley de Faraday.

El efecto Faraday se basa en medir la rotación del plano de polarización de la luz, esto se realiza a través de un campo magnético. Según la siguiente ecuación que describe el efecto:

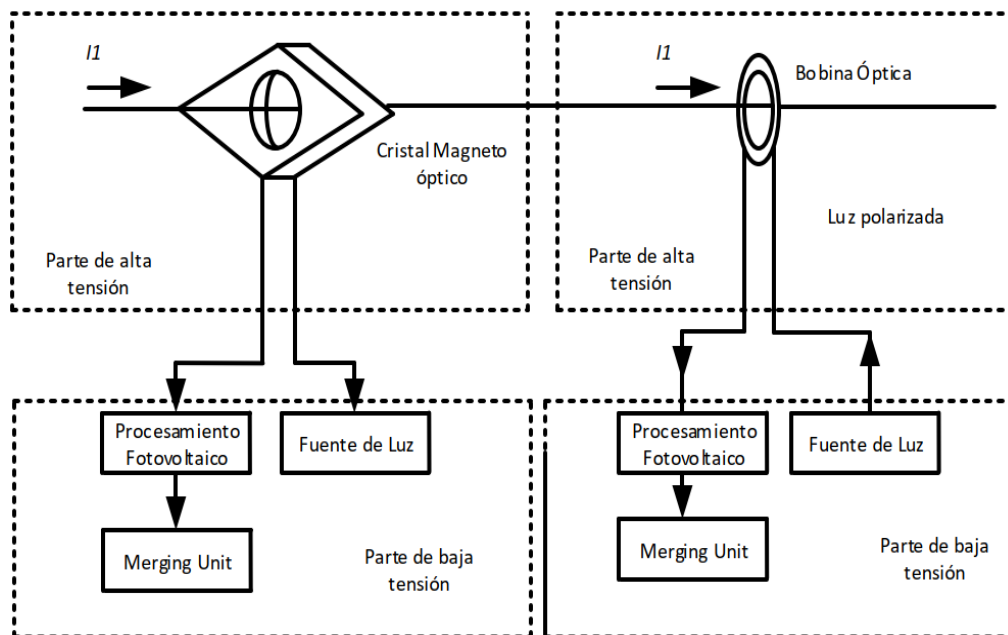
$$\varphi = V \int H \cdot dl$$

Donde φ es el ángulo de rotación de Faraday, y V representa la constante de Verdet del medio, como ya es bien conocido H es la intensidad de campo magnético y L es la longitud del medio óptico que atraviesa la luz polarizada, y se puede deducir que el ángulo de rotación depende directamente de la intensidad del campo magnético y de la longitud que recorra la luz polarizada.

El plano de polarización gira gracias a que en el momento en que la luz linealmente polarizada pasa a través del medio, en este caso un cristal óptico, bajo el campo magnético generado por la corriente.

La constitución de los transformadores se representa en la figura 36.

Figura 36. **Diagrama de transformador de corriente óptico con elementos pasivos**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

3.2.1.2. Transformadores de tensión

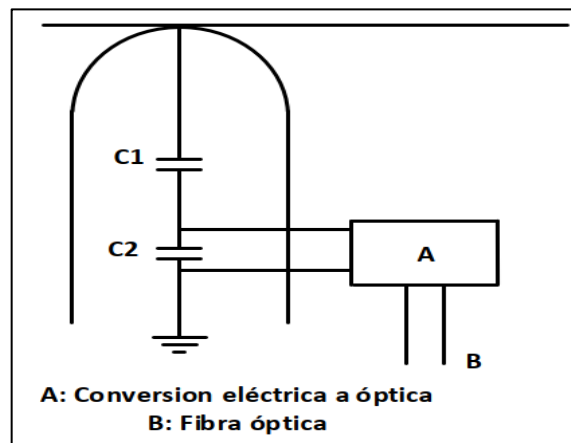
Al igual que los transformadores de corriente ópticos, los transformadores de tensión ópticos se rigen por medio de elementos activos y elementos pasivos.

- Elementos activos

Son transformadores que tienen en el primario un sensor como divisor de tensión conformado por resistencias o bien por capacitores, que genera una salida de tensión que va directamente a un conversor análogo-digital y luego a un conversor digital-óptico a través de un módulo remoto electrónico.

Los transformadores electrónicos con divisores de tensión es la tecnología más sencilla y la más frecuentemente utilizada. Se basa en el empleo de condensadores en serie para dividir la tensión. El captador se coloca en la parte de baja tensión, de tal manera que los circuitos electrónicos convierten las señales de baja tensión en pulsos digitales para la transmisión, como se muestra en la figura 37.

Figura 37. **Conversión de señales eléctricas a ópticas**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

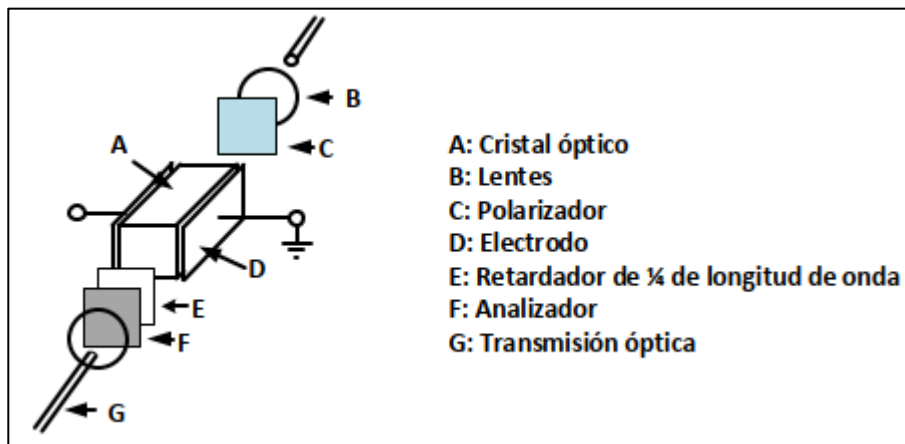
- Con elementos pasivos

Son transformadores que usan los principios ópticos para las medidas. Cuando un material cristalino se expone ante un campo eléctrico puede cambiar sus propiedades anisotrópicas, resultado en el efecto de birrefringencia.

- El efecto Pockels

Consiste en la rotación del plano de luz polarizada por su interacción con un campo eléctrico. El efecto Pockels únicamente se produce en cristales desprovistos de un centro de simetría, como el Litio Nobio Oxígeno y el Galio Arsénico.

Figura 38. **Estructura de un captador por efecto Pockels**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Los transformadores de voltaje ópticos se clasifican en tres tipos según los principios del efecto Pockels electroóptico, siendo estos el efecto Kerr y el efecto piezoeléctrico inverso.

El tipo de cristal electroóptico de transformador de voltaje óptico hace un uso completo del efecto Pockels para evaluar la medición de voltaje. El medio cristalino es isotrópico sin voltaje aplicado, pero se convierte en un cristal biaxial anisotrópico bajo el voltaje aplicado.

El efecto electroóptico de Pockels, cambia o produce birrefringencia en un medio óptico inducido por un campo eléctrico, la birrefringencia se deriva de cambios en el índice de refracción y el estado de polarización de la luz que pasa a través del cristal.

Los principales dispositivos ópticos incluyen un polarizador, una placa de onda $\lambda / 4$, un cristal electroóptico y un analizador. Entre ellos, el polarizador y el analizador se coloca en ambos extremos del sistema de ruta óptica para formar un sistema de detección de interferencia de polarización, que se utiliza para medir la diferencia de fase causada por el efecto electroóptico lineal en la ruta óptica.

Algunas características generales son las siguientes:

- La interface análoga de baja energía se encuentra en los siguientes rangos para protección.
- 0-200 mV y 0-2 V.
- La interface análoga de alta energía para medición es la siguiente: 0-1 A y 100 V.
- No existe ningún riesgo debido a secundarios en circuito abierto o por ferro resonancia.

- Mayor precisión con corrientes bajas.
- No tiene problemas de saturación.
- Funcionan tanto para AC como para DC.

3.2.1.3. Mergin Unit

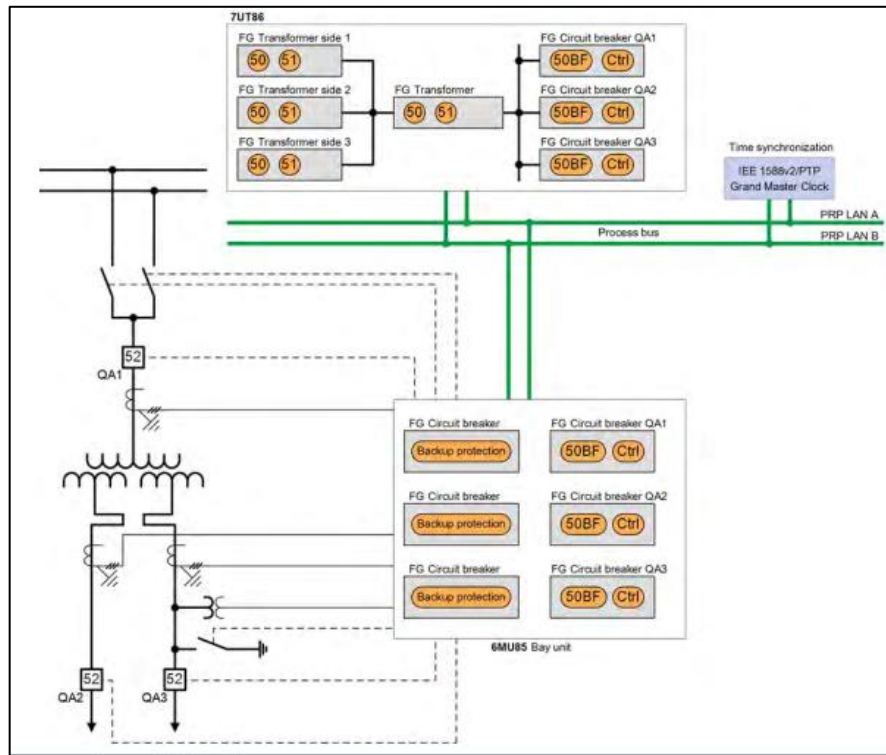
Dada la nueva tendencia para subestaciones digitales en cuanto a la migración de todos los equipos convencionales a equipos con funcionalidad totalmente digital, ventajas como el reemplazo complejo del cableado entre los niveles de patio y el nivel 1 de las subestaciones convencionales.

Las funciones principales es la digitalización de medidas y eventos, utilizando protocolos es posible la transmisión rápida de información por medio de GOOSE o Sampled Values, en una subestación digital se procura que la información proveniente de los transformadores de instrumentos sea enviada al bus de proceso por medio de Sampled Values.

La Mergin Unit es el elemento fundamental para conectar los transformadores de instrumentos convencionales u ópticos con los equipos de control, medición y protección, aportando una interfaz digital entre los equipos mencionados y creando un conjunto de muestras de magnitudes eléctricas.

La Mergin Unit implementa los nodos lógicos de los transformadores ópticos, cuidando y separando la información de los transformadores de tensión y de corriente en el modelo de datos, el convertidor de medio ubicado en los transformadores ópticos descrito en la sección anterior, envían la información hacia las Mergin Unit como se muestra en la figura 39.

Figura 39. Implementación de una Mergin Unit 6MU85



Fuente: SIEMENS. *SIPROTEC 5: protection, control, automation, monitoring, Power Quality – Basic*. p. 292.

Según el protocolo que utilice el enlace entre el transformador y la Mergin Unit, se podrá adaptar la Mergin Unit para que reciba los mensajes de la red y posteriormente sean convertidos al protocolo 61850 para enviarlo al bus de proceso en caso la subestación sea totalmente digital.

La utilidad de instalar una Mergin Unit en una subestación se basa en la norma que se haya implementado en los transformadores de instrumentos y los equipos que se tienen.

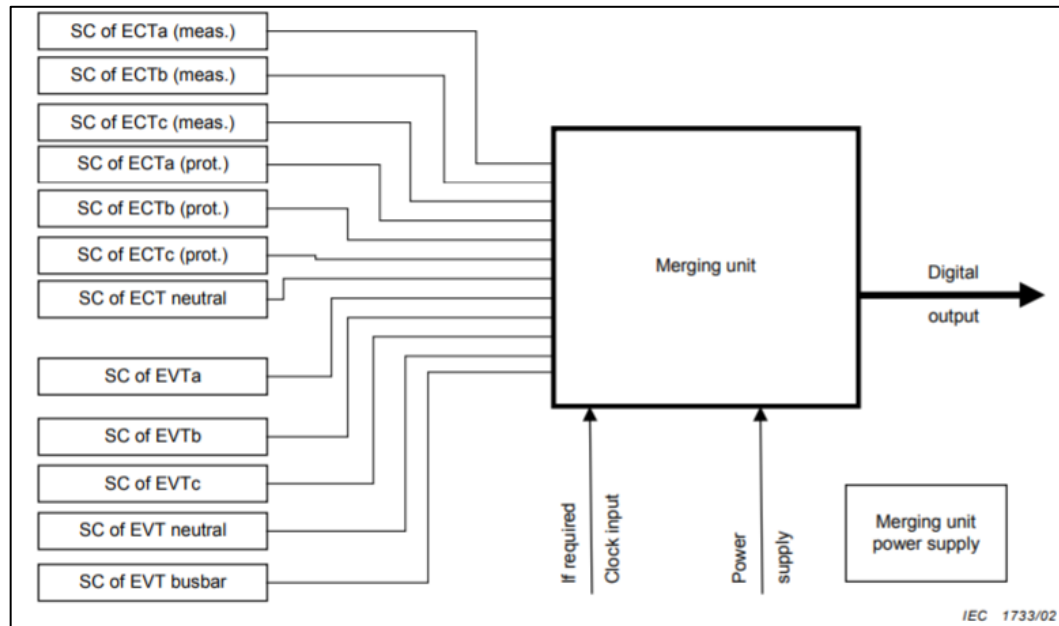
De acuerdo con la interfaz digital establecida en la norma IEC 60044-8, la Mergin Unit es de uso obligatorio. Según lo establece IEC 61850-9-2 no se necesita obligatoriamente una Mergin Unit, y el convertidor ubicado en el lado secundario utiliza una salida que cumpla la IEC 61850-9-2. La necesidad de implementar muestreo sincronizado y la existencia de una red de sincronización en la subestación hacen que el uso de una *Merging Unit* sea necesario.

La comunicación de las *Merging Unit* consiste en enviar señales síncronas a los transductores de voltaje y corriente, y los convertidores de analógico al digital se activan para llevar a cabo el muestreo, dependiendo del protocolo que los transductores utilicen enviarán los resultados de conversión a la *Merging Unit* por medio de fibra óptica, una vez el microprocesador de la *Merging Unit* finaliza con el proceso de decodificación se obtienen los valores muestreados y son transmitidos hacia la CPU, se empaquetan y se envían en el formato estándar de mensaje según IEC 61850 9-1.

Según esta misma norma, se pueden agrupar como máximo hasta cinco transformadores de tensión y siete transformadores de corriente utilizando una *Merging Unit*.

La entrada de reloj es del tipo síncrona y la salida digital debe cumplir los mensajes de los protocolos definidos en IEC 61850-9-1 o IEC 61850-9-2. Se muestra en la figura 40.

Figura 40. Entradas en una *Merging Unit*



Fuente: IEC60044-7. *Instrument transformer- Part 8: electronic current transformers*. p. 9.

Se pueden tener múltiples entradas en fibra óptica y la salida digital únicamente es una hacia los equipos ubicados en el bus de proceso.

3.2.1.4. Bus de proceso

El bus de proceso es una parte elemental de las subestaciones digitales, permite obtener toda la información analógica enviada por los equipos de patio a través de la *Merging Unit*, la función principal es comunicar datos de equipo primario al sistema de protección y control basado en IEC 61850-9-2, que se centra en el mapeo de servicios de comunicación específicos (SCSM), esta parte del estándar define la interoperabilidad entre dispositivos de los distintos fabricantes por la combinación de IEC 61850-7 e IEC 61850-6, determinando el

mapeo modelo de clase de valor muestreado (IEC 61850-7-2), a ISO/IEC 8802-3.

La IEC 61850-7 proporciona una descripción general de la arquitectura para la comunicación y las interacciones entre sistemas para la automatización de servicios públicos de energía, como dispositivos de protección, disyuntores, transformadores, hosts de subestaciones, entre otros.

En el bus de proceso todas las señales binarias y análogas son llevadas en el mismo bus, es independiente al bus de estación dada la funcionalidad en factor tiempo con la que deben contar los IEDs que se encargarán de la protección de las líneas o barras en la subestación.

La adquisición de datos puede darse de manera directa, por medio de fibra óptica, o bien, por una red Ethernet conformada por *switches* de comunicación y para que tenga dominio con el tiempo se necesitan GPS.

- Equipamiento de bus de proceso
 - Unidad de interfaz de Proceso (PIU)

Conformada por:

- *Merging Units* (MU)
- E/S Remotas (RIO)
- Enlace en el dominio de tiempo (TiDL)
- Instrumentos de Transformación Digitales (DIT)

- Instrumentos de transformación no convencionales NCIT

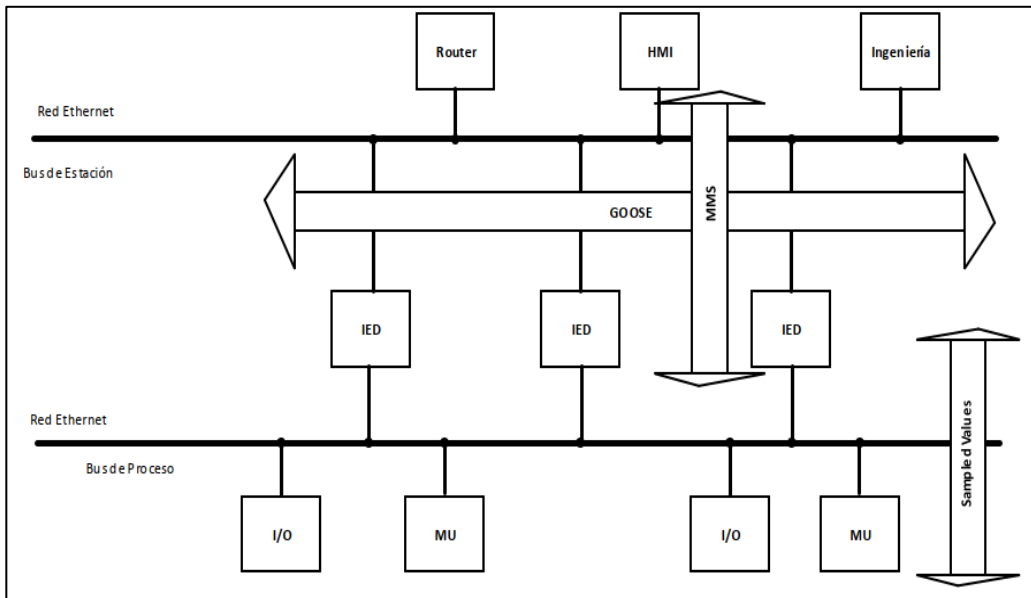
Dado que todos los equipos están conectados a la misma red dada la implementación en el mismo bus, es posible ahorrar la cantidad de equipos de protección que es necesario implementar, dado que los equipos pueden abarcar mayor cantidad de funciones.

Por cuestiones de ciberseguridad, el bus de proceso se separa del bus de estación, si por algún motivo se tiene acceso remoto al bus de estación, con la red independiente para el bus de proceso no se cuenta con acceso a la red de los equipos de control y protección.

Al contar con una configuración de bus para la red de los diversos equipos de control y medición, se encuentra el inconveniente de la saturación por el tráfico de la información, que es posible evitar por medio del enrutamiento por medio de VLAN.

El tipo de mensajería según la IEC 61850 en el bus de proceso, se define de la forma en que se muestra en la figura 41.

Figura 41. Mensajería según estándar IEC 61850



Fuente: elaboración propia, empleando Microsoft Visio 2016.

3.2.1.4.1. MMS

Por su significado *Manufacturing Messaging Specification*, es la mensajería que se intercambia entre jerarquías, entre los IEDs del Bus de Proceso y los equipos que se encuentran en el bus de Estación, están conformados por las RTUs, HMIs y *routers*.

Las características principales son las siguientes:

- Cuentan con menos restricción de tiempo crítico, por eso se utiliza para SCADA.

- La velocidad media de los mensajes es de 100 ms; lleva información de estado y valores de medición.
- La baja velocidad cuenta con las siguientes características para datos.
 - Cambios de configuración o parámetros (500 ms)
 - Transmisión del informe de eventos (500 ms)
 - Comandos de estación HMI (500 ms)
 - Archivos grandes (1 000 ms)

La arquitectura de cliente servidor para MMS se realiza de manera vertical, se cuenta con los equipos de diversos fabricantes.

Por lo que se pueden enviar funciones de control por medio del MMS, la idea es reemplazar o complementar las funciones del DNP 3.0, según aplique.

El cliente MMS puede obtener automáticamente el modelo de datos de jerarquía y los valores de IED. La autodescripción del MMS proporciona una lista de los datos y servicios disponibles, cada punto incluye el tipo de datos, la estructura de datos y un nombre comprensible.

3.2.1.4.2. GOOSE

Por sus siglas en inglés *Generic object oriented substation evento*.

Estos mensajes son intercambiados entre dos IEDs, ocupa el paquete Ethernet con 1 500 bytes. La transmisión de datos puede ser digital o analógica pero siempre entre equipos presentes en el bus de proceso, lo que implica una comunicación tipo horizontal con paquetes Ethernet 802.1p/802.1q etiquetados,

lo que da prioridad al tipo de mensaje que se está enviando, si es algún disparo que requiere atención inmediata en el tráfico de datos.

Dado que el bus de proceso está conformado por los arreglos de los *switch* de comunicación, todos los Goose son reenviados a todo lo que esté conectado al bus de proceso, por eso, el mensaje es tipo Multicast que permite enviar la información en tiempo real de eventos críticos de forma simultánea a todos los nodos de la red, y el ancho de banda no es constante.

En la comunicación de Multicast en la capa 2, las direcciones MAC desempeñan un papel importante para el direccionamiento y la identificación.

Se utilizan dos direcciones MAC en la comunicación, una dirección de multidifusión del mensaje GOOSE para suscripción en el destinatario y una dirección de origen del dispositivo remitente.

Una vez que las direcciones MAC del dispositivo se han asignado claramente a una interfaz de hardware, es posible que esta dirección de origen no se analice a nivel de aplicación en los dispositivos de destino con respecto a la ausencia de una reacción porque cambia cuando se intercambian los dispositivos de la parte remitente.

Esto también es necesario para facilitar las pruebas con dispositivos de simulación. Sin embargo, ya no es posible realizar una prueba para determinar si el interlocutor correcto ha enviado este GOOSE.

- Trama GOOSE

Cuentan con diversas características a considerar:

- Las tramas Goose cuentan con requisitos de tiempo estrictos, como son los mensajes rápidos en otras palabras los disparos y tienen que cumplir con 3 ms. Para comandos que son los mensajes sencillos, el tiempo es de 20 ms.
- Asignado directamente a la capa de enlace de datos.
- Tráfico solo dentro de LAN.
- No tiene dirección IP, es por esta razón que el mensaje GOOSE no es enrutable.

3.2.1.4.3. Sampled Values

Esta clase de dato se utiliza para representar muestras de valores analógicos instantáneos, este está creado para llevar medidas por muestreo entre 80 y 256 de cada señal analógica, se tiene que enviar un mensaje cada 208 μ S.

Se tiene un ancho de banda constante, se envían señales analógicas, específicamente voltajes y corrientes, a través de un muestreo.

La transmisión de Sampled Values mediante Multicast se basará en la configuración en el dispositivo productor. El intercambio de datos se basará en la asociación de aplicaciones de multidifusión. Para respaldar las capacidades de autodescripción, cualquier cliente puede leer los atributos de la instancia de control de valor muestreada.

Los clientes autorizados pueden modificar los atributos del control de valor muestreado.

3.2.2. Redundancia

Dada la información y funcionalidad que se maneja en el bus de estación es importante la rápida respuesta de los equipos por ello es necesario tomar en cuenta el estándar IEC62439-3 para el restablecimiento de la comunicación en caso de la falla en un equipo, para ello se consideran los protocolos de redundancia PRP y HSR.

La necesidad de tiempos de recuperación menores a 10 μ s, basados en capa 2, específicamente para SAS.

3.2.2.1. Tipos de redundancia

Dada la necesidad de tiempos de recuperación menores a 10 μ s, surge la implementación de los protocolos PRP y HSR, estos se describen en los siguientes incisos:

3.2.2.1.1. PRP

Un sistema que contenga implementado PRP cuenta con las siguientes características:

- Mínimo de dos LAN independientes
- El sistema es capaz de superar un solo fallo de red
- Recuperación de tiempo cero contra una falla en la red, dado el envío de la trama a las dos LAN.
- Requiere que los dispositivos finales sean un nodo con capacidad para doble conexión y que en cuestión de hardware contengan los puertos necesarios para PRP (DANP).

- Etiqueta adicional en el paquete en las LAN para identificar la duplicación.

Este protocolo implementa redundancia en los nodos, al enviar una trama en ambos puertos del DANP (*Doubly Attached Node implementing PRP*), de aquí que existirá un DANP fuente (emisor) y un DANP de destino (receptor).

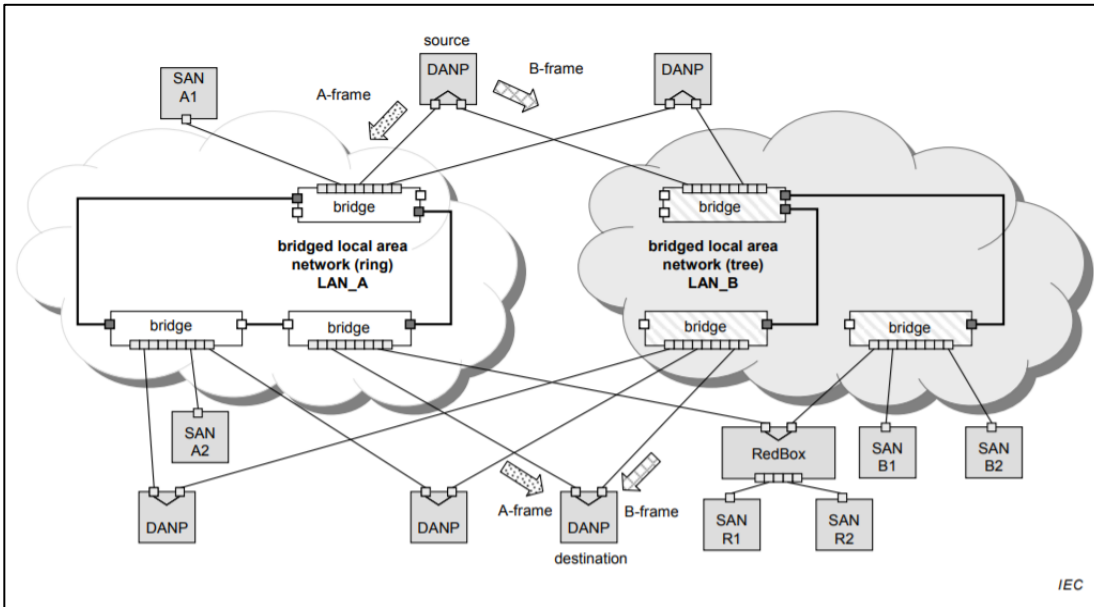
Un DANP es un dispositivo capaz de realizar un envío de datos, se conecta a dos redes de área local (LAN), independientes de topología similar, denominadas LAN A y LAN B, que operan en paralelo como se aprecia en la figura 42. Un DANP que actúa como fuente, envía la misma trama a ambas LAN y un DANP de destino lo recibe después que la trama ha pasado por ambas LAN dentro de un cierto tiempo, se asegura el envío de la trama y se descarta el duplicado al identificar que el mensaje ya ha llegado al DANP de destino por cualquiera de las dos LAN. En la figura se muestra una red redundante que consta de dos LAN, pueden tener cualquier topología.

Es por esta razón que el tiempo de recuperación se torna en cero, dado el envío de una misma trama por dos LAN independientes.

Es importante tomar en cuenta que para un equipo funciones para PRP, dicho elemento tenga disponibilidad para funcionar como tal, tiene que tener ambos puertos.

En caso se quieran integrar equipos que no están fabricados para funcionar como PRP, denominados como SAN en la figura 42, para evitar saturación de tráfico en la red, se implementan las RedBox (cajas redundantes que crean los dos puertos para cada SAN para luego enviar las tramas a cada LAN).

Figura 42. Esquema de configuración de PRP



Fuente: INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Industrial communication networks – high availability automation networks – Part 3: parallel redundancy protocol (PRP) and high – availability seamless redundancy (HSR). Standard IEC 62439-3. p. 14.*

Las dos LAN son idénticas en protocolo a nivel MAC-LLC, pero pueden diferir en rendimiento y topología. Los retrasos de transmisión también pueden ser diferentes, especialmente si una de las redes se reconfigura, por ejemplo, utilizando RSTP, para superar una falla interna.

Las dos LAN siguen reglas de configuración que permiten que los protocolos de administración de red, como el Protocolo de resolución de direcciones (ARP), y el Protocolo simple de administración de red (SNMP), funcionen correctamente.

Las dos LAN no tienen conexión entre ellas y se supone que son independientes de fallas. La redundancia se puede vencer por puntos únicos de falla, como una fuente de alimentación común o una conexión cuya falla derriba ambas redes.

Los equipos en PRP son los siguientes:

- Double Attached Node PRP (DANP), es un nodo doble de PRP
- Single Attached Node (SAN), es un nodo simple que no trabaja en PRP
- Redundancy Box (RedBox) es la caja redundante que convierte equipos simples a PRP.

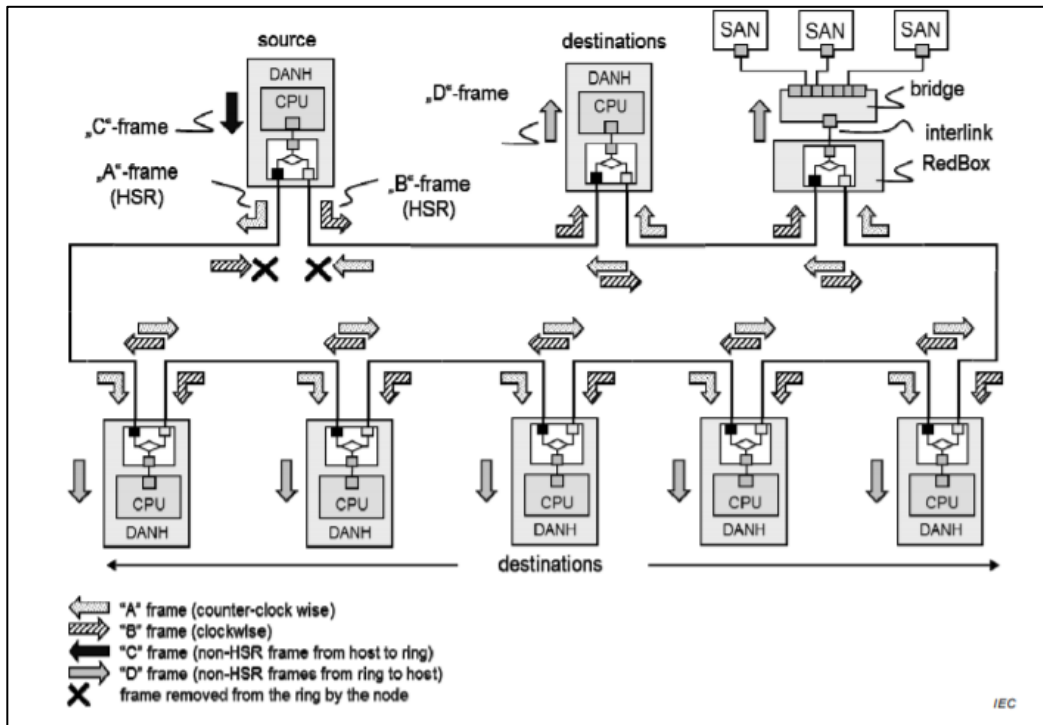
3.2.2.1.2. Principio de operación HSR

Funcionamiento básico con topología en anillo.

Como en PRP, un nodo tiene dos puertos operados en paralelo; y que para este caso se conoce como DANH (nodo doblemente adjunto con protocolo HSR). Esta configuración no es recomendada para Bus de Proceso, dado el alto tráfico que se genera en la red, ahora bien, para fines de explicación se dará detalle de la configuración; puede ser utilizada en subestaciones convencionales.

Una red HSR simple consta de nodos de puente doblemente conectados, cada uno con dos puertos de anillo, interconectados por enlaces full-duplex, como se muestra en el ejemplo de la figura 43 (Multicast), y la figura 44 (Unicast), para una topología de anillo.

Figura 43. Esquema de configuración de HSR para Multicast



Fuente: INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Industrial communication networks – high availability automation networks – Part 3: parallel redundancy protocol (PRP) and high – availability seamless redundancy (HSR). Standard IEC 62439-3. p. 34.*

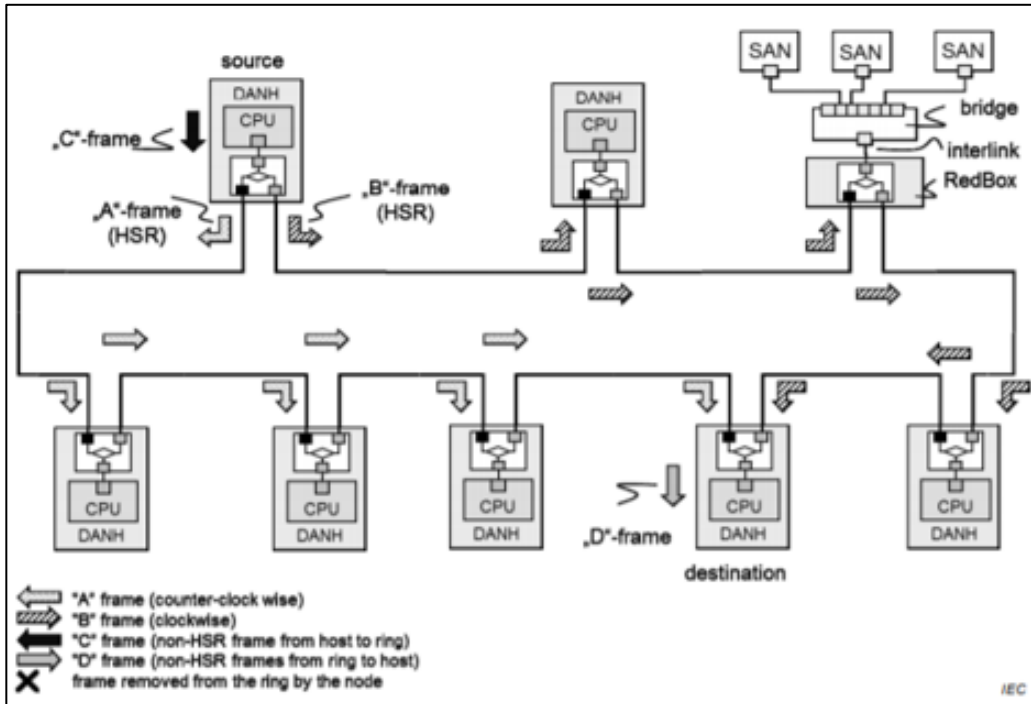
Una DANH de origen envía una trama pasada desde sus capas superiores (trama "C"), la antepone una etiqueta HSR para identificar las tramas duplicadas y envía la trama a través de cada puerto (trama "A" y trama "B"), en direcciones opuestas de la conexión en anillo.

Un DANH de destino recibe, en el estado libre de fallas, dos tramas idénticas de cada puerto dentro de un cierto intervalo, elimina la etiqueta HSR de la primera trama antes de pasarla a sus capas superiores (trama "D"), y descarta cualquier duplicado.

Los nodos admiten la funcionalidad de puente IEEE 802.1D y envían tramas de un puerto a otro, de acuerdo con cuatro reglas estipuladas en el estándar IEC 62439-3, siendo estos:

- Un nodo no enviará una trama ya introducida en el anillo o la malla
- Un nodo no reenviará una trama a un DANH de destino único (excepto para aplicaciones especiales como la supervisión de redundancia).
- Los DANH deben ser capaces a través de sus puertos de no enviar una trama que sea un duplicado de una trama que ya envió en esa misma dirección.
- Un puerto se abstendrá (opcionalmente) de enviar una trama que sea un duplicado de una trama que ya recibió de la dirección opuesta (excepto para las tramas de supervisión y temporización).

Figura 44. Esquema de configuración de HSR para Unicast



Fuente: INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Industrial communication networks – high availability automation networks – Part 3: parallel redundancy protocol (PRP) and high – availability seamless redundancy (HSR). Standard IEC 62439-3. p. 35.*

Las tramas que circulan en el anillo llevan la etiqueta HSR insertada por el DANH fuente, que contiene un número de secuencia para mantener el orden de las tramas. El doblete (dirección MAC de origen, número de secuencia), identifica de forma única copias de la misma trama.

La estructura a diferencia de PRP, presenta el inconveniente que no presenta *switches* de comunicación, de aquí que la falla de dos DANH en el anillo implicaría la pérdida de comunicación al destino.

Otro inconveniente es la capacidad de equipos que se pueden conectar, debido al tráfico de red que se pueda generar y evitar saturar las tarjetas de comunicación de los DANH.

Los equipos en PRP son:

- Double Attached Node HSR (DANH), es un nodo doble de HSR
- Single Attached Node (SAN), es un nodo simple que no trabaja en HSR
- Redundancy Box (RedBox) es la caja redundante que convierte equipos simples a HSR.
- QuadBox, permite interconectar dos redes HSR.

4. CASO DE SUBESTACIÓN DE 230/69 KV DEL SISTEMA NACIONAL INTERCONECTADO

4.1. Análisis causa raíz del problema

El presente análisis causa raíz, para efectos de la investigación de la implementación de Ciberseguridad en subestaciones eléctricas, se realiza por el método de Análisis causa y efecto de manera que se muestre lo mejor posible el caso para las subestaciones de transmisión del Sistema Nacional Interconectado de Guatemala.

El procedimiento indicado en el documento Procedimiento para el análisis causa raíz (acr), de fallas relevantes en equipos, accidentes e incidentes, ocurridos en las instalaciones de CFE, se utilizó como guía y propone varios métodos para realizar estudios de este tipo dependiendo de la naturaleza del evento que se requiere analizar. Para este caso de estudio se eligió el método de Análisis de Causa – Efecto, y tomando en cuenta que el principio establece que para cada efecto debe haber una causa, y esta última se debe convertir en el siguiente efecto.

El proceso básico es el siguiente:

- Identificar el último efecto o consecuencia
- Con base en la información disponible, determinar cuál fue la causa del mencionado efecto.

- Muestre cómo se establece la relación entre la causa y efecto.
- Repita los pasos b) y c), anteriores hasta llegar a una causa que si fuera eliminada prevendría la repetición del evento.

Tomando en cuenta lo anterior, se listan las siguientes consecuencias con sus respectivos efectos:

- Causa: las empresas de transmisión han desarrollado e implementado las tecnologías operativas (OT), de manera separada de la tecnología de la información (IT) derivado de la funcionalidad final de las mismas, dado que las OT continúan actualizándose tanto en hardware como en software y sus comunicaciones, de aquí que tienen a adaptarse a las IT. (Descrito en el documento artículo para el capítulo 1).
 - Efecto: las subestaciones del Sistema Nacional Interconectado operan sin las suficientes características de Ciberseguridad en las redes OT.
- Causa: a pesar de los distintos fabricantes de los IEDs como son SIEMENS y SEL, han adoptado normas de ciberseguridad en sus tecnologías más recientes, las empresas de transmisión por falta de cultura para la seguridad no han habilitado en su totalidad todas las configuraciones que los equipos han ido adquiriendo, incluso puede ser falta de orientación de los mismos fabricantes hacia los clientes.
 - Efecto: actualmente no se aprovechan todas las bondades que los equipos de control y protección brindan, esto porque no se

encuentran configuradas ciertas funciones esenciales que son recomendadas por el estándar IEEE 1686.

- Causa: falta de capacitación a personal de operación y administración derivado de la falta de cultura de seguridad que se ha manejado en el país, siendo el tema de seguridad muchas veces un segundo plano y como plano principal la funcionalidad del sistema. Impartiendo cursos donde se capacite al personal según el rol que desempeña en la empresa y enfatizado a las normas correspondientes y un plan de resiliencia.
 - Efecto: en términos generales para proteger el acceso físico a la subestación como tal y por consiguiente el acceso a los equipos de patio y tableros de control, protección y medida, el personal de operación mantenimiento y administración de las subestaciones no está tomando en cuenta en su totalidad todas las acciones a tomar indicadas en el estándar IEEE C. 37.240.

- Causa: dada la gestión de cambio, los softwares sin parches para los IEDs antiguos con sistemas operativos que ya no son compatibles con el fabricante.
 - Efecto: por las diferencias de funcionalidad y prioridad operacional y de información entre las tecnologías OT e IT, para IEDs antiguos existe alta probabilidad que los parches actuales ya no sean aplicables, afectando incluso actualizaciones de *firmware*, siendo el propio software de los equipos una de las mayores vulnerabilidades del sistema. El personal de Operación mantenimiento y administración de las subestaciones no tiene planes de actualización de software, firmare ni hardware.

- Causa: los protocolos que actualmente se utilizan en las redes LAN en su mayoría fueron diseñados para la eficiencia de la comunicación y no para ser protegido contra ataques, esto porque en su momento los fabricantes se enfocaban en la buena funcionalidad de los protocolos.
 - Efecto: el tráfico de información a través de los *switches* de comunicación de las redes LAN que conforman la comunicación entre los IEDs del nivel 1 de la subestación, actualmente no se envía por protocolos seguros.

- Causa: el abordaje de las nuevas implementaciones de tecnología como son el acceso a la red IT de la empresa de transmisión, no se ha tenido la precaución de definir los límites que un operador pueda tener desde la computadora de su casa o incluso desde su teléfono móvil, y la implementación y adecuada configuración de *firewall* y técnicas de autenticación y control de acceso basado en roles RBAC.
 - Efecto: muchos accesos por VPN (acceso remoto a una red), adquieren vulnerabilidad para las subestaciones y no se tiene controlado el número de dispositivos que pueden incluso realizar operaciones de equipos desde dispositivos móviles y no se cuenta con la seguridad de cifrado que estable el estándar IEEE C37.240 y limitar funciones de operación de mandos.

- Causa: la ciberseguridad inició implementándose únicamente para tecnologías IT con el fin de proteger únicamente la confidencialidad y seguridad de la información, dado que los requisitos para OT tienen diferentes requisitos de rendimiento y confiabilidad, a diferencia que los

sistemas IT pueden soportar cierto nivel de demora y fluctuación, y que las OT son críticas en cuanto al tiempo para dar respuestas en milisegundos.

- Efecto: la ciberseguridad comúnmente es aplicada de mejor manera a nivel 3 de subestaciones únicamente para proteger información empresarial y comercial y no se le da la adecuada protección a la red de equipos protección, monitoreo, control y en caso del equipo primario, de maniobra.
- Causa: tomando en cuenta la época en que se construyeron las subestaciones energizadas actualmente y dado que la implementación de la zona de seguridad en una subestación es una necesidad y medida de seguridad que actualmente ha tomado relevancia dadas las recientes amenazas cibernéticas consecuencia del desarrollo informático y de comunicación en equipos de OT e IT.
 - Efecto: falta de una adecuada zona segura en la subestación, hace que una subestación funcione sin comunicación desde la zona segura de la subestación hacia su Centro de Control Remoto, lo que muchas veces hace vulnerable la red que interconecta los puntos receptores entre los límites de la subestación punto de análisis con su Centro de Control; puede estar conectado con más subestaciones.
- Causa: falta de capacitación a personal de operación y administración derivado de la falta de cultura de seguridad que se ha manejado en el país, siendo el tema de seguridad muchas veces un segundo plano y como plano principal la funcionalidad del sistema. Impartiendo cursos donde se

capacite al personal según el rol que desempeña en la empresa y enfatizado a las normas correspondientes y un plan de resiliencia.

- Efecto: no se cuenta con un plan de respuestas o resiliencia para incidentes ocasionados por un intento de ciberataque.







Para implementar ciberseguridad de acuerdo con estándares IEEE, IEC o NERC CIP, se debe realizar una inversión económica dado que actualmente ninguna subestación construida cuenta totalmente con todos los requisitos recomendados en las normas correspondientes.

Dando seguimiento al método anterior, se realizó el diagrama de eventos y factores causales, y para este caso de estudio específico se obtienen los eventos principales después de analizar las causas y efectos de no aplicar correctamente ciberseguridad en subestaciones del SNI, derivándolos de los efectos secundarios (son eventos de ciberataques que han ocurrido en otros países), obteniendo de esta manera, un efecto final. Todos estos aspectos tienen su origen proponiendo “condiciones” y se originan las relaciones entre los eventos y el efecto final en el diagrama.

Es necesario aclarar que el objetivo de realizar el diagrama es establecer el factor causal del por qué no se ha implementado ciberseguridad en las subestaciones del SNI de manera completa y con base en lo que recomiendan las normas pertinentes.

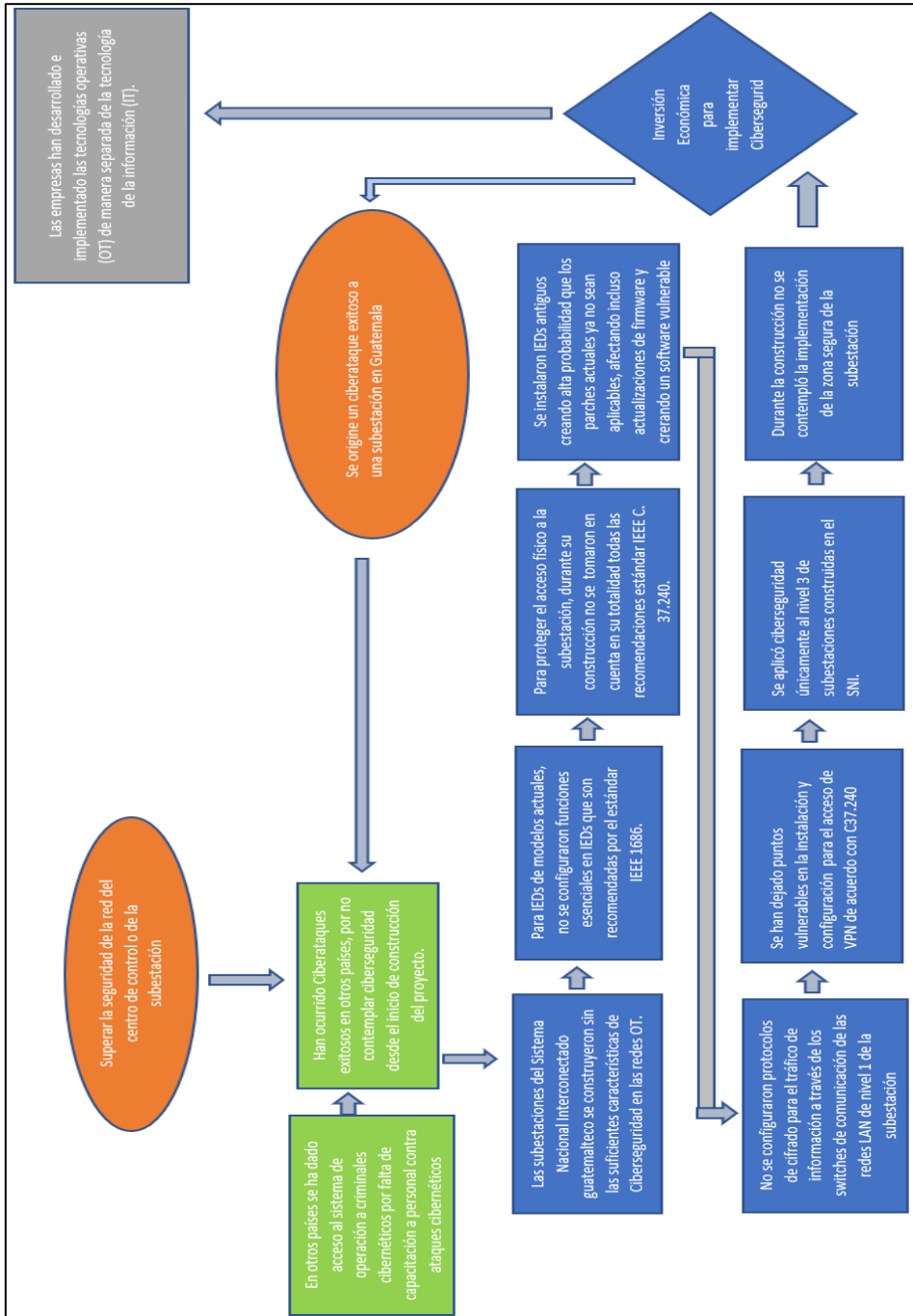
Las formas del diagrama que se deben tomar en cuenta son:

Tabla XI. **Formas para diagrama de eventos y factores causales**

Descripción	Símbolo
Evento principal	
Evento secundario	
Condición	
Factor causal del problema	
Efecto final	
Conectores de eventos y condiciones	

Fuente: elaboración propia.

Figura 45. Diagrama de eventos y factores causales



Fuente: elaboración propia.

4.2. Estudio de mercado

El presente estudio de mercado tiene como finalidad mostrar la variación del mercado eléctrico en Guatemala durante los últimos años y el vínculo que tiene el subsector de transmisión eléctrica con la variación del PIB.

Dado que el crecimiento económico de un país es un indicador confiable del aumento de consumo de energía; tomando en cuenta el producto interno bruto per cápita, se puede estimar si un habitante ha logrado, o no, un crecimiento económico y se ve reflejado en su consumo de energía.

De esta manera se puede estimar el crecimiento que tendrá el sector de transmisión y la economía en las empresas transmisoras. Este será un punto indicativo que podría aprovecharse para implementar Ciberseguridad en las subestaciones. Es necesario aclarar que este no es un factor determinante, pero que si refleja la situación económica del subsector eléctrico en Guatemala.

En la siguiente tabla se muestra la variación que ha tenido el PIB en los últimos años.

Tabla XII. **Variación del PIB de Guatemala durante el periodo 2014 al 2018**

Año/Descripción	2014	2015	2016	2017	2018
PIB nominal valores en millones de quetzales	447,326,30	476,022,80	502,001,70	526,200,40	549,790,00
Tasa de variación anual en porcentajes	7,40 %	6,40 %	5,50 %	4,80 %	4,50 %
PIB real	434 508,31	461 844,18	481 628,80	497 918,62	537 376,60
Tasa de inflación	2,95 %	3,07 %	4,23 %	5,68 %	2,31 %

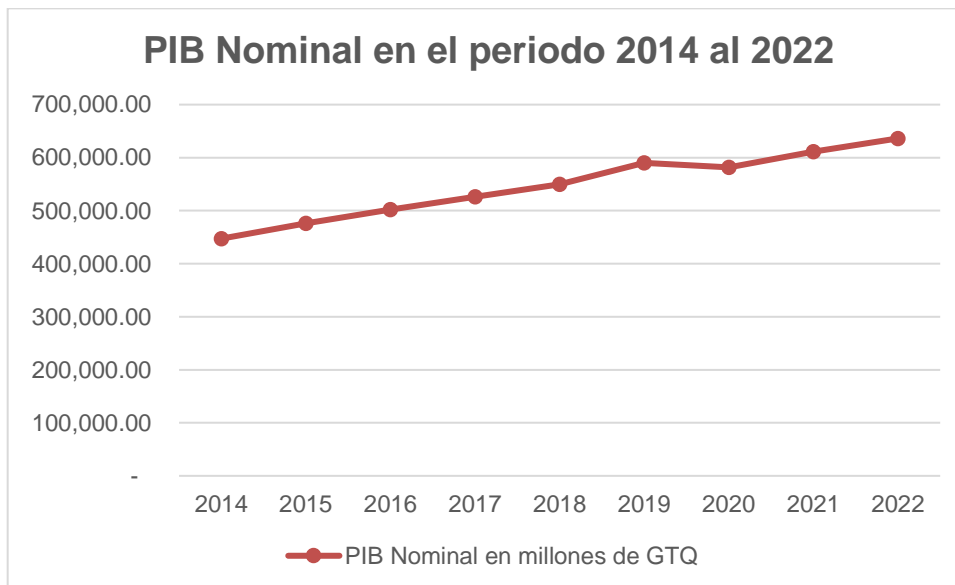
Fuente: elaboración propia.

Tabla XIII. **Variación del PIB de Guatemala durante el periodo 2019 al 2022**

Año/Descripción	2019	2020	2021	2022
PIB nominal valores en millones de quetzales	590 416,80	581 560,55	611 220,14	636 280,16
Tasa de variación anual en porcentajes	7,40 %	-1,50 %	5,10 %	4,10 %
PIB real	570 947,49	563 527,66	583 448,01	609 055,39
Tasa de inflación	3,41 %	3,20 %	4,76 %	4,47 %

Fuente: elaboración propia.

Figura 46. **Variación del PIB de Guatemala del año 2014 al 2022**



Fuente: elaboración propia.

Donde se aprecia un crecimiento en el PIB de cada año, con diversas tasas de variación anual siempre en aumento, únicamente para el año 2020 se observa una caída de -1,5 %, consecuencia de las medidas de prevención y contingencia

de la pandemia COVID-19, lo que afectó significativamente la economía en todas las categorías que conforman el PIB de Guatemala, a pesar de ello para el año 2021 se estima un crecimiento de 5,10 % y para el año 2022 un crecimiento de 4,10 %, resultado de la recuperación de la actividad económica.

El PIB de Guatemala se encuentra conformado por las siguientes actividades económicas:

- Agricultura, ganadería, silvicultura y pesca
- Explotación de minas y canteras
- Industrias manufactureras
- Suministro de electricidad, agua y saneamiento
- Construcción
- Comercio y reparación de vehículos
- Transporte y almacenamiento
- Actividades financieras y de seguros
- Actividades inmobiliarias
- Actividades de servicios administrativos y de apoyo
- Administración pública y defensa
- Enseñanza
- Salud
- Otras actividades de servicios

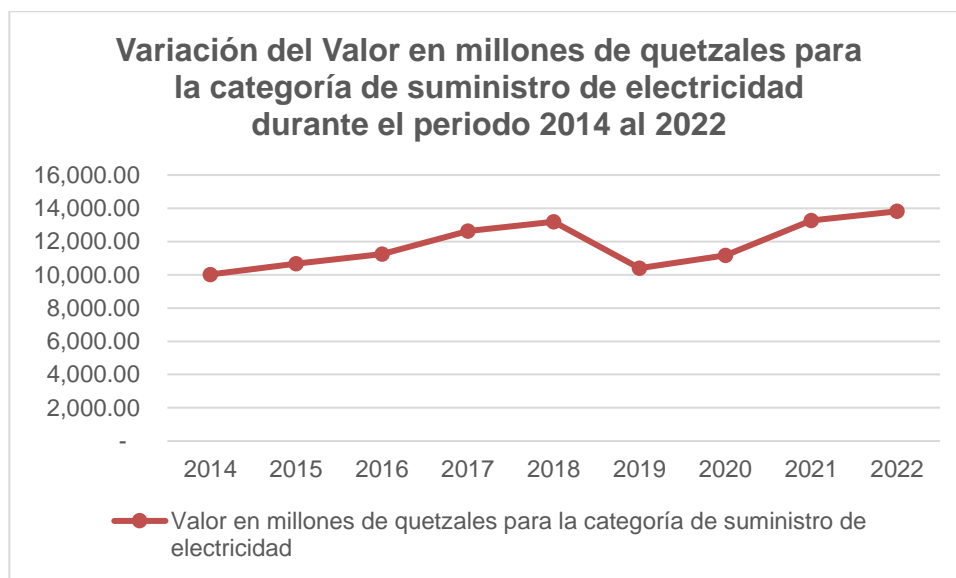
Y para los objetivos de esta investigación, los valores obtenidos en el PIB anual y los valores son elaborados por el método del origen de la producción. A partir del porcentaje que representa la categoría de Suministro de electricidad, agua y saneamiento, para cada año a partir del 2014, se sustrajo de fuentes directas del Banco de Guatemala el porcentaje de participación de esta categoría, como se muestra en la tabla XIV.

Tabla XIV. **Porcentaje de participación de la categoría de suministro de electricidad, agua y saneamiento en el PIB de Guatemala**

Año	Monto en millones de Quetzales	Porcentaje del PIB correspondiente a cada año	Valor en millones de Quetzales para la categoría de suministro de electricidad (80 % de la categoría)
2014	12 525,14	2,80 %	10 020,11
2015	13 328,64	2,80 %	10 662,91
2016	14 056,05	2,80 %	11 244,84
2017	15 786,01	3,00 %	12 628,81
2018	16 493,70	3,00 %	13 194,96
2019	12 989,17	2,20 %	10 391,34
2020	13 957,45	2,40 %	11 165,96
2021	16 590,26	2,71 %	13 272,21
2022	17 270,46	2,71 %	13 816,37

Fuente: elaboración propia.

Figura 47. **Variación en millones de GTQ de la categoría de suministro de electricidad en el periodo del año 2014 al 2022**



Fuente: elaboración propia.

Y de acuerdo con lo indicado por el Banco de Guatemala, que el suministro de electricidad representa el 80 % de su categoría, se procede a elaborar la columna Valor en millones de quetzales, para la categoría de suministro de electricidad, donde se puede apreciar que para los años de 2014 a 2018 se aprecia un crecimiento considerable con relación al aumento del PIB y del porcentaje que representa la categoría en cada año. Sin embargo, se aprecia un descenso de la actividad económica a partir del año 2019, derivado de las consecuencias del inicio de la pandemia, y su posterior recuperación a partir del año 2021.

Considerando lo anterior se espera tener un buen panorama económico para poder realizar inversiones en el subsector eléctrico de Guatemala, lo que incluye el subsector de transmisión; este es el objeto de estudio de este documento.

El mercado para el que está diseñado el presente estudio es para las subestaciones eléctricas propiedad de las empresas de Transmisión en Guatemala; tienen participación en el Sistema Nacional Interconectado, y que para fines prácticos y explicativos se tomarán únicamente las tres empresas tanto privadas como estatales que tienen mayor posesión longitud en kilómetros de líneas de transmisión.

El Ministerio de Energía y Minas realiza un estudio en el que incluye los niveles de Tensión de líneas de transmisión utilizados en el país, son de 400 kV, 230 kV, 138 kV, 69 kV, aunque los niveles de tensión más utilizados por mayoría en el total de subestaciones son de 230 y 69 kV, siendo ETCEE la que tiene mayor cantidad de activos de líneas de transmisión cubriendo un total de 3 189,88 km y siendo la única subestación de 400 kV es Los Brillantes, que es la

interconexión eléctrica entre Guatemala y México; sigue TRELEC, S.A. con 684,88 km y luego TRECESA con 418,97 km. como se indica en la tabla XV.

Tabla XV. **Longitud de líneas de transmisión, en kilómetros, por nivel de tensión y por tipo de propiedad, al mes de diciembre de 2018**

Tipo de Propiedad	Kilómetros de línea de transmisión (*)				
	400 kV	230 kV	138 kV	69 kV	TOTAL
Estatal					
Empresa de Transporte y Control de Energía Eléctrica del INDE.	71.15	464.95	367.09	2,286.69	3,189.88
Subtotal					3,189.88
Privada					
Transporte de Electricidad de Occidente.		132.20			132.20
Transportista Eléctrica Centroamericana, S.A.		64.36		620.52	684.88
Transmisora de Energía Renovable.		34.52			34.52
Empresa Propietaria de la Red.		284.50			284.50
Orazul Energy Guatemala Transco Ltda.		32.00			32.00
Redes Eléctricas de Centroamérica, S.A.				31.12	31.12
Transportadora de Energía de Centroamérica, S.A.		401.13		17.84	418.97
Transportes Eléctricos del Sur, S.A.		28.12			28.12
EBB Ingeniería y Servicios, S.A.		95.28			95.28
Transporte de Energía Eléctrica del Norte, S.A.		1.30		17.70	19.00
Subtotal					1,760.59
TOTAL					4,950.47

Fuente: MINISTERIO DE ENERGÍA Y MINAS. *Dirección General de Energía. Estadísticas subsector eléctrico 2018.* p. 6.

4.2.1. Empresas de transmisión

En los siguientes incisos se describen las diferentes empresas que prestan servicios de transmisión en Guatemala.

4.2.1.1. ETCEE-INDE

El Instituto Nacional de Electrificación INDE, es una entidad estatal, que desde el año 1,959 ha desempeñado diversos roles en el subsector eléctrico de Guatemala. En 1997 surge la Empresa de Transporte y Control de Energía Eléctrica ETCEE, como resultado de la separación de funciones internas del INDE, derivado de lo estipulado en la Ley General de Electricidad promulgada en 1996, donde establece que una entidad no puede ser generadora, transmisora y distribuidora al mismo tiempo. También se establece por el Decreto No. 64-94 del Congreso de la República, la autonomía de INDE.

ETCEE es la división de INDE cuya funcionalidad es la transmisión de energía eléctrica y es parte del SNI y participando en el subsector eléctrico nacional y en el mercado eléctrico regional.

ETCEE cuenta con 68 subestaciones de transmisión, estas tienen diversos niveles de tensión y tienen presencia de sus subestaciones en varios departamentos del país, siendo estos:

- Guatemala
- Escuintla
- Retalhuleu
- Huehuetenango
- Chimaltenango
- Quetzaltenango
- San Marcos
- Quiché
- Totonicapán
- Chiquimula

- Santa Rosa
- Alta Verapaz
- Baja Verapaz
- Izabal
- Jutiapa
- El Progreso
- Zacapa
- Petén
- Jalapa

Algunas de sus subestaciones más importantes son las siguientes:

- GUATE SUR

La subestación de transformación Guatemala Sur, cuya ubicación está en el departamento de Guatemala, tiene nivel de tensión es 230/69 kV, es un nodo muy importante para el país, esto porque muchas líneas de 230 kV provenientes del departamento de Escuintla, teniendo conexión con subestaciones de Guatemala, Escuintla, Chimaltenango y la subestación La Vega en Oriente.

- GUATE NORTE

Es una subestación de transformación, ubicada en el departamento de Guatemala tiene un nivel de tensión de 69 kV, tiene conexión con muchas líneas de distribución de EEGSA y alimenta a la subestación Sanarate.

- **GUATE ESTE**

Es una subestación de transformación con nivel de tensión de 230/69 kV, cuya capacidad actualmente es de 390 MVA. Cuenta con varias conexiones importantes con las Subestaciones Guatemala Norte, Guatemala Sur y San Antonio.

ETCEE cuenta con subestaciones encapsuladas en SF6 como Subestación Brillantes y Subestación Tactic.

4.2.2. TRELEC

La Empresa Transportista Eléctrica Centroamericana, S.A. -TRELEC-, es una empresa privada que forma parte del grupo EPM de Guatemala, el mismo grupo al que pertenece la Empresa Eléctrica de Guatemala, S.A. -EEGSA-. TRELEC se dedica al transporte de energía eléctrica, es una de las principales entidades transportistas. Fue creada en 1999 derivado de la separación de funciones establecida en la Ley General de Electricidad, esto porque inicialmente TRELEC formaba parte de EEGSA.

TRELEC tiene presencia en nueve departamentos, siendo estos:

- Guatemala
- Escuintla
- Sacatepéquez
- Suchitepéquez
- Santa Rosa
- Jutiapa
- Jalapa

- Zacapa
- Chiquimula

Ha desarrollado importantes proyectos de expansión como son los siguientes proyectos:

- Plan de Expansión de Transporte de energía, durante los años del 2010 al 2013.
- Plan de Expansión de Transporte, del 2013 al 2019.
- Plan de Expansión de Transmisión nacional PETNAC a partir de 2015.

Cada proyecto PET abarca distinta cantidad de subestaciones de transmisión. Dentro de los proyectos de PET, entre los más populares se encuentran:

Ampliación de subestaciones:

- TINCO de 69 kV
- Minerva 69 kV
- Ciudad Vieja 68 kV
- Monserrat 69 kV
- San Juan de Dios 69 kV

Entre otros proyectos se encuentran:

- Ampliación de subestación GIS Incienso
- Subestación Costa Linda
- Ampliación de la subestación Santa Isabel

Para el proyecto PETNAC, se tiene la siguiente información:

En 2015 el Ministerio Energía y Minas (MEM), adjudicó a TRELEC la construcción y ampliación de subestaciones y 160 km de líneas de transmisión.

En el PETNAC, es donde es permitido a Trelec ampliarse a nueve departamentos de Guatemala, el avance a la fecha es superior al 85 %, y contempla las siguientes subestaciones:

- Nueva Subestación Taxisco 69 kV, ubicada en Santa Rosa
- Ampliación Subestación Iztapa 69 kV, ubicada en Escuintla
- Nueva Subestación Guanagazapa 138 kV, ubicada en Santa Rosa
- Nueva Subestación Pasaco en 138 kV, ubicada en Santa Rosa
- Subestación Barberena 69 kV
- Ampliación de Subestación La Vega II 230/69 kV

También se han realizado otros proyectos como la construcción de la subestación Santa Isabel 230/69 kV, Guatemala Sur Santa Mónica 3 y 4.

Algunas subestaciones del PET 3, quienes inician en el año 2019, son las siguientes:

- Subestación Llano Largo 69/13,8 kV
- Subestación Santa Rosa 69/13,8 kV
- Subestación San Miguel Dueñas 69/13,8 kV
- Subestación La Castellana 69/13,8 kV

4.2.3. TRECSA

La Transportadora de Energía de Centroamérica S.A., es una entidad privada que pertenece al Grupo de Energía Bogotá (GEB), cuyas funciones son prestar servicios de operación y desarrollo de infraestructura de transporte de energía.

Dentro de sus principales proyectos se encuentran los siguientes:

- PET-01-2009

Su impacto y competitividad lo llevó a considerarse uno de los proyectos de infraestructura más importantes de Latinoamérica.

Por lo que con este proyecto se tienen los siguientes beneficios:

- En su momento existían diversas sobrecargas en el sistema de energía, la implementación del proyecto ayudó a evitar dichas sobrecargas y reducir vulnerabilidades.
- Dado que el proyecto evita que existan sobrecargas en el sistema nacional interconectado, se presenta un beneficio en la factura eléctrica nacional.
- Se considera una rebaja en el precio de la energía al implantar este proyecto, derivado de la diversificación de la matriz energética.

- Proyecto Anillo Pacífico Sur – APS

El diseño, construcción y energización del Anillo Pacífico Sur -APS a cargo de EEBIS, quien es filial del Grupo Energía Bogotá surgida desde 2011, significó para Guatemala la puesta en servicio al 100 % del primer proyecto completo e integral de transmisión de energía eléctrica, aprobado por la CNEE, realizado por iniciativa propia y que forma parte del Plan de Expansión del Sistema de Transporte 2012-2021.

Con este proyecto se mejora la confiabilidad del suministro de energía eléctrica a muchas regiones del país.

Las áreas del Centro, Occidente y Oriente del Sistema Nacional Interconectado obtienen diversos beneficios para recibir suministro de energía.

Cuenta con 97 kilómetros de líneas de transmisión, 4 construcciones de subestaciones nuevas y 1 ampliación de subestación.

- Proyecto Interfaz

- Se busca maximizar la infraestructura existente del PET-01-2009 para mejorar la calidad de la energía en Livingston y sus alrededores.
- Se conectará la demanda a la subestación y mejorará la percepción del usuario final respecto a la calidad del voltaje e interrupciones.
- Fortalece las oportunidades para la expansión de la electrificación rural y nuevos usuarios.

- Fortalece el sistema para exportar e importar energía eléctrica a Centroamérica, México y en un futuro a Belice.

4.2.4. Proveedores de equipos con requisitos de ciberseguridad

Los proveedores con mejor presencia el mercado guatemalteco y sus equipos cumplen de mejor manera con requisitos de ciberseguridad según lo estipulado en las IEEE1686 e IEEE C37.240 son las siguientes:

4.2.4.1. SIEMENS

Siemens es una empresa de origen alemán fundada en octubre de 1847, tiene alcance en múltiples áreas de la ingeniería eléctrica, en la fabricación de máquinas eléctricas, equipos de protección control y medición, digitalización, ingeniería de centrales generadoras, subestaciones eléctricas, para alta, media y equipos en baja tensión, es uno de los mayores productores del mundo de tecnología de eficiencia energética y adquiriendo renombre de la marca en otros ámbitos industriales.

Es fabricante de equipos de protección y tienen múltiples beneficios tecnológicos, siendo confiables y de buena calidad, y que actualmente son fabricados cumpliendo con características importantes de ciberseguridad cumpliendo con normas IEEE 1686 e IEEE C37.240 y NERC CIP.

Entre los equipos para subestaciones objeto de estudio de ciberseguridad, se encuentran los siguientes:

- Relevadores de protección Siprotec 4 y Siprotec 5

- Fabricación y diseño de tableros de protección
- Medidores multifuncionales de la familia SICAM
- RTUs de la familia SICAM y HMIs de la familia SIMATIC
- Computadoras industriales de la familia SIMATIC
- *Switches* de comunicación de la familia Ruggedcom, pueden ser de igual manera *routers* y *firewall*.

4.2.4.2. SEL

Schweitzer Engineering Laboratories es una empresa de origen estadounidense fundada en 1982. Es fabricante de productos en distintas áreas de ingeniería eléctrica e industria energética, tiene presencia en varios países. Sus productos están enfocados en normas ANSI/IEEE y que para fines de seguridad están enfocados en NERC CIP.

Entre los equipos para subestaciones objeto de estudio de ciberseguridad, se encuentran:

- Relevadores de protección
- RTUs y HMIs
- Computadoras industriales
- *Switches* de comunicación, pueden ser de igual manera *routers* y *firewall*

4.3. Estudio técnico

Con la finalidad de proteger la confidencialidad y privacidad de la información y posesión de activos que poseen las empresas transportistas del Sistema Nacional Interconectado, se presenta un caso de subestación supuesto, derivado de las marcas más populares y utilizadas en el país para la

implementación de equipos en subestaciones. Por ese motivo, se suponen estas premisas:

- Subestación de transmisión de 69 kV

Conformada por los siguientes equipos:

- Nivel 1

Configuración de la subestación: barra simple de 69 kV; tiene dos bahías de línea, con tablero de protección con:

- Tablero 1:
 - ✓ Un (1) relevador SIPROTEC 4 (7SD52)
 - ✓ Un (1) relevador SIPROTEC 5 (7SL87)
- Tablero 2:
 - ✓ Un (1) relevador SEL 411L
 - ✓ Un (1) relevador SEL 311L

Bahía de transformación, con tablero de protección con:

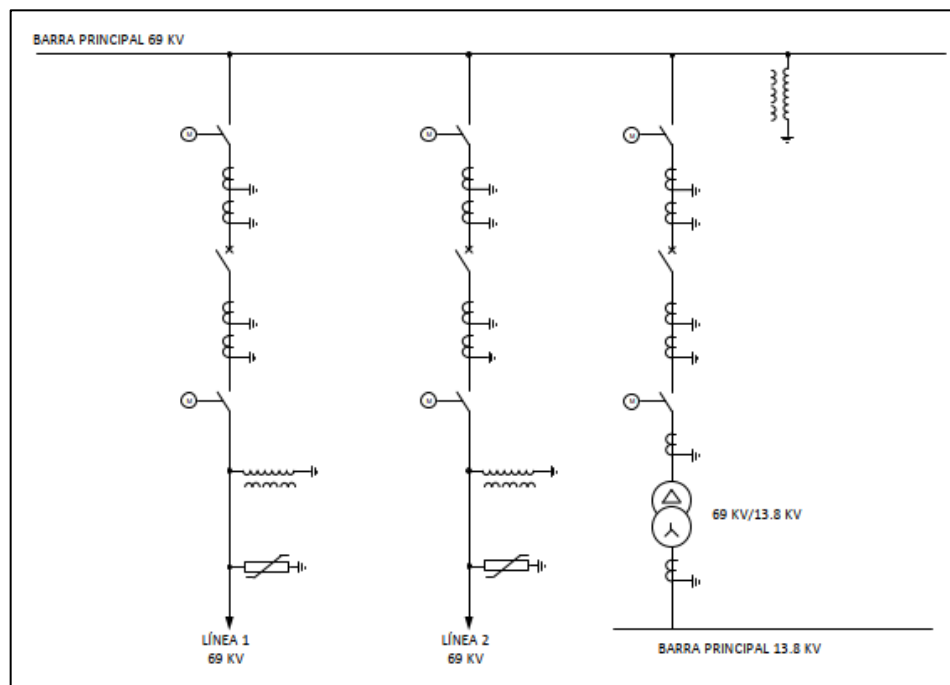
- Dos (2) relevadores SIPROTEC 5, 7UT85 para protección principal y de respaldo.

Una red LAN conformada por dos *switches* de comunicación marca Ruggedcom RSG2100 con puertos Ethernet, en configuración de anillo para hacer un sistema redundante.

- Nivel 2:
 - RTU SICAM PAS
 - HMI marca SIMATIC
 - *Switch* Ruggedcom RX 1 500: Con función de *switch*, Router y *firewall*.

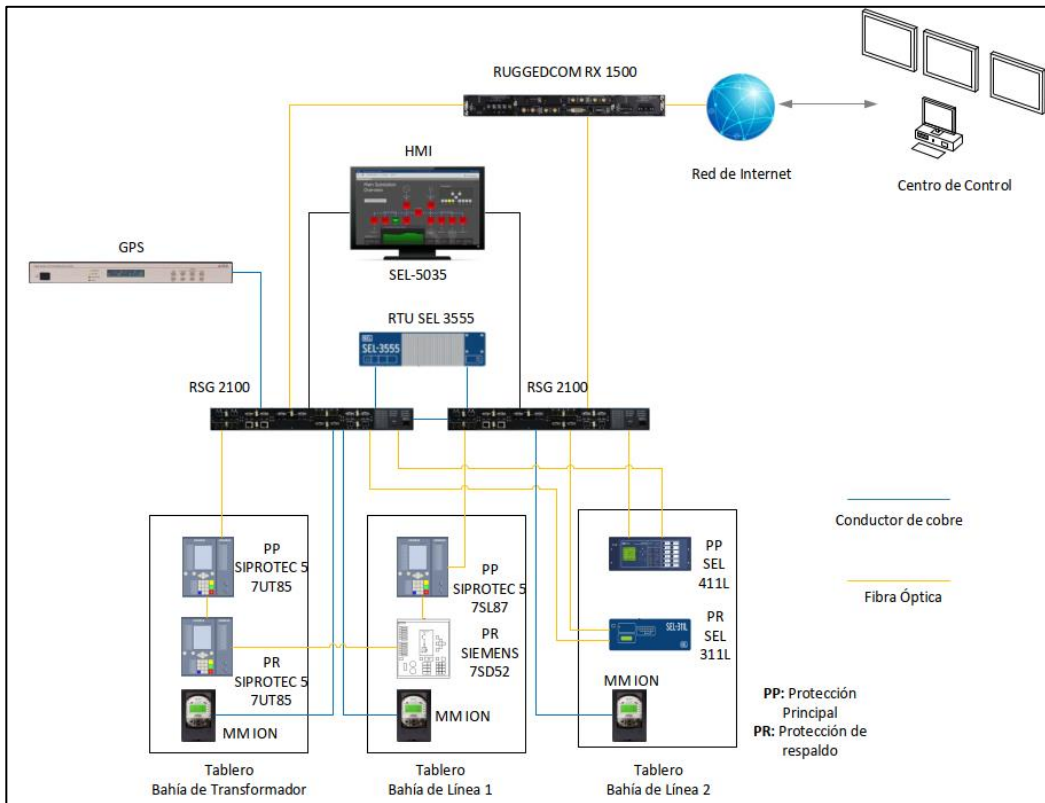
- Nivel 3:
 - Servidores
 - Red LAN
 - Router

Figura 48. **Diagrama unifilar de subestación**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Figura 49. **Arquitectura de comunicación de subestación**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

- **Vulnerabilidades en la subestación**

Según la norma IEEE C37.240, existe una cantidad considerable de vulnerabilidades en una subestación, cada una de ellas puede abarcar varios niveles de mando, o bien puede ser específicamente para un dispositivo, protocolo de comunicación, red específicamente de un nivel. En seguida, se mencionan vulnerabilidades en todos los niveles.

4.3.1. Vulnerabilidades para nivel 0 (equipos de patio)

Respecto a nivel de patio, se pueden dar diversas vulnerabilidades en cuanto a acceso no deseado a equipo primario, algunas buenas prácticas se encuentran indicadas en el estándar IEEE 1402, y de las más frecuentes en las subestaciones se tienen:

- Para el acceso a patio, una vulnerabilidad de seguridad frecuente es falta de mantenimiento a las cerraduras que ya no se encuentren en buen estado, tales como la cerca que permite el acceso directo a los equipos primarios.
- Mantenimiento al tablero de mando de los interruptores de potencia, para evitar un accionamiento manual directo.
- Falta de utilización de candados del tipo llave no reproducible.
- Falta de implementación de sensores de movimiento en los puntos de posible acceso a las instalaciones, como lo son puertas principales, puertas traseras y de emergencia, portones para el acceso vehicular.
- Un sistema de cámaras para videovigilancia que cubra la totalidad de la subestación, tanto en patio, y principalmente en todos los posibles puntos de acceso, como en el interior de la caseta de control y en caso de tener instalaciones para mando y monitoreo.
- Mantenimiento a cerraduras y buen estado de la puerta a la caseta de control para evitar cualquier tipo de acceso a los tableros de protección y control, y dispositivos importantes que son los relevadores de protección y

los *switches* de comunicación de donde se podrían extraer información crítica como certificados, claves, entre otros, o incluso reprogramar los equipos.

- El diseño de los tableros de control, protección y medición, al igual que los tableros de control y monitoreo deben tener cierre con llave, y de igual manera mantener el tablero cerrado con llave.

4.3.2. Vulnerabilidades para el nivel de automatización (nivel 1)

Para el nivel 1 las vulnerabilidades se encuentran en los IED's, y se hace énfasis en estos dispositivos.

4.3.2.1. Vulnerabilidades que aplican a IED's

Las vulnerabilidades de los IED's se mencionan enfocadas a los relevadores de protección como se indica en la sección 4.3.2.1.1. y 4.3.2.1.2. de acuerdo con las normas correspondientes.

4.3.2.1.1. Relevadores de protección

Las siguientes características son mencionadas de acuerdo con las vulnerabilidades encontradas en los relevadores de protección marca SIEMENS y SEL y de acuerdo con las normas IEEE 1686 e IEEE C37.240.

- A nivel general no se cuenta con una buena administración del control de acceso basado en roles, y no se aprovechan las bondades de restricción de acceso al uso de información de acuerdo con las características de cada usuario.

- Falta de una adecuada protección de datos en reposo en los relevadores: los dispositivos de protección suelen manejar archivos en diversos formatos para la configuración de parámetros de protección, de oscilografías, de estampa de tiempo, reportes de eventos, entre otros (en ocasiones los usuarios que tienen acceso a los IEDs), por diversos motivos, se tiende a guardar en memoria externa dichos resultados evitando proteger el acceso a la información de cualquier persona que tenga en su dominio el dispositivo, o bien, al no proteger adecuadamente la computadora que se utiliza para parametrizar, utilizando una contraseña sólida o el extravío de la misma.
- Falta de la implementación adecuada para el bloqueo de autenticación de usuarios, tomando en cuenta el escenario de que algún usuario no autorizado tenga acceso físicamente al IED o bien, al software y pretenda acceder a las funciones del dispositivo.
- Los dispositivos poseerán la sesión de autenticación de usuario, idealmente tendría que estar apoyado de un sistema PKI para que el acceso sea autorizado mediante contraseña y verificación de usuario cuando se requiere acceder al dispositivo mediante una PC con el software propio del dispositivo.
- Los procedimientos requerirán que el usuario que haya iniciado sesión, posterior a realizar los trabajos de parametrización en el dispositivo, éste “cierre la sesión” en un tiempo no demasiado prolongado cuando haya terminado para mantener la seguridad y evitar de esta manera que una persona no autorizada utilice el mismo acceso.

- No existe una buena gestión o administración de claves para enviar y recibir datos cifrados entre equipos.
- Para fines de autenticación, no se cuenta con ninguna de las opciones de llave que proporciona el estándar IEEE C.37.240.
- Para fines de auditoría, el propietario de la subestación no maneja directamente una lista de usuarios con acceso a los dispositivos, con los datos necesarios para la identificación en caso de algún acceso no autorizado.
- Los relevadores como tarea principal deben manejar registros con información esencial del acceso de los usuarios que acceden a la parametrización.
- La gestión de contraseñas sobrepasa el periodo recomendado de 12 meses.
- Al menos la cantidad de 4 roles de usuario en los IEDs, dado que se manejan 3 roles de usuario en los equipos actuales.
- Para fines de auditoría, no se encuentra correctamente monitoreada la actualización de *firmware* de los dispositivos.
- Se debe corregir el tipo de memoria para fines de control de pista de auditoría, y se debe implementar memoria intermedia circular secuencial.

- Equipos SEL no indica que su ciberseguridad se base con la tabla de cumplimiento del estándar IEEE 1686.
- Para diversos medios de comunicación con conexiones a los IEDs de la subestación, no están realizados por medio del acceso remoto al IED por *Gateway RIAG (Remote IED Access Gateway)*.
- No cuenta con el apoyo de la gestión de configuración de dispositivo, el almacenamiento de configuración y la operación de *sotware/firmware* para backup.

4.3.2.1.2. Vulnerabilidades específicas según estándar IEEE 1686 de los relevadores de protección propuestos en el diseño de la subestación caso de estudio

Las vulnerabilidades para los relevadores SIEMENS y SEL se obtuvieron posteriormente del análisis de las tablas XX, XXI y XXII contenidas en la sección de apéndices del presente estudio, siendo estos:

- Marca SIEMENS
 - SIPROTEC 5
 - En la configuración de alarmas para detectar actividades no autorizadas, se deben configurar en campo estas funciones:
 - ✓ Intento de uso de software no autorizado

- ✓ Señal de tiempo fuera de tolerancia
- ✓ Cambios de hardware de campo no válidos

- Para la agrupación de eventos y alarmas, el estándar propone que el dispositivo cumpla con un grupo de eventos y alarmas, de aquí que en sitio debe configurarse esta opción.

- Se debe configurar en sitio el control permisivo de supervisión.

- Se debe configurar en sitio, la cantidad mínima de cuatro roles definidos por el usuario como indicado en el estándar IEEE 1686.

- Respecto a las características criptográficas.
 - ✓ El estándar 1686 propone que la transferencia de archivos sea por medio de protocolo SFTP, ahora bien, el dispositivo realiza dicha acción mediante HTTPS.
 - ✓ Siprotec 5 no admite comunicación orientada al texto.
 - ✓ Siprotec 5 no admite ninguna función de tunelización.

- Respecto a técnicas criptográficas, Siprotec 5 no se admiten estas funciones:
 - ✓ Funciones de derivación clave
 - ✓ Generación de números aleatorios

- Respecto a la encriptación de comunicación serial, Siprotec 5 no admite la comunicación en serie para acceso remoto.
 - Los puertos de comunicación, físicos y lógicos que no se estén utilizando, se debe realizar la configuración en sitio para deshabilitarlos.
- Marca SIEMENS
 - SIPROTEC 4
 - Se debe configurar en sitio, la opción para que se puedan admitir como mínimo 10 usuarios individuales para tener acceso al dispositivo.
 - Se debe configurar en sitio, la cantidad mínima de cuatro roles definidos por el usuario como indicado en el estándar IEEE 1686.
 - Se deben configurar en sitio los siguientes eventos para el seguimiento de auditoría:
 - ✓ Configuración de acceso
 - ✓ Cambio de configuración
 - ✓ Acceso al registro de auditoría
 - ✓ Hora/cambio de fecha
 - Estos tipos de eventos no son admitidos por Siprotec 4 para el seguimiento de auditoría:

- ✓ Cierre de sesión manual
- ✓ Cierre de sesión programado

- Para la funcionalidad de supervisión y control de supervisión, estas opciones no se encuentran disponibles:
 - ✓ Grupos de eventos y alarmas
 - ✓ Control permisivo de supervisión
 - ✓ Alarmas que apliquen

- Configuración en sitio de las siguientes alarmas
 - ✓ Intento de uso de software de configuración no autorizado.
 - ✓ Configuración inválida o descarga de *firmware*
 - ✓ Señal de tiempo fuera de tolerancia
 - ✓ Cambios de hardware de campo no válidos.

- Para funciones de ciberseguridad, Siprotec 4 no admite la gestión de red SNMP versión 3.

- Respecto a las características criptográficas.
 - ✓ El estándar 1686 propone que la transferencia de archivos sea por medio de protocolo SFP, empero, el dispositivo realiza dicha acción mediante HTTPS.
 - ✓ Siprotec 4 no admite comunicación orientada al texto.
 - ✓ Siprotec 4 no admite ninguna función de tunelización.

- Para funciones criptográficas de Siprotec 4, no se admite lo siguiente:
 - ✓ La función de transferencia de archivos no es compatible.
 - ✓ Función de derivación clave.
 - ✓ Generación de números aleatorios.

 - Respecto a la encriptación de comunicación serial, Siprotec 4 no admite la comunicación en serie para acceso remoto.

 - Respecto a la configuración del software, DIGSI 4, para realizar cambios de datos de configuración.

 - La función de seguimiento de cambios actualmente no se encuentra soportada.

 - Se debe realizar la configuración en sitio para las descargas en el IED.

 - Los puertos de comunicación, físicos y lógicos que no se estén utilizando, se debe realizar la configuración en sitio para deshabilitarlos.
- Marca SEL 411L
 - No está configurado el mínimo número de usuarios que solicita el estándar IEEE1686.

- No está configurado adecuadamente el control de acceso basado en roles RBAC.
- No están configuradas las siguientes funciones de seguridad.
 - Cambio de *firmware*
 - Gestión de contraseñas
- Los próximos eventos de seguimiento de auditoría, no están disponibles en el dispositivo.
 - Cierre de sesión manual
 - Cierre de sesión programado
- No está configurada la función de eliminación de contraseña para el seguimiento de auditoría.
- Configuración en sitio de las siguientes alarmas:
 - Configuración no autorizada o archivo de *firmware*
 - Cambios de hardware de campo no válidos
- Para las características criptográficas, se deben configurar las próximas funciones:
 - Comunicación por SSH
 - Implementación de SNMP versión 3
- Respecto a las características criptográficas.

- No admite comunicación orientada al texto
 - No admite ninguna función de tunelización
- Respecto a la encriptación de comunicación serial, Siprotec 4 no admite la comunicación en serie para acceso remoto.
- No admite firma digital para la actualización de software de configuración/programación.
- No admite las combinaciones de contraseñas sugeridas por el estándar IEEE 1686 para la configuración de software.
- Los puertos de comunicación, físicos y lógicos que no se estén utilizando, se debe realizar la configuración en sitio para deshabilitarlos.
- El aseguramiento de la calidad de *firmware* no está soportado de acuerdo con el estándar IEEE C37.231, como lo sugiere IEEE 1686.
- Medidor multifuncional
 - Configuración correcta para la autenticación de usuarios
 - Falta la configuración de bloqueos de cuentas de usuario configurables con el número de intentos de inicio de sesión fallidos.
 - Actualmente el control de uso se utiliza para restringir las acciones permitidas al uso autorizado del sistema de control.

- Los supervisores pueden anular las autorizaciones de los usuarios eliminando su cuenta.
- Cambio de la contraseña predeterminada y gestión y administración periódica de contraseñas.
- Falta de la correcta configuración de la menor funcionalidad para prohibir y restringir el uso de funciones, puertos, protocolos y / o servicios innecesarios.
- El bloqueo de sesión se usa para requerir el inicio de sesión después de un período de inactividad para SFTP, SSH y la pantalla, pero no para el protocolo ION.
- No se están auditando los registros de eventos para identificar los cambios en la configuración del medidor y los eventos del sistema de gestión de energía.
- No se está realizando la auditoría periódica para la comunicación de la capacidad de almacenamiento de registros para notificar a un usuario cuando se acerca el umbral.
- Audite la capacidad de almacenamiento de 5 000 registros de eventos de forma predeterminada y métodos alternativos para la gestión de registros.
- Para la defensa en profundidad, se requiere una mejora en la segmentación de la red de comunicación, de tal manera que:

- Se segmente físicamente las redes del sistema de control de las redes del sistema sin control.
- Se segmente físicamente las redes de sistemas de control críticos de las redes de sistemas de control no críticos.
- ION, Modbus, DNP, DLMS, IEC 61850 y algunos protocolos de TI no son seguros. El dispositivo no tiene la capacidad de transmitir datos encriptados usando estos protocolos.

4.3.3. Vulnerabilidades para el nivel de estación (nivel 2)

Vulnerabilidades presentes en la zona segura:

- Implementación de todo el tráfico de datos desde la LAN hacia el bus de estación de manera que pase por el *firewall*.
- Los *routers* de la red no implementan protocolo de resolución de acceso proxy (ARP) y ocultar las direcciones IP de LAN de la subestación.
- No se encuentra instalado un buen sistema de detección de intrusiones (IDS) para monitorear el tráfico de la red en el *router*.
- Falta de requerimientos de Router usados en las LAN de la subestación según IEEE C37.240 en cuanto a proporcionar los niveles de seguridad de autenticación, configuración, y configuración de VLAN, como es mencionado para los puertos LAN.

- Falta de la correcta Protección de datos en movimiento según IEEE C37.240.
- Falta de una adecuada implementación de zona DMZ en el nivel de estación de la estación.
- Falta de implementación de acceso basado en roles para todos los usuarios en el nivel 2.
- Falta de la correcta segmentación de red en los dispositivos de la zona segura del bus de estación.

A continuación, se listan vulnerabilidades para cada equipo que conforma el nivel de estación.

4.3.3.1. *Switch* de comunicación

Para este dispositivo de comunicación, se han detectado posibles puntos vulnerables de acuerdo con las características técnicas que se mencionan en el manual de configuración del equipo RSG2100 de la marca Ruggedcom, indicado en la bibliografía con el número 57, y se hace mención de lo siguiente:

- No presenta la adecuada autenticación de dispositivos o usuarios que se conecten a sus puertos antes de permitir que el dispositivo o usuario se comunique en la red.
 - No se reemplazaron las contraseñas predeterminadas en el *switch*, y es necesario que se cambien, dado que dichas contraseñas son genéricas y puede tenerse acceso a los procesos.

- No se utilizan contraseñas con los requerimientos mínimos para una contraseña segura.
- Las contraseñas suelen reutilizarse.
- Las contraseñas se anotan y almacenan en archivo editable no encriptado.
- Se debe generar un certificado SSL personalizado y dos o más claves de host SSH antes de la puesta en servicio del dispositivo.
- En necesario que se aseguren los diversos canales donde se realizan actualizaciones de manera remota, dado que es necesario realizar autenticación del RADIUS.
- No se utiliza la autenticación de clave pública SSH.
- No está configurada la opción para el cifrado web de SSH/SSL para el tráfico de información en la red LAN.
- No se encuentra habilitado el protocolo SNMPv3 como protocolo oficial de la circulación de toda la información que sale del dispositivo.
- Suele utilizarse el PAP (protocolo de autenticación de contraseña), en entornos que no son seguros. Se debe tomar en cuenta que éste no se considera un protocolo seguro y se desea utilizar se debe utilizar en un entorno seguro de la red.

- Otra vulnerabilidad respecto a los protocolos que interactúan en la capa 2 (de enlace) que no tienen dentro de sus facultades otorgar ninguna autenticación inherente entre puntos finales, como ARP en IPv4, DAD en IPv6 y Wi-Fi en redes inalámbricas, dado que es posible llevar a cabo un ataque a los dispositivos conectados a la red de capa 2, interceptando el tráfico en la misma.
- Configurar adecuadamente el rol de los puertos en MSTP para fines de redundancia.
- Se deben filtrar las tramas de Broadcast, por medio de un umbral definido por el usuario para evitar las conocidas tormentas de Broadcast, para evitar saturación en la red y provocar inconvenientes en el funcionamiento de IEDs por mala comunicación.
- En la red de comunicación de la subestación, actualmente se da muy poco uso a la segregación de redes por medio de VLAN; un uso correcto para configurar las LAN virtuales, (VLAN), para segregar el tráfico de la red y aislar por partes la red LAN, y limitar del dominio de difusión, esta brindará una mayor protección contra efectos de ataques contra la continuidad del servicio.
- No se utiliza adecuadamente la función para habilitar o deshabilitar los puertos de comunicación, para evitar que los puertos innecesariamente habilitados puedan utilizar para obtener acceso a la red.
- Para el acceso físico y remoto, se debe evitar lo siguiente:

- La manipulación física directa en el *switch* por un usuario no autorizado permite acceso completo a este pudiendo interrumpir la comunicación, o en su defecto, puede interceptar información compartida en la LAN.
- No se encuentra configurado adecuadamente el filtrado de entrada para controlar el flujo de tráfico.
- No se encuentra configurado de manera correcta el filtrado de entrada en los puertos espejo para controlar el tráfico bidireccional, pudiendo reenviar el tráfico a puertos no deseados.
- Los documentos de configuración que por algún motivo se extraigan del dispositivo, se deben guardar en un dispositivo que cuente con la facultad de cifrar y restringir el acceso a usuarios no autorizados de la información.
- Para el adecuado uso del protocolo SNMP, se deben agregar los dispositivos que se conectarán al equipo, pero no está limitado el número de direcciones IP que pueden darse de alta para que se conecten a los *switches*, y no se han cambiado los nombres de la base de direcciones.
- Aunque no se estén utilizando, no se encuentran desactivados los servicios inseguros Telnet y del Trivial file transfer Protocol (TFTP).
- No se encuentra limitado el número de sesiones simultáneas de servidor web.

- Se debe evitar la utilización de protocolos no seguros pero que están habilitados en el *switch* como son el HTTP, MMS, Telnet y RSH, esto porque éstos pueden utilizarse en el dispositivo, pero no fueron creados para ser protocolos seguros para la protección de transmisión de datos.
- Algunas funciones de parches de seguridad no se encuentran instaladas, es importante actualizarlas recientemente.
- No se hace uso correcto del protocolo de registro de unidades de datos de protocolo de puente BPDU (GVRP), esto porque no está habilitado para puertos donde no se esperan operaciones RSTP BPDUs.
- Se debe emplear correctamente el protocolo de administración de grupos de internet (IGMP) y el protocolo de registro de Multicast (GMRP), para el filtrado Multicast.
- Los cifrados de *Transport Layer Security* (TLS), están disponibles, pero no se están empleando correctamente, esto porque al realizar las actualizaciones del navegador web, no se configuran de manera adecuada al *firewall*.
- Se proceda a colocar en “desactivado” la configuración de IP, para evitar el enrutamiento de paquetes.
- La Auditoría en *switches* no se lleva a cabo periódicamente para asegurar el cumplimiento de recomendaciones mínimas de ciberseguridad.

- Habilitación de todas las alarmas disponibles para detectar todos los eventos ocurridos en la red, como la falla y recuperación de enlaces, o un acceso no autorizado.

4.3.3.2. Unidad Terminal Remota (RTU)

Las vulnerabilidades para las unidades terminales remotas marca SIEMENS y SEL se obtuvieron posteriormente del análisis de las tablas XXIII y XXIV contenidas en la sección de apéndices del presente estudio, siendo estos:

- SICAM PAS
 - No aplican ciertos eventos de auditoría esenciales
 - Cierre de sesión programado
 - Valor forzado
 - Configuración de acceso
 - Cambio de configuración
 - No aplican alarmas esenciales.
 - Intento de uso de software de configuración no autorizado
 - Configuración inválida o descarga de *firmware*
 - Configuración no autorizada o archivo de *firmware*
 - Cambios de hardware de campo no válidos
- RTU SEL 3555
 - No aplica la protección contra anulación de contraseña

- El mínimo de usuarios admitidos es de 6 únicamente, la IEEE 1686 establece que como mínimo de 10.
- No cuenta con la capacidad de almacenamiento de almacenamiento de al menos 2048 eventos antes que la memoria intermedia comience a sobrescribir el evento más antiguo con el evento más nuevo.
- Los tipos de eventos de auditoría no incluidos son:
 - Cierre de sesión programado
 - Valor forzado
 - Configuración de acceso
 - Cambio de configuración
 - Cambio de *firmware*
 - Alarma
 - Acceso al registro de auditoría
- No se registran los eventos que corresponden a la auditoría
- No tiene alarmas para las siguientes actividades
 - Intento de uso de software de configuración no autorizado
 - Configuración inválida o descarga de *firmware*
 - Señal de tiempo fuera de tolerancia
 - No tiene capacidad para emitir firma digital

4.3.3.3. *firewall*

Para este dispositivo de comunicación, se han detectado posibles puntos vulnerables de acuerdo con las características técnicas que se mencionan en el manual de configuración del equipo RX 1 500 de la marca Ruggedcom, indicado en la bibliografía con el número 58, y se menciona lo siguiente:

- Actualmente no se cuenta con una buena implementación de defensa en profundidad tomando en cuenta el *firewall* basado en host.
- No se cuenta con una configuración orientada a ciberseguridad en el *firewall*.
- Implementación de *firewall* para impedir el acceso a los servidores de la DMZ desde PC externas a dicha zona.
- Reforzar la protección DoS mediante la configuración del *firewall*.
- Dado que se utilizan *firewalls* que normalmente cumplen con la funcionalidad de *switches* de comunicación con *router*, se listan las posteriores vulnerabilidades:
 - No se reemplazaron las contraseñas predeterminadas en el *switch*, es necesario que se cambien dado que dichas contraseñas son genéricas y puede tenerse acceso a los procesos.
 - No se utilizan contraseñas con los requerimientos mínimos para una contraseña segura.

- Las contraseñas se anotan y almacenan en archivo editable no encriptado y no se tiene el control de personas con quienes se comparten.
- Las contraseñas suelen reutilizarse.
- Se debe generar un certificado SSL personalizado y dos o más claves de host SSH antes de la puesta en servicio del dispositivo.
- Se debe incluir dentro del perímetro de seguridad toda la red de comunicación para realizar de manera confiable la autenticación de usuarios mediante RADIUS o TACACS +, o bien deberán estar protegidas por un canal.
- Suele utilizarse el PAP (protocolo de autenticación de contraseña), en entornos que no son seguros. Se debe tomar en cuenta que éste no se considera un protocolo seguro y se desea utilizar se debe utilizar en un entorno seguro de la red.
- No se realiza la buena práctica de utilizar llaves para la autenticación entre enrutamiento.
- Otra vulnerabilidad respecto a los protocolos que interactúan en la capa 2 (de enlace) que no tienen dentro de sus facultades otorgar ninguna autenticación inherente entre puntos finales, como ARP en IPv4, DAD en IPv6 y Wi-Fi en redes inalámbricas, dado que es posible llevar a cabo un ataque a los dispositivos conectados a la red de capa 2, interceptando el tráfico en la misma.

- Configurar adecuadamente el rol de los puertos en MSTP.
- No se realiza la buena práctica de utilizar el protocolo L2TP en conjunto con IPSec para asegurar la tunelización de la comunicación.
- Se deben filtrar las tramas de broadcast, por medio de un umbral definido por el usuario para evitar las conocidas tormentas de Broadcast, evitando saturación en la red y provocar inconvenientes en el funcionamiento de IEDs por mala comunicación.
- Es importante tomar medidas de seguridad contra acceso físico o acceso remoto, estas pueden ser:
 - No se encuentran aseguradas correctamente las claves/llaves para el usuario root, lo que puede perjudicar en el caso de enviar datos más allá de la zona de confianza.
 - El dispositivo puede generar automáticamente certificados para SSL, se debe tomar en cuenta que estos son predeterminados, de aquí que se deben validar con una autoridad de confianza.
 - No se encuentra configurado adecuadamente el filtrado de entrada para controlar el flujo de tráfico.
 - No se encuentra configurado de manera correcta el filtrado de entrada en los puertos espejo para controlar el tráfico bidireccional, pudiendo reenviar el tráfico a puertos no deseados.

- No se ha realizado el uso correcto del protocolo SNMP.
- Cuando se utiliza el dispositivo para realizar alguna actualización o transmisión de syslog, no se percatan de conectarse de forma segura a un servidor, es decir, no hay confirmación que el lado del servidor esté configurado con cifrados y protocolos sólidos.
- No se limita el número de servidores Web permitidos para una sesión autorizada.
- No se encuentra configurado el uso de IPSec en todos los puertos.
- Dadas las características de la marca del dispositivo, no se encuentra activada la función para la aplicación de la protección BFA (Brute force Attack).
- No se encuentra configurada la función de auditoría.
- Se debe realizar la auditoría respecto a que todos los accesos a los servicios de administración se estén realizando desde redes privadas.
- Se debe configurar la opción para realizar cifrados de llaves con la medida de 2048 *bits*.
- Evitar el uso de protocolos que no son seguros como lo son SNMPv1 y SNMPv2c, y RSTP, esto porque no están fabricados para la protección de información.

- Algunas funciones de parches de seguridad no se encuentran instaladas, es importante actualizarlas recientemente.
- Se debe emplear correctamente el protocolo de administración de grupos de internet (IGMP) y el protocolo de registro de Multicast (GMRP), para el filtrado Multicast.
- La Auditoría en *switches* no se lleva a cabo periódicamente para asegurar el cumplimiento de recomendaciones mínimas de ciberseguridad.
- Habilitación de todas las alarmas disponibles para detectar todos los eventos ocurridos en la red, como la falla y recuperación de enlaces, o un acceso no autorizado.
- Es importante evitar el acceso a páginas web externas que no sean de confianza mientras accede al dispositivo a través de un navegador web.

4.3.4. Vulnerabilidades para el nivel Centro de Control (nivel 3)

Las vulnerabilidades que se listan son casos generales que se pueden dar en los Centros de Control de las subestaciones, no se hace referencia a ningún Centro de Control en específico del Sistema Nacional Interconectado, debido a que se debe proteger la información integral de cada empresa de transmisión, por ese motivo se presenta esta información:

- Dado que el Centro de Control en su mayoría se encuentra físicamente ubicado en un distinto lugar a la subestación, es probable que se incumplan algunos puntos de la seguridad física, como es la falta de seguridad en los puntos de acceso a las instalaciones y suma seguridad

en los cuartos donde este ubicados los servidores y las HMI remotas encargadas para monitoreo y control remoto.

- No se tiene creada una buena defensa en profundidad.
- Falta de la configuración orientada a ciberseguridad en los *firewall* periféricos e internos en la zona segura para establecer control de acceso y salida de información al Centro de Control.
- No se realiza auditoría de archivos.
- No se implementa el sistema de detección de intrusos directamente en el Centro de Control.
- Los entornos de ejecución no se encuentran totalmente aislados.
- Falta de administración de contraseñas en los equipos de Networking.
- Lineamientos establecidos para actualización de parches de seguridad de todos los softwares que se estén utilizando en el Centro de Control.
- No se cuenta con una administración correcta del manejo de certificados de autenticación SSL para el intercambio seguro de datos dentro de la distribución del sistema, y para herramientas de acceso de usuarios de ingeniería remotos y la segmentación adecuada para clientes que requieran de acceso remoto.
- No se hace buena práctica del control de acceso basado en roles, y se crean ciertas vulnerabilidades para proteger ciertos servicios esenciales.

- Falta de implementación de llave digital entre servidores por medio de software que cuente con una autoridad de confianza.
- Falta de servidor propio para fines de autenticación, autorización y auditoría para la operación crítica que debería incluir los servidores para el monitoreo, servidor de implementación de parches de seguridad y antivirus y los servidores para monitoreo.
- No se tiene cuidado en deshabilitar los puertos no utilizados en los elementos de la red de comunicación interna del Centro de Control, con la finalidad de proteger los servidores.
- No se cuenta con un adecuado monitoreo de eventos de seguridad según NERC CIP-007-6.
- Los servidores para sistemas fronterizos independientes deben estar ubicados en otra zona separada a los demás servidores que pertenecen a la operación crítica, son los que tienen comunicación con las RTU y dispositivos de la subestación.
- En otra zona deberían estar instalados los servidores UI que brindan acceso para el cuarto de control de los operadores que también forman parte de la operación crítica.
- Es recomendable colocar los servidores SCADA en propia zona con las configuraciones necesarias de ciberseguridad en su unidad terminal maestra.
- No se les da la correcta protección a los elementos del SCADA, como:

- Interfaz gráfico del operador
 - Configuración y distribución del entorno de trabajo
 - Módulo de proceso
 - Gestión de archivo de datos
-
- En otra zona de negocio crítico deben instalarse los servidores para los HIS Host integration server y los servidores de aplicación.

 - Servidores Web que permiten la interfaz de usuario deberían estar ubicados fuera de la red del Centro de Control en una zona desmilitarizada DMZ separada.

 - Correcta implementación de un servidor que sea el central del Centro de Control y de la subestación monitoreada para soportes como SIEM, AD y servicios de PKI.

 - Falta de lineamientos para entrenamiento al personal asignado en el Centro de Control para la seguridad física, y medidas de ciberseguridad de acuerdo con las normas NERC CIP.

4.3.4.1. Vulnerabilidades de la red de la subestación

- Falta de respaldo de Seguridad de IP (IPSec).
- A nivel general no se aprovechan las bondades del Transport Layer Security TLS como en protocolos TCP/IP.
- Falta de centralización del control de la red.
- Para tener el control de acceso de los dispositivos a la red, falta la implementación del esquema del Protocolo extensible de autenticación, (EAP).

- Se podía aplicar la seguridad por UDP/IP basado en comunicación, en los casos en donde el TLS no es aplicable.
- Falta de generación y uso de la infraestructura de clave pública X.509 y certificado de perfil de lista de revocación (CRL).
- Implementación del Control de acceso basado en puertos.
- Seguridad de MAC.
- Identificación segura del dispositivo.
- Segmentación correcta de la red.
- Autenticación segura en toda la red.
- Soporte en la comunicación en un control de acceso basado en roles.
- Seguridad de datos para transmitir y almacenar información.
- Dispositivos de seguridad separados como *Gateways* y VPN.
- Seguridad de comunicación.
- Vigilancia de seguridad y medidas preventivas para asegurar la confiabilidad y disponibilidad de las operaciones y servicios de ingeniería.

4.3.4.2. Vulnerabilidades en la red del Centro de Control

- Vulnerabilidades en los protocolos que se utilizan entre la comunicación y el Centro de Control.
- Comunicación serial entre equipos del Centro de Control.
- Red LAN interna.
- Comunicación operacional.
- Comunicación de ingeniería.
- En caso exista método de intercambio de información entre aplicaciones OLE (Objetc Linking and Embedding).

- Correcta protección para protocolo DNP3 o 60870-5-104 para la comunicación entre la subestación y Centro de Control.

4.3.5. Solución técnica

La siguiente propuesta de solución técnica está basada en la arquitectura de comunicación mostrada en la figura 56, quien es el caso de estudio y con apoyo de lo indicado principalmente en las normas IEEE 1686 e IEEE C37.240. También se toman recomendaciones importantes de las normas complementarias que contribuyen a la correcta implementación de ciberseguridad en los diversos niveles de mando.

4.3.5.1. Para el nivel 0 de la subestación

En cuanto al acceso no deseado a equipo primario, con base en el estándar IEEE 1402, se propone lo siguiente:

- Para el acceso a patio, se recomienda contar con un programa de mantenimiento que contemple al menos una vez por semana, la inspección visual de las cerraduras que forman parte de las cercas perimetrales para el acceso directo a los equipos primarios y a nivel general de todas las cerraduras que permitan una entrada a la subestación, es decir, todos los puntos de acceso de la protección perimetral total de la subestación incluyendo casetas y cuartos de control y monitoreo.
- Mantener cerrado con llave el tablero de mando de los interruptores de potencia, y contar una bitácora de trabajos que se realicen en éste con el objetivo de llevar un control del personal que ha tenido acceso al tablero.

- Utilización de candados del tipo llave no reproducible para puertas de gabinetes que no cuentan con cerradura, al igual que las puertas de acceso a la subestación.
- Es recomendable la implementación de sensores de movimiento en los puntos de posible acceso a las instalaciones, como lo son puertas principales, puertas traseras y de emergencia, portones para el acceso vehicular.
- Instalación de sistema de cámaras para videovigilancia que cubra la totalidad de la subestación, tanto en patio, y principalmente en todos los posibles puntos de acceso, como en el interior de la caseta de control y en caso de tener instalaciones para mando y monitoreo.
- Mantenimiento al menos cada 6 meses de la chapa de la caseta de control.
- Inspección al menos una vez por semana a los tableros de control, protección y medición, al igual que los tableros de control y monitoreo con el fin de verificar que se encuentren cerrados con llave.

4.3.5.2. Para el nivel 1 de la subestación

Las características son mencionadas de acuerdo con fortalezas indicadas en los estándares IEEE 1686 e IEEE C37.240.

- Se debe habilitar la función de control de asignación de tareas de usuario, a causa de los dispositivos de las marcas utilizadas tienen la posibilidad de configurar cada rol de usuario al ingresar al sistema de parametrización del dispositivo.

- Como buena práctica de auditoría, se debe implementar un programa utilizado por la empresa interesada, para que se tome el control de PC autorizadas para ingresar a la configuración de los relevadores y realizar control de acciones para que los archivos no se guarden en memorias externas, discos externos o cualquier otro tipo de dispositivo de almacenamiento externo. Al mismo tiempo se debe implementar la gestión de contraseñas para las computadoras autorizadas, para que se cambien contraseñas cada mes, y en caso de accesos directos en campo ya sea para alguna configuración de los equipos, se debe llevar control de las computadoras del personal del fabricante o distribuidor autorizado que tuvo acceso para realizar las correcciones pertinentes en el dispositivo.
- Respecto al bloqueo de autenticación de usuarios, los dispositivos de protección deben bloquear el ingreso a la configuración en caso la contraseña sea ingresada incorrectamente cierta cantidad de veces de manera consecutiva en un periodo de tiempo. Dicho bloqueo negará temporalmente el acceso al sistema, aunque se deja libre la decisión de definir el tiempo de bloqueo del acceso, pudiendo ser monitoreada la liberación automática. Todo bloqueo o liberación deberá ser registrado en el sistema como una función de auditoría. Esta configuración puede realizarse directamente mediante el software correspondiente de cada marca.
- Respecto a la autenticación de usuario mediante PKI, la identificación debe realizarse mediante una identificación desde una computadora ubicada en el nivel 2, es decir, el bus de Estación propia de la subestación, permitiendo el acceso autorizado dentro de la zona segura de la subestación.

- Respecto al inicio de sesión en los dispositivos para acceder a la configuración, se debe realizar la configuración en los relevadores para que después de cierto periodo de inactividad el dispositivo cierre automáticamente la sesión. En caso sea necesario tener algún periodo de inactividad, se debe desconfigurar esta función temporalmente con previa autorización de los gestores de la empresa dueña de la subestación, teniendo un control externo al del dispositivo de la autorización correspondiente para fines de auditoría.
- Respecto a la gestión de claves para enviar y recibir datos cifrados, es necesario contar con una llave de encriptación, como lo es el PKI.
- Las opciones de llave que proporciona el estándar IEEE C.37.240, conjunto denominado como multifactor para la autenticación de usuario, se recomienda el uso de *token*, estos pueden ser:
 - Una llave
 - Una memoria USB
 - Una tarjeta magnética
 - Una propiedad del usuario (como una huella dactilar o un patrón de retina).
- Respecto a la lista de usuarios con acceso a los dispositivos, se debe mantener control de la adición, modificación y eliminación de las entradas en la lista. Tomando en cuenta los detalles mínimos de autenticación, estos deben ser: nombre, posición, detalles del contacto, fecha y hora en que se agregó el usuario a la lista.

- Respecto a los usuarios autorizados que acceden a la parametrización de los dispositivos; el almacenaje de información es crucial, como el tiempo en el que los usuarios permanecen conectados en el sistema, teniendo ciertas características:
 - Manteniendo la duración de los registros al menos 90 días
 - Los registros deben ser del tipo no volátil
 - Deben ser del modo solo lectura, y sin opción a eliminar

Los registros deben contener información mínima siguiente:

- Identificador para el usuario que accede
 - La fecha y hora de acceso y finalización
 - La interfaz por la cual el usuario tuvo acceso y los intentos fallidos para acceder al dispositivo.
-
- Para evitar que la gestión de contraseñas sobrepase el periodo de 12 meses mínimo indicado en el estándar IEEE C.37.240, es recomendable instalar software para que realice automáticamente el cambio de contraseñas o en su defecto, enviar mensajes a las PC del bus de estación en la zona segura, incluyendo al Centro de Control, algún software recomendado puede ser el *Keypass* para aplicaciones de Windows.

 - Respecto a la cantidad de 4 roles de usuario en los IEDs, dado que se manejan 3 roles de usuario en los equipos actuales, se debe asistir a sitio para la configuración de los roles correspondientes.

- Para fines de auditoría, no se encuentra correctamente monitoreada la actualización de *firmware* de los dispositivos, así que se debe configurar la alarma correspondiente en cada uno de los relevadores de protección de la subestación.
- Se debe corregir el tipo de memoria para fines de control de pista de auditoría, y se debe implementar memoria intermedia circular secuencial, en algunos dispositivos este tipo de memoria está instalada, y como excepción puede implementarse una memoria que sea capaz de almacenar el mínimo de 2048 eventos antes de que la memoria comience a sobrescribir eventos, por medio de configuración propia del IED.
- Equipos SEL no indica que su ciberseguridad se base con la tabla de cumplimiento del estándar IEEE 1686.
- En el caso del RIAG, se deben realizar trabajos de reconfiguración de red de manera que toda la comunicación cuyo punto final se con cada IED, se tenga que pasar a través de la RTU de la subestación.
- No cuenta con el apoyo de la gestión de configuración de dispositivo, el almacenamiento de configuración y la operación de *sotware/firmware* para backup, estas funciones deberán configurarse en sitio, entrando directamente en los IED correspondientes.
- Es importante validar la integridad del *firmware* en ejecución tantas veces como sea necesario. Esta tarea se puede automatizar programando un trabajo para que se repita todos los días o cada semana. La integridad del Firmware también se puede comprobar automáticamente en la puesta en marcha. Si se detecta una modificación no autorizada / inesperada,

inspeccione el syslog en busca de mensajes relacionados con la integridad del *firmware* para identificar qué programas y / o archivos pueden haber sido comprometidos. Si se configura el registro del sistema remoto, esta tarea también se puede automatizar mediante secuencias de comandos para identificar los mensajes de registro clave.

Respecto a las vulnerabilidades listadas para los relevadores de protección marca SIEMENS y SEL, se debe ir a sitio para configurar en cada uno de los relevadores las funciones que actualmente no se encuentran habilitadas. Para funciones específicas que el equipo no proteja, se recomienda realizar un cambio de equipos a una versión más reciente aprovechando la oportunidad en que se presente un *retrofit*.

- Medidor multifuncional

Para medidores multifuncionales, tomando en cuenta el dispositivo analizado correspondiente a la familia ION8650B, es posible realizar la configuración en el software propio del dispositivo o a través de PrimeRead, para estas actividades:

- Configuración correcta para la autenticación de usuarios
- Configuración de bloqueos de cuentas de usuario configurables con el número de intentos de inicio de sesión fallidos.
- Se debe configurar al usuario correspondiente, por medio de un rol configurado por el usuario de manera que el control de uso se utilice para restringir las acciones permitidas al uso autorizado del medidor.

- Configurar en el software la función para que los supervisores no pueden anular las autorizaciones de los usuarios eliminando su cuenta.
- Utilizar software propuesto *Keypass* para que gestione los cambios de contraseña.
- Configurar en el medidor de manera que se restrinja el uso de funciones, puertos, protocolos y / o servicios innecesarios.
- Configurar el bloqueo de sesión para todo el dispositivo de manera que se restrinja todo el acceso incluyendo puntos de acceso como puertos de comunicación.
- Configurar la función de auditoría para el registro de eventos y así poder identificar los cambios en la configuración del medidor y los eventos del sistema de gestión de energía.
- Habilitar la función de auditoría periódica para la comunicación de la capacidad de almacenamiento de registros para notificar a un usuario cuando se acerca el umbral.
- Cambiar de forma predeterminada a funcional para la capacidad de almacenamiento de 5 000 registros de eventos y métodos alternativos para la gestión de registros.
- Configurar en el dispositivo para utilizar los protocolos adecuados y poder enviar información encriptada como SNMPv3.

4.3.5.3. Nivel de estación (nivel 2)

- Modificación de la red de comunicación de manera que todo el tráfico de datos desde la LAN hacia el bus de estación de manera que pase por el *firewall*. Esto se logra con la configuración de los *switch* de comunicación con conexión redundante, de manera que toda la comunicación de equipos de nivel 1 lleguen a dichos elementos, incluyendo al mismo tiempo todos los elementos del nivel 2, incluyendo dentro de este al *firewall*; se encargara de la protección y división con la red que interconecta al Centro de Control, y para que la función de *router* aisle los dominios de difusión no sean propagados más allá de este dispositivo, y el *firewall* debe permitir el tráfico entre las redes IT y OT.

- En cuanto a que Los *routers* de la red no implementan protocolo de resolución de acceso proxy (ARP), y ocultar las direcciones IP de LAN de la subestación. Se configurarán las conexiones en los puertos y los protocolos necesarios para activar un ARP proxy en la interfaz a proteger, dado que el mismo *firewall* es *router* y en el caso que sea compatible con un cliente IPsec remoto, se le asigna una dirección en una subred de una interfaz local. Para implementar el protocolo Ipsec se deben configurar estos protocolos y puertos:
 - Protocolo 51, encabeza de autenticación IPSEC-AH
 - Protocolo 50, IPSEC-ESP Encapsulando la carga útil de seguridad
 - Puerto UDP 500

- Se debe instalar un sistema de detección de intrusiones (IDS), para monitorear el tráfico de la red en el *router*, para detectar actividades no autorizadas desde el exterior o interior de la infraestructura de la red propia

de la subestación, de acuerdo con el análisis del tráfico de la red, compara la situación con firmas de ataques conocidos para evaluación. Por tanto, el IDS como mínimo debe contar con una base de datos “firmas” de ataques conocidos, esto le permite distinguir entre el uso normal de los dispositivos en la red segura y las actividades inusuales, y contar con la funcionalidad de detectar el escaneo de puertos o la transmisión de paquetes de datos mal cifrados.

- Respecto a los requerimientos de *router* usados en las LAN de la subestación según IEEE C37.240 en cuanto a proporcionar los niveles de seguridad de autenticación y configuración de VLAN, como es mencionado para los puertos LAN, esto se indica en la sección de *firewall*, correspondiente, a causa del equipo incluido en la arquitectura de configuración caso de estudio, si puede cumplir con los requerimientos de acuerdo con las normas.
- Para otorgar la protección de datos en movimiento, es necesario la creación de una zona segura dentro de la subestación, que establece los límites de seguridad de los dispositivos en la zona, encriptando toda la información que circula en dicha y zona y al igual que toda la información que sale de ella hacia el Centro de Control, así que el uso de *Transport Layer Security* (TLS), a partir del nivel 2 de la subestación, utilizando el protocolo en los *switches* de comunicación de la red LAN hasta el mismo *firewall* instalado.
- Para el control de acceso basado en roles, primero se debe configurar esta función en todos los equipos que forman parte del nivel de control y monitoreo (nivel 2), y todos los accesos de usuario al sistema de control (PC de servicio, HMI, IED, RTU y dispositivos de red), deben contar con la

funcionalidad RBAC para lograr este control de forma homogénea sobre la subestación. Esto incluye capacidades para asignar los derechos apropiados a los usuarios que administran las cuentas de usuario del sistema. Se pueden configurar roles apropiados para el sistema, incluidos operadores, ingenieros y visores, como establecido en IEEE C37.240.

- Para correcta segmentación de red en los dispositivos de la zona segura del bus de Estación, se debe aplicar una zonificación resultado de un análisis de amenazas y riesgos (TRA), tomando en cuenta que todas las funciones esenciales del sistema de automatización de la subestación están ubicadas en la zona de control de la subestación.
- Para la implementación de zona DMZ en el nivel de estación de la estación, primero es necesario conocer los alcances y funciones de dicho elemento fundamental. Considerando la solución técnica mencionada en el manual *Declaration of Security Conformance* de SIEMENS; se indica como la bibliografía número 59, se propone la siguiente solución:

Se define como la Zona o segmento de LAN utilizado para asignar niveles de acceso a aplicaciones de *User Interface* (UI), archivos e información entre otras dos zonas. La DMZ debe ir localizada detrás de un *firewall*, pero avara una zona semiconfiable entre la red interna y externa, y tendiendo la capacidad de poder filtrar paquetes de información y contenido en la capa 3, poder seleccionar colas de tráfico y prioridad y manejo bidireccional para el caso de la subestación, a causa de que es necesario exportar información hacia el Centro de Control y recibir instrucciones incluso de disparos desde este, hasta los equipos de maniobra de la subestación.

Para dar una mayor efectividad de toda la información que circula entre la subestación y su Centro de Control, es necesario proteger la subestación con una DMZ cuyo diseño debe permitir el acceso de ingeniería desde la PC de servicio dentro de la DMZ de la subestación y La configuración DMZ en conjunto con el *firewall* deben impedir el acceso desde otras fuentes.

La segmentación de red que se consigue con la DMZ debe permitir la conexión desde la red LAN interna y la red privada externa, esta necesita internet y debe ser capaz de proporcionar un control de acceso distinto al servidor de archivos, el servidor que contiene los datos del historial, así como la automatización y la zona del bus de procesos hasta los dispositivos de campo y los IED. Este enfoque también admite la administración remota al proporcionar acceso a través de un servidor de terminal ubicado en la DMZ, lo que evita el acceso directo desde una ubicación remota a un dispositivo de campo.

Se debe tener en cuenta que los elementos que estén dentro de la DMZ, como servidores, aunque físicamente estén dentro de la subestación y misma ubicación que los equipos de nivel 2, éstos no pueden tener conexión directa con la LAN interna de la subestación, sin pasar por lo menos por un *firewall*, este tiene como función determinar la zona de confianza, a causa de que este dispositivo se debe configurar de manera que deje ingresar ciertos paquetes y sacar otros paquetes de la zona de confianza, este proceso se hace con la configuración de las direcciones IP, creando políticas de acceso y denegación de paquetes entre zonas, y donde se deben crear clases para los protocolos permitidos para el tráfico de entrada y salida de la DMZ.

Los servidores instalados en el DMZ son accedidos desde fuera de la subestación, y se convierte en necesidad contar para DMZ básicas con servidores para correo electrónico (SMTP), acceso web (HTTP), y del tipo DNS

(DHCP), y estos servidores mediante sus funciones son los encargados de establecer el tráfico de información y eventos entre la DMZ y la red interna, y así que es de suma importancia proteger la conexiones de la DMZ con la red externa por medio de *Port Address Translation* (PAT), y con *Network Address Translation* (NAT), que permitirá manera toda la información de los servidores en la DMZ con direcciones IP privadas y poder manejar estas mismas desde fuera del perímetro de seguridad de la subestación con direcciones IP públicas.

De acuerdo con la propuesta de DMZ a la que se hace mención, el *firewall* debe ser capaz de soportar 3 redes conectadas a éste, desde un puerto distinto, se debe utilizar la configuración *Three-legged firewall*.

Es recomendable contar con 3 diferentes servidores dedicados a diversas funciones:

- Servidor de registro de seguridad centralizada en la subestación: recopila a través del protocolo syslog todos los registros de seguridad de los componentes del sistema. Se considera como fuente de todos los registros de seguridad para un sistema superior, conservando durante un tiempo determinado en días los registros de seguridad, también como medida adicional de seguridad es posible que se conecte a un sistema +SIEM (*Security Information and Event Management*), súper ordenado sin interferir con la configuración del componente de la subestación, permitiendo detectar rápidamente, responder y neutralizar las amenazas detectadas y soporta la capacidad máxima de registros, configurando un umbral porcentual para eventos, permitiendo generar un anillo para el registro de seguridad de acuerdo con IEEE 1686 para relevadores de protección y RTUs, tomando en cuenta que el servidor syslog está limitado por la capacidad del espacio en disco, y se debe configurar la capacidad

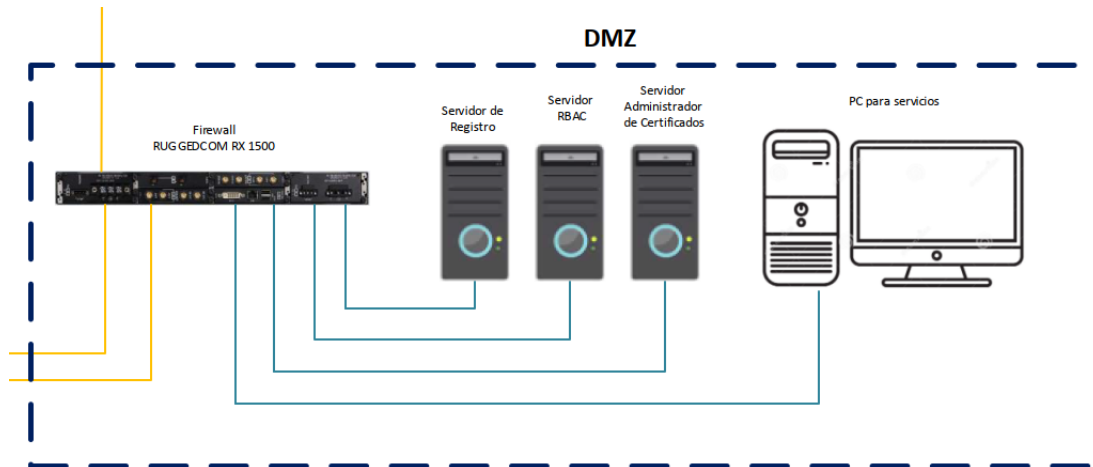
para que automáticamente las entradas de registro antiguas sean borradas después de enviarlas al SIEM.

- Servidor de directorio activo y servidor RADIUS: compilación como controlador de dominio de solo lectura (RODC), alojado en un sistema operativo Windows, y tiene su funcionalidad para que el sistema de la subestación este diseñado para continuar funcionando independiente sin depender de servicios de red externos, en caso se pierda la conectividad con otras zonas y redes externas, aumentando la robustez mediante el diseño de la arquitectura de seguridad independiente para ejecutar funciones básicas de protección y automatización desde fuera de la zona segura.
- Servidor administrador de certificado: debe estar basado en normas internacionales, y cuya función será gestionar automáticamente certificados digitales para permitir una administración eficiente de los controles de seguridad, este podrá estar alojado en un sistema operativo Windows.

Al mismo tiempo se tendrá que instalar una PC para que actúe como host de salto para el acceso remoto, y para que en este equipo se almacenen todas las herramientas de ingeniería y punto único de todos los accesos de ingeniería, alojado en un sistema operativo Windows.

Y estos equipos mencionados son los que conforman la zona desmilitarizada, como se muestra en la figura 50.

Figura 50. Zona DMZ propuesta



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Con esta propuesta se tiene el sistema permite segmentar la red para que los accesos de diversos roles se operen por separado, es decir para los accesos administrativo y de ingeniería se tengan desde la PC de servicio dentro de la PC en la DMZ.

Diseñando la zona de seguridad, se tendría el acceso desde la PC de HMI para realizar funciones de control, como es propio de este dispositivo.

Para ambas zonas, tanto en la DMZ como en la zona de confianza, puede utilizarse autenticación mediante el control de acceso basado en roles de manera que este servicio esté centralizado a través de Active Directory para el sistema operativo Windows y aplicaciones, y RADIUS para IED, RTU y dispositivos de red.

Otro aspecto a considerarse con esta configuración es que es posible implementar alguna plataforma de acceso remoto que refuerce las autenticaciones del personal como ingenieros y personal por medio de PKI y la utilización de contraseña.

Para IED, RTU y componentes de red, la seguridad de la contraseña se puede aplicar mediante la administración centralizada con RADIUS.

Para el control de dispositivos móviles y portátiles:

- El diseño del sistema solo permite el acceso de ingeniería desde la PC de servicio dentro de la DMZ de la subestación. La configuración DMZ / *firewall* impedirá el acceso desde otras fuentes.
- No se utilizan ni habilitan tecnologías inalámbricas en el sistema. Por lo tanto, el acceso de ingeniería / mantenimiento con dispositivos inalámbricos no es posible.
- Las medidas de refuerzo incluyen el refuerzo de los puertos USB y Ethernet no utilizados dentro de la zona segura a través de la configuración y la protección física.

Para la integridad de protección cifrada:

- Todas las comunicaciones que atraviesan zonas no confiables están protegidas criptográficamente. Las conexiones de acceso remoto a través de redes no confiables terminan en una computadora de servicio que actúa como servidor terminal en la DMZ de la subestación. La solución de acceso remoto se debe basar en un software que incluya comunicaciones seguras

de última generación basadas en una VPN IPsec, y la seguridad IEC 62351 para IEC.

- Se puede implementar la comunicación de proceso 60870-5-104.

Protección de la confidencialidad en reposo o en tránsito a través de redes no confiables:

- El acceso remoto al sistema está disponible solo a través plataformas o software que termine en la subestación DMZ, y cuyo canal de comunicación este protegido por un túnel VPN. Para que de esta manera la comunicación se reduce a una conexión de escritorio remoto.

Independencia de las redes de sistemas sin control:

- El sistema de la subestación está diseñado para continuar con la operación independiente sin depender de servicios de red externos. Esto también garantiza la solidez en situaciones en las que no se puede mantener la conectividad a otras zonas y redes externas.
- Los ejemplos de diseño son el servidor RBAC implementado como RODC en la subestación y el servidor de registro en la DMZ. Las funciones de protección y automatización de la base se pueden garantizar dentro de la zona de control de la subestación.

4.3.5.3.1. **Switch de comunicación**

Se listan las recomendaciones que toman como base características técnicas que se mencionan en el manual de configuración del equipo RSG 2100 de la marca Ruggedcom, indicado en la bibliografía con el número 57.

En cuanto a la adecuada autenticación aplicada a los *switches* de comunicación, se presenta lo siguiente:

- En la configuración del dispositivo se debe proceder a cambiar la contraseña predeterminada.
- Para registrar contraseñas con los requerimientos adecuados de ciberseguridad, se recomienda realizarlas de acuerdo con lo estipulado en el estándar IEEE 1686.
- Se debe crear una auditoría externa que permita llevar el control de las contraseñas que se han utilizado con anterioridad, y el documento debe ser protegido mediante cifrado con llave PKI y cualquier revisión debe implementarse en computadoras que se encuentren dentro de la zona segura de la subestación.
- Las contraseñas se deben almacenar en documento cifrado, puede ser utilizando el tipo AES.
- Respecto al certificado SSL personalizado y dos o más claves de host SSH antes de la puesta en servicio del dispositivo.

- Se puede utilizar certificado digital X.509v3, formato PEM y para versiones controladas es posible utilizar claves RSA de 1204, 2048 o 3072 *bits*, no es recomendable utilizar claves menores a 2048 *bits* de longitud.
- Para los pares de claves SSH pública/privada, se debe cumplir con lo siguiente: Formato PEM, par de claves DSA, 1024, 2048 o 3072 *bits* de longitud y aplican las mismas longitudes para claves RSA.
- En caso de no poder realizar esta acción durante la puesta en servicio puede realizarse posteriormente.
- En necesario que se aseguren los diversos canales donde se realizan actualizaciones de manera remota, dado que es necesario realizar autenticación del RADIUS, de manera que cuando un usuario deba autenticarse, ya sea a través de una conexión basada en explorador, lo realice por conexión HTTPS, o bien, puede realizarse por medio de una IPSec.
- No se utiliza la autenticación de clave pública SSH, para este punto se debe tomar en cuenta que las claves públicas SSH se generan en el momento de la autenticación del cliente, es necesario establecer el nivel de acceso en los archivos *flash*, en donde se almacenan, al tener varias entradas de clave pública de usuario ssh, las entradas deben editarse de la siguiente manera par su encabezado y llave:
 - Encabezado: contiene los parámetros de la entrada, separados por comas, en secuencia:
 - ID: un número entre 0 y 9999

- Tipo de entrada: UserKey
 - Nivel de acceso: administrador, operador o invitado
 - Nombre de usuario: debe ser el del cliente
- La clave debe estar en formato RFC4716 o formato PEM, cada llave deberá contemplar lo siguiente:
 - Tipo RSA 2048 *bits* o 3072 *bits*
 - El tipo de entrada en el encabezado no debe exceder los 8 caracteres ASCII.
 - El nivel de acceso en el encabezado no debe exceder los 8 caracteres ASCII.
 - El estado de revocación no debe exceder los 8 caracteres ASCII.
 - El nombre de usuario no debe superar los 12 caracteres ASCII.
- Se debe configurar en el *switch* la función para que todas las contraseñas e información que circula por la red LAN, sea cifrada por medio de SSH/SSL.
- Se debe configurar la función en el *switch* para que sea posible la utilización del protocolo SNMPv3 para enviar toda información que salga del dispositivo a niveles superiores, no se recomienda utilizar las versiones SNMP v1 y tampoco la v2.

- Suele utilizarse el PAP (protocolo de autenticación de contraseña), en entornos que no son seguros, es recomendable no utilizarlo para enviar información fuera de la zona segura de la subestación, y se debe tomar en cuenta que es mejor la utilización de SNMPv3.

- Otra vulnerabilidad respecto a los protocolos que interactúan en la capa 2 (ARP en IPv4 y DAD en IPv6), es necesario asegurar el acceso físico a la red local y utilizar protocolos seguros de capa superior, por ejemplo, IPSec, para evitar el acceso no autorizado a la red.

- Para configurar adecuadamente el rol de los puertos en MSTP, se debe tomar en cuenta que se puede tener más de un rol CIST y MSTI dependiendo de instancias y topología STP definidas en el puerto, teniendo en cuenta:
 - Para los roles de puerto CIST: el puerto raíz (root), proporciona el costo mínimo desde el puente hasta la raíz CIST a través de la raíz, uniendo todas las funcionalidades, es decir si el puente es la raíz y el puerto raíz es el puerto maestro para todos los MSTI, se puede optimizar el costo mínimo a una raíz CIST ubicada fuera de la región.

Un puerto designado proporciona la ruta de costo mínimo desde una LAN conectada a través del puente a la raíz regional CIST.

Los puertos alternativos y de respaldo funcionan igual que en RSTP, pero en relación con el CIST que se utilice como raíz regional.

- Para los roles de puerto MSTI en un puente: el puerto raíz proporciona la ruta de costo mínimo desde el puente hasta la raíz regional MSTI, si el puente en sí no es la raíz regional MSTI. Un puerto designado proporciona la ruta de costo mínimo desde una LAN conectada, a través del puente a la raíz regional MSTI. Los puertos alternativos y de respaldo funcionan igual que en RSTP, pero en relación con la raíz regional de MSTI.
- Respecto a las tramas de broadcast, en cuanto a las tormentas de Broadcast, se puede resolver aplicando correctamente la VLAN para restringir el flujo de tráfico entre grupos de dispositivos, el tráfico broadcast innecesario se puede restringir a la VLAN requerida, impidiendo que afecte a los usuarios de otras VLAN.
- En las redes de comunicación de subestaciones, comúnmente no se realiza un uso correcto para configurar las LAN virtuales, (VLAN), el aislamiento se puede lograr mediante el uso de filtrado de puente creativo y múltiples VLAN para dividir en subredes las IP aparente unificadas en múltiples regiones controladas por diferentes políticas de acceso o seguridad. Los hosts de múltiples VLAN pueden asignar diferentes tipos de tráfico a diferentes VLAN.
- Para la habilitación o deshabilitar los puertos de comunicación, se puede realizar directamente en la configuración del *switch* y al mismo tiempo se puede agregar seguridad al puerto habilitado proporcionando la capacidad de filtrar o aceptar el tráfico de direcciones MAC específicas, a causa de que se inspeccionan las direcciones MAC de origen de las tramas recibidas y se validan con la lista de direcciones MAC autorizadas por el puerto y las tramas no autorizadas se filtra y como opción la parte que

recibió dicha trama se puede cerrar de forma permanente o durante un periodo de tiempo definido, contando con alarma que indique la detección de trama no autorizada.

- Para el acceso físico y remoto, se debe evitar lo siguiente:
 - El gabinete donde se encuentra el *switch* de comunicación debe mantenerse cerrado con llave.
 - Para el filtrado de entrada para controlar el flujo de tráfico, se debe realizar lo siguiente:
 - Dirigirse a las LAN virtuales y configurar los parámetros de VLAN globales.
 - Configurar los parámetros según sea necesario, habilitando o deshabilitando el filtrado de entrada de VLAN en todos los puertos. Cuando está habilitado, cualquier paquete etiquetado que llegue a un puerto, que no esté registrado como un miembro de una VLAN con la que está asociado ese paquete, se descarta. Cuando está deshabilitado, los paquetes no se descartan.
 - Para habilitar el filtrado de entrada en todos los puertos de forma determinada, se deben seguir los mismos pasos que lo indicado anteriormente, en la configuración de VLANs globales.
 - Los documentos de configuración en forma CSV, deberán ser cifrados mediante protocolo si es que se guardan en algún

dispositivo de la red, y en caso sean extraídos, se deben guardar en un lugar seguro sin transferir a través de canales inseguros.

- Para el adecuado uso del protocolo SNMP, el número de direcciones se limitará con la configuración de cada puerto para las VLAN que sean implementadas. Los niveles de seguridad para cada usuario se deben crear grupos en donde se definan a los usuarios que van a pertenecer a un grupo en específico y estos tendrán políticas de acceso distintas.
- Se debe proceder a desactivar los protocolos inseguros Telnet y del *Trivial file transfer Protocol (TFTP)*, aunque no estén en uso.
- Se limita el número de sesiones simultáneas con el acceso de Servidor Web para el direccionamiento IPv4 e IPv6. Es posible limitar el número de sesiones mediante la cantidad de IP que se configuren a cada puerto ethernet y en cada subred del dispositivo, estableciendo una cantidad limitada en la estación de trabajo por medio de rangos de direcciones IP.
- Se debe configurar el SNMP como función determinada para que la información no sea transferida por medio de HTTP, MMS, Telnet o RSH, a niveles superiores como lo es la transferencia al bus de estación o Centro de Control.
- Algunas funciones de parches de seguridad no se encuentran instaladas, es importante actualizarlas recientemente, para este caso es efectivo mantener monitoreadas las versiones de *firmware* instaladas, y activar la alarma de actualización de *firmware* como función de auditoría.

- Habilitar Guardia BPDUs en puertos donde no se esperan operaciones RSTP BPDUs.
- Para el filtrado Multicast, los hosts IP utilizan IGMP para informar sobre la pertenencia a grupos de hosts con enrutadores de Multicast, a medida que los hosts se unen y abandonan grupos de Multicast específicos, los flujos de tráfico se dirigen o retienen de ese host. El protocolo IGMP opera entre enrutadores de Multicast y hosts IP. En el caso en que se coloca un *switch* no administrado entre los enrutadores de Multicast y sus hosts, los flujos de Multicast se distribuirán a todos los puertos, lo que puede introducir un tráfico significativo en los puertos que no lo requieren y no reciben ningún beneficio de ello. IGMP *Snooping*, cuando está habilitado, actuará sobre los mensajes IGMP enviados desde el enrutador y el host, restringiendo los flujos de tráfico a los segmentos de LAN apropiados.
- Los cifrados de *Transport Layer Security* (TLS), están disponibles, y se tendrán que asegurar de que se empleen las versiones más recientes cuando se utiliza la última versión del navegador web compatible con el dispositivo.
- Se proceda a colocar en “desactivado” la configuración de IP, para evitar el enrutamiento de paquetes a causa de que de acuerdo con la topología de red estudiada no se encuentra ningún inconveniente.
- La auditoría en *switches* se llevará a cabo periódicamente para asegurar el cumplimiento de recomendaciones mínimas de ciberseguridad.

- Habilitación de todas las alarmas disponibles para detectar todos los eventos ocurridos en la red, como la falla y recuperación de enlaces, o un acceso no autorizado, se hará directamente en sitio.

4.3.5.3.2. Unidad Terminal Remota (RTU)

Para las RTU, si se tiene instalada una RTU modelo 3555 marca SEL, o bien, la SICAM PAS de SIEMENS, pueden tomarse en cuenta estos casos de configuración en sitio:

- SICAM PAS
 - No aplican ciertos eventos de auditoría esenciales, como son
 - Cierre de sesión programado
 - Valor forzado
 - Configuración de acceso
 - Cambio de configuración
 - No aplican alarmas esenciales
 - Intento de uso de software de configuración no autorizado
 - Configuración inválida o descarga de *firmware*
 - Configuración no autorizada o archivo de *firmware*
 - Cambios de hardware de campo no válidos
- RTU SEL 3555

- No aplica la protección contra anulación de contraseña
- El mínimo de usuarios admitidos es de 6 únicamente, la IEEE 1686 establece que como mínimo de 10.
- No cuenta con la capacidad de almacenamiento de almacenamiento de al menos 2048 eventos antes que la memoria intermedia comience a sobrescribir el evento más antiguo con el evento más nuevo.

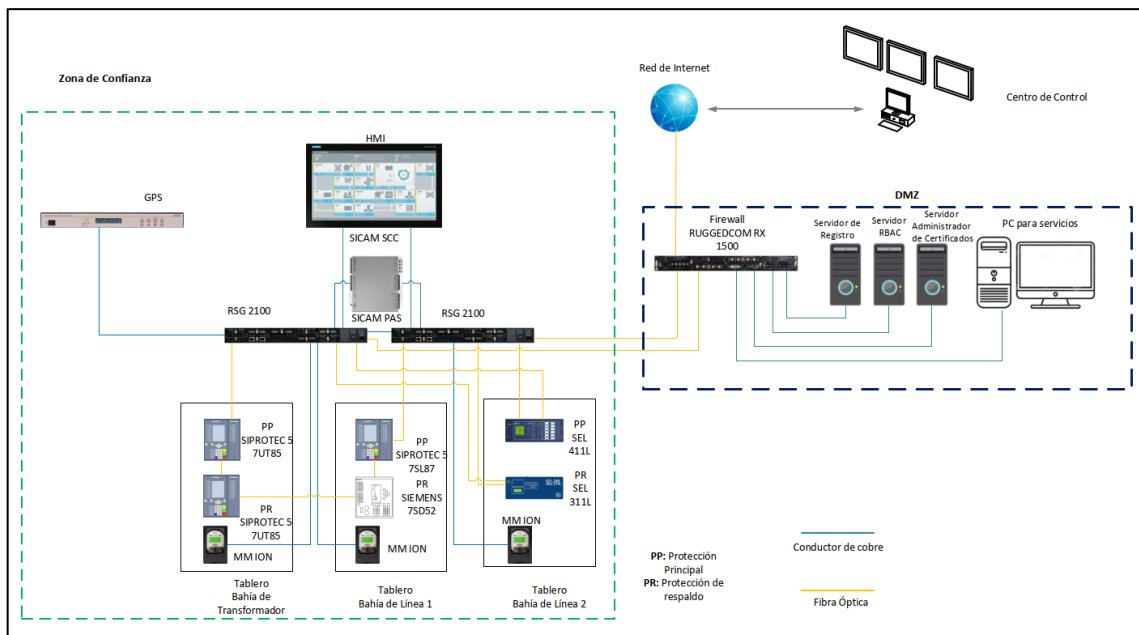
Los tipos de eventos de auditoría no incluidos son:

- Cierre de sesión programado
 - Valor forzado
 - Configuración de acceso
 - Cambio de configuración
 - Cambio de *firmware*
 - Alarma
 - Acceso al registro de auditoría
- No se registran los eventos que corresponden a la auditoría
- No tiene alarmas para las siguientes actividades
- Intento de uso de software de configuración no autorizado
- Configuración inválida o descarga de *firmware*
- Señal de tiempo fuera de tolerancia
- No tiene capacidad para emitir firma digital

4.3.5.3.3. Solución propuesta para arquitectura incluyendo DMZ

En la figura 51 se muestra una arquitectura de comunicación que incluye una zona desmilitarizada.

Figura 51. Solución propuesta para Arquitectura de comunicación incluyendo la DMZ



Fuente: elaboración propia, empleando Microsoft Visio 2016.

Donde los IEDs que se encuentren con redundancia HSR están conectados directamente a los *switch* de comunicación, estos están conectados de forma redundante y donde se forma una sola LAN para todo el nivel 1, todo el tráfico de información de la red pasa a través de estos dos *switches* y toda la información es enviada a nivel superior 2, a la RTU y HMI, en el bus de estación, y es donde

se puede tener control y monitoreo de la subestación. Lo mencionado anteriormente es la zona segura de la subestación.

En la misma ubicación física del nivel de estación se encuentra la zona desmilitarizada conformada por sus respectivos servidores y PC, siendo esta zona externa a la zona de segura de operación, impidiendo la conexión física entre las dos redes para mayor seguridad. Ambas zonas se conectan al mismo *firewall* del tipo proxy que permitirá la salida y entrada de la información autorizada.

Posteriormente se sale a una red no confiable que será el medio de unión de comunicación entre la subestación y el Centro de Control. En el Centro de Control se tendrá otro *firewall* para controlar el ingreso y egreso de la información.

4.3.5.3.4. firewall

- Para crear una estrategia de defensa en profundidad, es recomendable habilitar también el *firewall* basado en host. Para crear un sistema con buen *hardening*, es recomendable activar el *firewall* de escritorio de Windows y abrir solo los puertos necesarios y conocidos para el tráfico entrante.
- En cuanto a la correcta configuración del *firewall*, los límites de las zonas seguras están protegidos por estos dispositivos. La configuración de *firewall* recomendada predeterminada solo permite la comunicación y los protocolos requeridos. Se niegan todas las demás comunicaciones, como los protocolos innecesarios que llevan la comunicación de persona a persona. Las medidas de refuerzo de todo el sistema incluyen la

eliminación de todo el software innecesario para la comunicación de persona a persona.

- Respecto al buen direccionamiento de las IP de las redes LAN de la subestación, toda la comunicación basada en IP hacia y desde la zona de control de la subestación pasa a través del *firewall* de la subestación, esto se hará posible al conectar el *firewall* directamente con los *switch* de comunicación de la red LAN.
- Para la implementación de *firewall* para impedir el acceso a los servidores de la DMZ desde PC externas a dicha zona, se realizará mediante control concurrente de sesión dado que el diseño seguro del sistema de subestación solo permite el acceso de ingeniería desde la PC de servicio dentro de la DMZ de la subestación. La configuración DMZ / *firewall* impedirá el acceso desde otras fuentes. La configuración predeterminada del sistema operativo del cliente Windows es permitir solo una sesión.
- Para reforzar la protección DoS mediante *firewall*, además de la comunicación necesaria con el Centro de Control y el acceso remoto a la subestación, el *firewall* de la subestación bloquea el resto del tráfico de la red, esto hace que se dificulten los ataques DoS en general, desde la subestación a otras redes conectadas.

La configuración correcta de un *firewall* y una VPN es tan importante como el *firewall* y la VPN en sí mismos. Se debe configurar un *firewall* con una regla de eliminación predeterminada en la que se eliminarán todos los paquetes que no estén explícitamente permitidos. Esta regla predeterminada debe estar activa para los paquetes que provienen de la red conectada directamente pero que también provienen del túnel VPN.

Después de eso, solo se deben permitir relaciones de comunicación dedicadas y conocidas. Esto se puede hacer con la dirección IP de origen y destino y el puerto de protocolos utilizado en esa relación de comunicación específica.

- Dado que se utilizan *firewalls* que normalmente cumplen con la funcionalidad de *switches* de comunicación más funciones de *router*, se listan las recomendaciones que toman como base características técnicas que se mencionan en el manual de configuración del equipo RX 1500 de la marca Ruggedcom. Dichas características son:
 - En la configuración del dispositivo se debe proceder a cambiar la contraseña predeterminada.
 - Para registrar contraseñas con los requerimientos adecuados de ciberseguridad, se recomienda realizarlas de acuerdo con lo estipulado en el estándar IEEE 1686, dado que el dispositivo si permite hacerlo.
 - Los documentos de configuración que por algún motivo se extraigan del dispositivo, se deben guardar en un dispositivo que cuente con la facultad de cifrar y restringir el acceso a usuarios no autorizados de la información.
 - Se debe crear una auditoría externa que permita llevar el control de las contraseñas que se han utilizado con anterioridad, y el documento debe ser protegido y contenido dentro de una carpeta cuyo acceso debe cifrarse con llave PKI y cualquier revisión debe

implementarse en computadoras que se encuentren dentro de la zona segura de la subestación.

- Respecto al certificado SSL personalizado y dos o más claves de host SSH antes de la puesta en servicio del dispositivo, se puede utilizar certificado digital X.509 v3, formato PEM y para versiones controladas es posible utilizar claves RSA de 1 204, 2 048 o 3 072 *bits*, no es recomendable utilizar claves menores a 2 048 bits de longitud.
- Para los pares de claves SSH pública/privada, se debe cumplir con lo siguiente: formato PEM, par de claves DSA, 1024, 2048 o 3072 *bits* de longitud y aplican las mismas longitudes para claves RSA.
- En caso de no poder realizar esta acción durante la puesta en servicio puede realizarse posteriormente.
- Es necesario que se aseguren los diversos canales donde se realizan actualizaciones de manera remota, dado que es necesario realizar autenticación del RADIUS o TACACS+, de manera que cuando un usuario deba autenticarse, ya sea a través de una conexión basada en explorador, lo realice por conexión HTTPS, o bien, puede realizarse por medio de una IPSec.
- Es recomendable utilizar claves para la autenticación entre enrutamiento para evitar actualizaciones de enrutamiento no autenticadas, para este factor es recomendable aprovechar las funciones del sistema PKI como llave e introducción de contraseña.

- La funcionalidad de L2TP para implementar túneles punto a punto de paquetes (PPP), todo esto en una red IP, la ventaja es que es posible establecer una conexión segura y privada con el enrutador utilizando Windows VPN/L2TP. Con este protocolo L2TP también es posible realizar un túnel de otros protocolos de capa 2.
- Respecto a las tramas de broadcast, en cuanto a las tormentas de Broadcast, es importante resolver de la misma manera que lo indicado en la sección de recomendaciones de *switch* de comunicación.
- Es importante tomar medidas de seguridad contra acceso físico o acceso remoto, estas medidas pueden ser:
 - Dado que las claves SSH y SSL son accesibles para el usuario root, se recomienda:
 - Reemplazar las claves SSH y SSL con claves desechables antes del envío.
 - Poner fuera de servicio las claves SSH y SSL existentes. Cuando el dispositivo regrese, crear y programar nuevas claves para el dispositivo.
 - Los certificados de cliente y servidor deben estar firmados por la misma Autoridad de confianza, así que los SSL son enviados de manera lleven la firma de la autoridad de confianza y Secure Remote Syslog cifra todos los registros del sistema enviados a los servidores de Syslog.

- Para el filtrado de entrada para controlar el flujo de tráfico, se debe realizar lo siguiente:
 - Dirigirse a las LAN virtuales y configurar los parámetros de VLAN globales.
 - Configurar los parámetros según sea necesario, habilitando o deshabilitando el filtrado de entrada de VLAN en todos los puertos. Cuando está habilitado, cualquier paquete etiquetado que llegue a un puerto, que no esté registrado como un miembro de una VLAN con la que está asociado ese paquete, se descarta. Cuando está deshabilitado, los paquetes no se descartan.

- Para evitar que el tráfico se reenvíe a puertos no deseados, cuando los puertos espejo están habilitados, se debe configurar adecuadamente, realizando lo siguiente en el software de configuración:
 - Se debe asegurar que el dispositivo esté en modo configuración.
 - Navegar para cambiar la duplicación de puertos.
 - Configurar la duplicación de puertos para un puerto específico escribiendo el código que aplique dependiendo de la marca del *router* a proteger.

Es importante que tomar en cuenta que para el caso de estudio se debe realizar lo siguiente:

- ✓ Habilitar el puerto espejo en los dos *switches*
- ✓ Habilitar el filtrado de entradas en los dos *switches*
- ✓ Configurar dentro de un mismo *switch* un puerto como puerto de origen y otro puerto como puerto de destino, y realizar lo mismo para el otro *switch*.
- ✓ Desactivar el protocolo RSTP en el puerto de destino para evitar la salida de cualquier paquete RSTP.
- ✓ Desactivar el protocolo de descubrimiento de capa de enlace (LLDP) en los puertos de destino de ambos *switches* para evitar que se envíen paquetes LLDP a otros puertos.
- ✓ Desactivar los protocolos de gestión de redes (GVRP, GMRP, IGMP) en los puertos objetivo.

Para el adecuado uso del protocolo SNMP, el número de direcciones se limitará con la configuración de cada puerto para las VLAN que sean implementadas. Los niveles de seguridad para cada usuario se deben crear grupos en donde se definan a los usuarios que van a pertenecer a un grupo en específico y tendrán políticas de acceso distintas.

- Para confirmar que el lado del servidor esté configurado con cifrados y protocolos sólidos, es necesario asegurarse que el syslog remoto encripte todos los registros del sistema enviados a los servidores syslog utilizando certificado de Secure Sockets Layer (SSL), firmado por una Autoridad Certificada (CA).
- No se limita el número de servidores Web permitidos para una sesión autorizada, se debe proteger el dispositivo y la red. Para tener en cuenta el número de servidores Web, el servidor debe tener suficiente ancho de banda, los requisitos de ancho de banda se basarán en el número de dispositivos, el ancho de banda también está limitado por defecto para cada dispositivo a 500 kbps. Un servidor modesto deberá poder servir archivos hasta el límite del ancho de banda de la interfaz de red.
- Dado que no se están protegiendo correctamente las conexiones seriales, se recomienda el uso de IPSec siempre que sea posible.
- Para activar la función para la aplicación de la protección BFA (*Brute force Attack*), y prevenir ataques a través de la interfaz de línea de comandos CLI, interfaz Web y NETCONF. Es importante recalcar su utilidad ya que este mecanismo se centra en los hosts externos que intentan acceder al puerto SSH, específicamente el número de logins fallidos, luego de ingresar cierta cantidad de intentos fallidos de inicio de sesión, la dirección IP del host se bloqueará durante cierto intervalo de tiempo.
- Para realizar la auditoría respecto a que todos los accesos a los servicios de administración se estén realizando desde redes

privadas, se recomienda configurar el dispositivo para reenviar todos los registros utilizando TLS a un servidor syslog remoto con *hardening*, manteniendo registros de cada uno de estos tipos: Registros de eventos de seguridad, Syslogs y registro de diagnósticos.

- Se debe configurar la opción para realizar cifrados de llaves con la medida de 2048 *bits*, se puede hacer desde la configuración de llave pública SSH, porque el dispositivo puede configurar para medidas menores, y se debe tomar en cuenta lo indicado anteriormente.

Para los siguientes puntos:

- La correcta aplicación del protocolo SNMP
- la correcta aplicación de los parches de seguridad
- El filtrado Multicast
- La habilitación de alarmas
- Las recomendaciones del uso del TLS

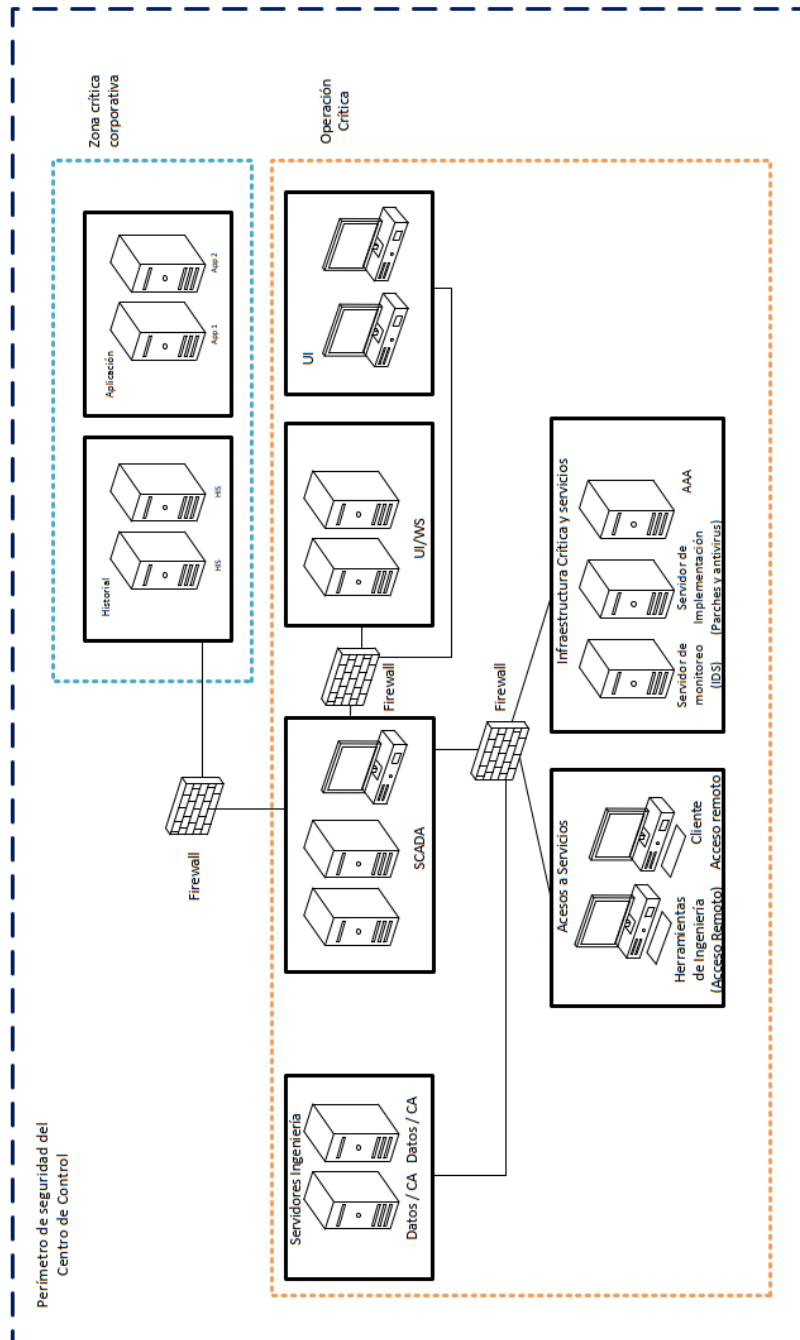
Dado que son características que se comparten con los *switches* de comunicación, se debe aplicar la misma recomendación que se menciona en el apartado del *switch*.

4.3.5.4. Recomendaciones para Centro de Control (nivel 3)

Las buenas prácticas recomendadas en esta sección están enfocadas en las vulnerabilidades que se pueden presentar en los Centros de Control de acuerdo con las mencionadas en la sección anterior y son:

- Dado que el Centro de Control en su mayoría se encuentra físicamente ubicado en un distinto lugar a la subestación, es probable que se incumplan algunos puntos de la seguridad física, como es la falta de seguridad en los puntos de acceso a las instalaciones y suma seguridad en los cuartos donde este ubicados los servidores y las HMI remotas encargadas para monitoreo y control remoto. Es necesario que se sigan las mismas recomendaciones en la IEEE 1702, siendo algunas de ellas:
 - Falta de implementación de puertas en correcto estado con capacidad de cerradura con llave para el acceso al cuarto de control y los servidores debe tener en la entrada lector de PKI y teclado para introducción de contraseña para los usuarios autorizados que designe la empresa.
 - Falta de implementación de sensores de movimiento en los puntos de posible acceso a las instalaciones, como lo son puertas principales, puertas traseras y de emergencia, portones para el acceso vehicular.
 - Un sistema de cámaras para video vigilancia que cubra la totalidad de la subestación, tanto en patio, y principalmente en todos los posibles puntos de acceso e instalaciones para mando y monitoreo.
- Para implementar una buena defensa en profundidad, se debe implementar el diseño de una arquitectura segura que incluya la división en grupos de servidores (serán zonas de seguridad por medio de *firewall* basados en host y basados en red), selectivamente ubicados de acuerdo con el perímetro de seguridad en el Centro de Control, una buena práctica se observa en la figura 52.

Figura 52. **Diseño de arquitectura de comunicación en un Centro de Control implementando defensa en profundidad**



Fuente: elaboración propia, empleando Microsoft Visio 2016.

- Para aplicar la configuración correcta en los *firewall* periféricos e internos en la zona segura para establecer control de acceso y salida de información al Centro de Control, se recomienda seguir las mismas recomendaciones para el *firewall* instalado en la subestación en cuanto a auditoría, autenticación e identificación de usuarios y utilización de protocolos correcto y la configuración para el acceso y egreso de información en el *router* de la DMZ de la subestación, implementando la aplicación de ACL (lista de control de acceso), para filtrar la información reforzando la seguridad en el Router realizando control del flujo de tráfico en la red interna.
- No se realiza auditoría de archivos, para solucionar este punto, es posible aplicar una directiva de auditoría básica en archivos o carpetas con información que se generen dentro del sistema del Centro de Control, estableciendo el tipo de permiso para registrar intentos de acceso correctos o intentos fallidos, en caso algún usuario no autorizado logre acceder a una PC del Centro de Control que tenga acceso a toda la información que se almacene y que circule en el Centro de Control, si toda la información está protegida, no podrá verla o descargarla.
- No se implementa el sistema de detección de intrusos directamente en el Centro de Control. El IDS como mínimo debe contar con una base de datos “firmas” de ataques conocidos lo cual le permite distinguir entre el uso normal de los dispositivos en la red segura y las actividades inusuales, y contar con la funcionalidad de detectar el escaneo de puertos o la transmisión de paquetes de datos mal cifrados.
- Para los entornos de ejecución que no se encuentran totalmente aislados, deben implementarse zonas dentro de la misma estructura del Centro de

Control, como lo indica el estándar IEC 62351-10, que dentro del perímetro de seguridad del Centro de Control deberán implementarse dos zonas principales:

- Operacional crítica: donde se ubican servidores para ingeniería, SCADA, UI y servidores Web, y en zonas separadas se deben ubicar los servidores para servicios periféricos como son los accesos a funciones de ingeniería remotos y los accesos de clientes remotos, y en otra zona el servidor para el monitoreo, como es el que va a almacenar los registros de eventos y el IDS, el servidor encargado de los parches de seguridad y antivirus y el servidor para AAA.
- Empresas críticas: se ubican los servidores para Historia HIS y aplicaciones. Es donde radica la importancia de la diferencia entre las OT e IT.
- Para la administración de contraseñas en los equipos de Networking, debe implementarse un software de gestión de contraseñas para que apoye como función de auditoría a gestionar y a programar fechas como recordatorio de actualización de contraseñas.
- Para mantener un procedimiento que permita la administración de los parches de seguridad, se debe realizar la auditoría de los tipos de parches a actualizar, donde se incluya información básica como la versión de los parches y documentar información de las mejoras que se van actualizando.

- Establecer un periodo mínimo para validar el funcionamiento de los parches, permitiendo verificar si los fabricantes han actualizado nuevas versiones de parches. Se debe crear un plan de mitigación en caso de falla de funcionalidad tras la aplicación del parche.

- Para contar con una administración correcta del manejo de certificados de autenticación SSL para el intercambio seguro de datos dentro de la distribución del sistema, y para herramientas de acceso de usuarios de ingeniería remotos y la segmentación adecuada para clientes que requieran de acceso remoto, primero se deben ubicar en la zona correcta los servidores que se van a utilizar para estas funciones, como es el servidor encargado de los certificados de encriptación, los servidores encargados para los diversos accesos de ingeniería y clientes remotos, y esto debe realizarse de manera que tengan conexión directa con el *firewall* periférico del Centro de Control y que este a su vez tenga comunicación directa con el *firewall* de la zona desmilitarizada de la subestación. Para ambos casos de *firewall* deberán considerarse las recomendaciones de configuración descritas en la sección de nivel 2.

- Preferiblemente un se debe implementar un control de acceso basado en roles RBAC de acuerdo con lo establecido en el estándar IEC 62351-8. Como complemento es importante conocer algunas medidas propuestas por NERC CIP-007-6, como lo son:
 - Contar con documentación que describa cómo autenticar los accesos.

 - Llevar control por medio de una lista de todas las cuentas genéricas identificando su grupo.

- En caso se implementen funciones para generación de listas de cuentas compartidas, es recomendable limitar a los usuarios autorizados para compartir el acceso a cuentas compartidas.
- Incluir límite de intentos fallidos de autenticación e implementar una alerta al llegar al máximo de intentos.
- Cambio de contraseña por defecto.
- En caso falte la implementación de llave digital entre servidores por medio de software que cuente con una autoridad de confianza, es posible integrara el denominado “protocolo de enlace SLL” para iniciar una sesión segura y proteger los mensajes que se intercambian entre servidores, dado se crea un canal cifrado a través de la red de comunicación y red de internet. Po lo que dentro las llaves se harán uso con el certificado SSL, y en caso de tener acceso a una red de internet segura, por medio de un navegador web que señale el acceso a un sitio web seguro, el servidor ya pueda compartir la llave pública con el cliente que requiere el acceso y de esta manera establecer un método de cifrado y una clave de sesión exclusiva.
- La falta de servidor propio para fines de autenticación, autorización y auditoría para la operación crítica que debería incluir los servidores para el monitoreo, servidor de implementación de parches de seguridad y antivirus y los servidores para monitoreo. Se recomienda que los servidores AAA, parches de seguridad y monitoreo deberán ubicarse en una zona periférica de manera que tengan conexión directa con el *firewall* periférico del centro control y de manera que todos los servicios estén centralizados para su gestión directa con la subestación y que, al mismo

tiempo, cuenten con un *firewall* intermedio entre ellos y el sistema SCADA, es decir, es preferible que se encuentren en una DMZ, cuya zona se designará como infraestructura CC & SS.

- Para deshabilitar los puertos no utilizados en los elementos de la red de comunicación interna del Centro de Control, con la finalidad de proteger los servidores, se recomienda realizar la habilitación de los puertos necesarios, siendo importante considerar:
 - Documentación que demuestre el uso de los puertos y la habilitación de puertos y servicios.
 - Manejar auditoría de los puertos habilitados, de manera selectiva y por grupos dependiendo del servicio que desempeñan.
 - Documentación de archivos de configuración de los puertos que se utilizan para cada dispositivo.

En cuanto al monitoreo de eventos de seguridad se recomienda:

- El monitoreo se debe realizar con la finalidad de almacenar eventos relevantes, con un listado de los incidentes como los que se mencionan acá:
 - Detección de intentos de conexión con éxito
 - Detección de intentos de acceso fallidos
 - Detección de códigos maliciosos
 - Generación de alertas para eventos de seguridad como la detección de intentos al sistema.

- Los sistemas fronterizos deben conformar un sistema frontal independiente, este consiste en implementar servidores exclusivos para que intercepten directamente la información que envía la RTU de la subestación o subestaciones para que el sistema de control del SCADA pueda recolectar los datos. Estos servidores estarán ubicados dentro de la zona de operación crítica en su propia zona separada y es recomendable que el medio de comunicación con la subestación sea por medio de su propia VPN con los protocolos de tunelización correspondientes, para la comunicación con el SCADA, es recomendable para fines de defensa en profundidad, que exista un *firewall* entre ambas zonas.
- En cuanto a los servidores UI, es una arquitectura de información y diferentes elementos visuales, cuya función es servir de interface para monitorear y operar la red eléctrica que permite interactuar y comunicar con los elementos, se encarga de administrar los accesos seguros para los usuarios. Para fines de defensa en profundidad, es recomendable que toda la información pase a través del mismo *firewall* que se encuentra entre el SCADA y los servidores del Sistema Fronterizo Frontal.
- Respecto a la ubicación de los servidores SCADA se instalan en dentro de la zona segura del Centro de Control, protegida por los *firewalls* producto de la buena segmentación de red recomendada. Para la correcta configuración de la unidad maestra, se debe filtrar correctamente la información proveniente de la RTU de la subestación, tendiendo así un buen manejo del control de almacenamiento de la información, es posible también organizar la información que se recibe dependiendo de la relevancia y del tipo que tenga la misma, y configurar el dispositivo para que sea posible la intersección de archivos no deseados y maliciosos por

medio de los *firewall* internos tanto de la zona de seguridad como de zonas externas del mismo Centro de Control, y es necesario recordar que los servidores de SCADA están conectados a los demás servidores de todo el Centro de Control.

Para elementos del SCADA, se recomienda tomar en cuenta lo siguiente:

- Para la configuración y distribución del entorno de trabajo, radica mucho la seguridad física en cuanto al acceso al cuarto donde se encuentren las pantallas HMIs remotas y el nivel de autenticación que se implemente en el Centro de Control, preferiblemente un control de acceso basado en roles RBAC de acuerdo con lo establecido en el estándar IEC 62351-8.
- Para el módulo de proceso, dado que permite realizar acciones de forma automática por medio de HMIs hasta los equipos de patio de una subestación, pudiéndose realizar acciones de mando automáticas preprogramadas, maniobras o secuencias de acciones de mando, animación de figuras y dibujos, por lo anterior, es totalmente necesario que el acceso este permitido únicamente al rol de operador del Centro de Control y dicho control este protegido por la autenticación por medio de PKI y contraseña.
- Para la gestión de archivo de datos, dado que es el encargado de almacenar y procesar de forma ordenada datos para elementos periféricos de hardware y demás elementos que intervienen en los procesos incluyendo bases de datos para ser compartidos a otros dispositivos, es importante realizar la transferencia de información por protocolo seguro y encriptado TLS.

- En cuanto a los servidores de almacenamiento histórico HIS, puede implementarse como un sistema cuya función principal será almacenar datos del sistema de potencia y almacenará datos análogos y todos los mensajes relevantes que se hayan enviado por la red, de manera que se archivan de manera segura. Estos servidores estarán en la zona de negocio crítico, así que se debe tomar muy en cuenta que estos pertenecen a los elementos de IT.

- Respecto al servidor Web es preferible que se encuentre de manera centralizada, ubicándose dentro de la misma zona de la infraestructura CC & SS, cuyos elementos son el monitoreo, despliegue y AAA, y cuya función será autorizar los sitios y páginas web a los que los usuarios de la subestación pueden tener acceso, preferiblemente sitios libres de virus y *malware*, y es recomendable que se implemente su propia VPN con red privada separada.

- Se recomienda que el servidor para soportes de SIEM, AD y servicios de PKI se encuentren dentro de la misma DMZ de infraestructura CC & SS, y que preferiblemente se encuentren en su propio servidor.
 - SIEM, Security Information and Event Management, en su servidor Syslog, para guardar, los registros del sistema, en mensajes transmitidos por todos los IEDs y computadores de toda la red.

- Algunas medidas de entrenamiento al personal encargado de las OT principales en el Centro de Control son:

- Es recomendable capacitar a las personas encargadas de administrar las redes que interactúan con el SCADA, en un periodo no mayor a dos meses.
- Capacitación de ciberseguridad general a todos los usuarios autorizados para acceder a funciones de ingeniería, y luego realizar un programa de capacitación específico dependiendo del nivel de acceso que tenga al sistema.
- Es importante mantener registro y el material adecuado para la capacitación del personal.
- Espacios de charlas semanales sobre concientización de los cuidados y buenas prácticas del manejo de información.

4.3.5.5. Recomendaciones para la red de comunicaciones en la subestación

- Para poder proteger la interacción entre dispositivos para establecer conexión desde redes distintas y hacer posible seleccionar una ruta entre dos sistemas hosts, lo que implica capa 3, es necesario hacer uso del respaldo de Seguridad de IP (IPSec), esto aplica para el uso de VPNs de acceso remoto como extensión de la LAN de la subestación, y con ello garantizar autenticación mutua, cifrado y asegurar flujo de paquetes en el caso de tener acceso y conectividad desde una red insegura de internet.
- Para asegurar la capa de transporte, capa 4, y garantizar la protección de información entre cliente y servidor a través de cifrado, utilizando comunicación basada en protocolo TCP/IP, es necesario tomar en cuenta

que para el buen uso de TLS que se deben preparar la clave pública y el certificado, como bien lo indica el estándar IEC 62351-3, lo recomendable es que se utilicen certificados X.509 y establecer una Autoridad DE Autenticación de confianza, de manera que el certificado generado se intercambie y valide de manera bidireccional para la autenticación mutua, para evitar que la conexión se vea obligada a finalizar. En cuanto a la llave pública es importante considerar que puede estar apoyado por mecanismos como RSA o bien, Diffie-Hellman.

En cuanto a la longitud de la clave se admiten:

- Mínimo: longitud de llave RSA mínima de 1024 Bit (para modo herado).
- Obligatorio: para la longitud de llave RSA se recomienda de al menos 2048 Bit (modo moderno).
- Para garantizar la centralización del control de la funcionalidad de Autenticación, Autorización y contabilidad (AAA), el estándar IEC 62351-10 recomienda seguir lo estipulado en la RFC 4962; es un estándar que sirve como guía para los diseñadores de algoritmos y protocolos de gestión de claves de AAA, donde se indica que la gestión de claves requiere un sólido sistema principalmente porque se puede dar el caso de tener almacenamiento de claves, de tal manera que se proporcione un nombre a la clave para que al utilizar un protocolo , todas las partes sepan a qué clave se refiere. Los objetos que no se pueden nombrar no se pueden administrar, tomando en cuenta que todas las claves deben tener un nombre único y que el nombre de clave no debe ser revelar directa o indirectamente el material clave y que un autenticador no perjudique a otro

dentro del mismo sistema de manera que si existe una jerarquía de claves, el compromiso de un nodo de la jerarquía no debe revelar la información necesaria para comprometer a otras ramas de la jerarquía de claves.

Algunas recomendaciones de gestión que brinda el estándar son:

- Confidencialidad de la identidad: si después de un estudio estratégico se determina que es necesario mantener confidencialidad de identidades de los usuarios, se puede aplicar, pero no es requerimiento obligatorio.
- Limitación de la autorización: si la autorización de pares está restringida, es importante considerar lo indicado en IEEE 802.11, donde se consideran aspectos como la vida útil de una clave, restricciones del tipo SSID, o restricciones Calling-Station-ID donde el teclado para ingresar la clave se habilita únicamente con dirección MAC autorizada.

En el caso que más de una parte del protocolo de gestión de claves AAA resida en el mismo host, por ejemplo, que un EAP y cliente AAA estén en la misma entidad, es recomendable dado que el EAP puede enviar una única identidad de autenticador al servidor de AAA, el uso de esta misma identidad en ambas interacciones permite al servidor peer y AA confirmar que el autenticador es consistente en su identificación, lo que hace posible evitar posibles ataques de suplantación. Si el autenticador EAP y el cliente AAA no se implementan juntos, entonces las identidades para ambos serán diferentes, y puede provocar una falta de sincronización de clave, lo que puede genera una serie de vulnerabilidades de seguridad.

- Para tener el control de acceso de los dispositivos y usuarios a la red, el acceso extensible a la red, falta la implementación del esquema del Protocolo extensible de autenticación, (EAP), el estándar IEC 62351-10 recomienda seguir lo estipulado en la RFC 5247, donde en este estándar se especifican las jerarquías de claves EAP, brindando un marco seguro para el transporte y uso de claves generados por algoritmos de autenticación EAP, y al mismo tiempo, proporciona un análisis para todo el sistema enfocado en el cumplimiento de las directrices de gestión de claves establecidas en RFC 4962. Donde en el marco para gestión de AAA, se incluye con soporte EAP que incluye RADIUS, y para considerar un servidor EAP, la entidad que termina el método de EAP con el “peer”, en el caso que no se utilice un servidor de autenticación de *backend*, el servidor EAP forma parte del autenticador, y en el caso que el autenticador funcione en modo *pass-through*, el servidor EAP se encuentra en el servidor de autenticación *backend*.
- Para el envío de información entre dos redes, para asegurar que los paquetes de información lleguen al equipo receptor atravesando toda la red, debe considerarse la seguridad de la capa de transporte de datagramas (DTLS), es posible aplicar la seguridad por UDP/IP basado en comunicación, en los casos en donde el TLS no es aplicable, y como ventaja del UDP, es un protocolo de internet que funciona sin conexión, de manera que se puede utilizar para consultas DNS y conexiones VPN, enviando datagramas a través de la red sin que se haya establecido con anterioridad una conexión entre el equipo emisor y el receptor, ya que se pueden enviar a la dirección IP preferida de la secuencia especificando el puerto de destino, sin embargo el UDP no ofrece ninguna garantía o integración de los datos, para ello el estándar IEC 62351-10 recomienda seguir lo estipulado en la RFC 6347.

- Para el buen uso y generación de infraestructura de clave pública X.509 y certificado de perfil de lista de revocación (CRL), el estándar IEC 62351-10 recomienda seguir lo estipulado en la RFC 5280, donde se describe el uso en internet para los certificados X.509 v3 y la lista de revocación de certificados X.509 v2, describiéndose extensiones de certificado estándar y se definen dos extensiones específicas de internet para ambas versiones y se describe un algoritmo para la validación de la ruta de certificación X.509.

- Para obtener un control de acceso basado en puertos, que brinde la posibilidad de brindar acceso restrictivo, donde sea definido por EAP basado en LAN, incluyendo la administración de llave, de acuerdo con IEEE 802.1AF, el estándar IEC 62351-10 recomienda seguir lo estipulado en el IEEE 802.1X, donde se establece que la arquitectura para un sistema de implementación de control de acceso basado en puertos debe incluir:
 - Las entidades que conforman una pila de interfaces que soporta un punto de acceso al servicio MAC, deben tener un puerto por el que se controla y asegura la comunicación.
 - La LAN adjunta, que proporciona el servicio MAC al cliente del puerto y sus pares.
 - Mecanismos que definan la conectividad entre el puerto y sus pares puerto por puerto.

Por cada puerto que es potencialmente un par en un acceso seguro de comunicación controlada, una entidad deberá contar con lo siguiente:

- Poseer una credencial de autenticación que esté conectada al mismo sistema que el puerto, y lo más importante, que tenga relación segura con el puerto y sus clientes.
- Autenticar mutuamente los puertos del mismo nivel y para la operación que tenga lo siguiente a tomar en cuenta:
 - Éxito o fracaso de la autenticación
 - Un *token*, que comprende claves criptográficas y datos asociados.
 - Un enlace a los datos de autorización o bien, utilizar un canal seguro que pueda ser utilizado para comunicar datos de autorización al puerto de acceso controlado y sus clientes.
- Con la finalidad que los clientes puedan permitir o negar el uso de capacidades de protocolo, es necesario comunicar los datos de autorización a los clientes del puerto.
- Con el objetivo de crear una conectividad segura entre puertos del mismo nivel es recomendable usar los resultados de la autenticación para acordar claves y proteger con cifrado la comunicación.
- Seguridad de MAC (MACsec), de acuerdo con IEEE 802.1 AE, que es definido por este estándar y permite que sistemas autorizados que se puedan interconectar a una LAN manteniendo confidencialidad de datos de transmisión y hacer posible tomar medidas contra tramas transmitidas o incluso modificadas por dispositivos no autorizados. Algunas funciones de MACsec son:

- Mantener la conectividad correcta a la red y servicios
- Aislamiento de ataques de denegación de servicio
- Localización de cualquier fuente de comunicación de red a la LAN de origen.
- La construcción de redes públicas, ofreciendo servicio a personas no relacionadas o clientes sospechosos, utilizando infraestructuras LAN compartidas.
- Comunicación segura entre organizaciones, usando una LAN para transmisión.
- Despliegue incremental y no disruptivo, protegiendo los componentes de red más vulnerables.

MACsec protege la comunicación entre dispositivos confiables de la infraestructura de red y opera en redes que comprenden estaciones finales y LAN de medios compartidos o punto a punto individuales, interconectados por sistemas intermedios como puentes MAC, puentes compatibles con VLAN y *routers*.

- Identificación segura del dispositivo de acuerdo con IEEE 802.1AR; especifica identificadores únicos por dispositivo (DevID), y la gestión y enlace criptográfico de un dispositivo a sus identificadores, define un mecanismo estándar para autenticar la identidad de un dispositivo, los DevID y su uso general son:

- Un DevID secret: es la parte de clave privada de un par de claves pública-privada.
- Un certificado DevID que contiene la clave pública correspondiente y un nombre de sujeto que identifica el dispositivo.
- La cadena de certificados, desde el certificado DevID hasta un ancla de confianza, que se puede utilizar para autenticadores potenciales.

De esta manera se permite que un dispositivo conectado a la red pueda afirmar su identidad en los protocolos de autenticación, siempre y cuando cuente con uno de los DevID. Segmentación correcta de la red, utilizando una DMZ para brindar un control de acceso distinto al servidor de archivos.

Para una autenticación segura, se recomienda:

- La computadora del servicio local basada en credenciales de tipo X.509 (certificados y llaves privadas asociadas), con las que puedan proporcionarse en *tokens* inteligentes.
 - Mutuamente para la operación relacionada máquina a máquina basada en TCP, IEC 61850, IEC 60870-5-104 o DNP de acuerdo con IEC 62351-3, -4 y -5 aplicando credenciales X.509.
 - Para mensajes GOOSE utilizados en los dispositivos de campo usar la IEC 62351-6.
- Según estándar IEC 62351-6 algunas recomendaciones importantes para la seguridad de los datos son:

- La encriptación no es recomendada para aplicaciones que utilicen GOSSE e IEC 61850-9-2 y que requieren tiempos de respuesta de 4 ms, configuración de Multicast, por lo tanto, el proceso de selección de la ruta de comunicación, sin embargo, considerando que la comunicación a través de GOOSE y SMV estén incluidos en la lógica de operación de una red LAN de la subestación, se utiliza la misma protección que se le debería dar a la red LAN para otorgar confidencialidad a los intercambios de información.
- Para aumentar y proteger el replay de GOOSE se utilizarán extensiones de seguridad, para clientes debería establecer y rastrear la hora actual. Un GOOSE con una estampa de tiempo que exceda un sesgo de 2 minutos no debe ser procesado. El periodo de sesgo debe ser configurable y deberá estar soportado para un máximo de 10 segundos.
- Para la detección de manipulación de los mensajes, estas amenazas se contrarrestarán a través del algoritmo utilizado para crear el mecanismo de autenticación.
- Según estándar IEC 62351-4, algunas recomendaciones para proteger MMS son:
 - Para mensajes MMS se recomienda la utilización de autenticación para este tipo de mensajes mediante el valor de llamada del AARQ y el valor de respuesta del AARE. La autenticación del certificado estará en una cadena de octetos que contenga un DER codificado con certificado de llave pública expedida al remitente para su

utilización en la evaluación de firma digital. El tamaño máximo para el certificado de llave pública debe ser de 8,192 octetos.

- Para la comunicación en un control de acceso basado en roles, se recomienda seguir con los lineamientos de la IEC 62351-8 para proteger los distintos accesos a los equipos para control e ingeniería hasta el nivel de equipo de campo. Algunas recomendaciones:
 - Si los certificados X.509 son usados, pueden llevarse en el *token* Smart y pueden combinarse con el certificado que se utilizó para la autenticación.
 - Se debe implementar un control de seguridad antes de asignar un rol al personal, y definición del área de responsabilidad del personal de servicio para permitir solo un acceso distinto.
 - Utilización de servicios de PKI para emitir y mantener la seguridad para credenciales para RBAC como se indica en IEC 62351-9.

Seguridad de datos para transmitir y almacenar información:

- Cifrado de datos de la información almacenada como ingeniería y datos de control o *backup* de datos en la DMZ.
- Cifrado de tráfico utilizado para protocolos de comunicaciones sensibles con el sistema de entidades externas.
- Opciones de seguridad de protocolo de protocolos de comunicación.

- La seguridad en protocolos para proteger las conexiones individuales (TLS, DTLS, IPSec).
- Dispositivos de seguridad separados como *Gateways* VPN, generando un túnel seguro basado en IPSec para comunicación basada en IP.
- Seguridad de comunicación: aplicación de opciones de seguridad utilizando protocolos de apoyo como tiempo de red: NTPv3 y SNMPv3.
- Vigilancia de seguridad y medidas preventivas para asegurar la confiabilidad y disponibilidad de las operaciones y servicios de ingeniería.

4.3.5.6. Recomendaciones en la red del Centro de Control

Con la implementación de nuevos roles comerciales, ciertas responsabilidades pueden quedar fuera del perímetro de seguridad del Centro de Control y formar parte de un perímetro por aparte con su propia seguridad, como es el caso de la *Bussiness Critical*.

Donde se puede apreciar que el nivel de seguridad de la subestación está conformado el nivel de bus conformado por IED y sus respectivos *switches* de comunicación conformando su propia red LAN y brindando seguridad hacia el bus de estación por medio de un *firewall*, luego hacia el bus de Estación donde se tiene todo el control y supervisión de la subestación, todo esto incluido en el perímetro de seguridad de la subestación como tal. Puede tomarse en cuenta

que para los dispositivos de control y protección del nivel 1, se puede contar con su propia RBAC y sus respectivos PKIs para la identificación y autenticación de cada usuario.

Para el nivel de estación se considera la utilización del PKI para la autenticación de cada usuario, dependiendo el rol asignado, para tener acceso a la RTU/HMI para realizar acciones de control y monitoreo de la subestación. Al mismo tiempo se debe considerar el uso de antivirus para los sistemas operativos de Windows que se utilicen en las computadoras y HMI, y considerando una DMZ detrás de cada *firewall* instalado.

En el perímetro del Centro de Control se debe considerar una VPN segura desde el nivel de estación para cada zona de seguridad dentro del Centro de Control.

Para la comunicación entre la subestación y el Centro de Control se deben tomar en cuenta:

- Comunicación operacional
 - Protocolos seriales RTU, como DNP
 - Protocolos RTU basados en IP (ejemplo 61850 sobre TCP/IP)

- Comunicación de ingeniería a través de:
 - Protocolos propietarios
 - Herramientas de ingeniería remota basadas usando HTTPS o HTTP.

- HMI remota, acceso de diagnóstico mediante protocolos como HTTPS, HTTP o RDP.

Comunicación relacionada con la gestión de seguridad:

- Datos de registro e intrusión utilizando SNMP
- Actualizaciones de parches y actualizaciones de anti *malware* para SO comerciales o común.
- Conexiones de autenticación, autorización y auditoría.

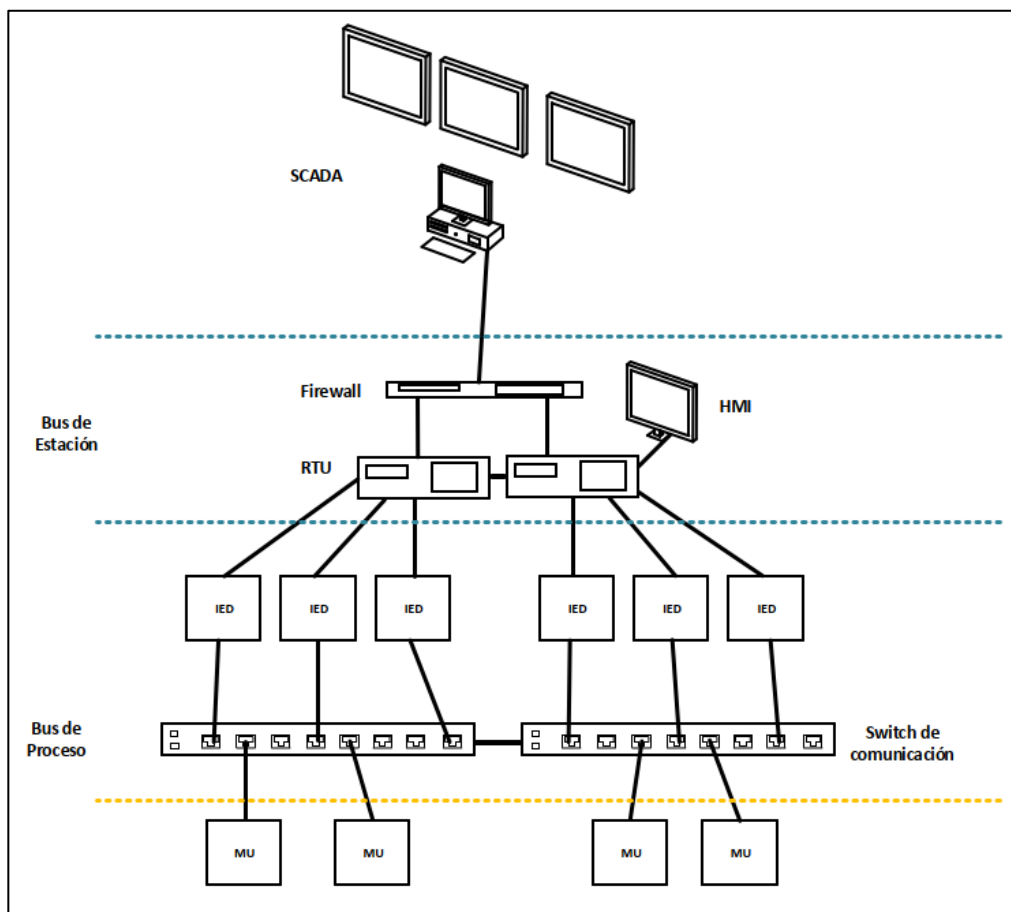
4.3.6. Subestación digital

Se han estudiado las vulnerabilidades que pueden tener las subestaciones convencionales, y es importante tomar en cuenta que esas mismas vulnerabilidades son las que se pueden presentar en las subestaciones digitales. La diferencia radica en que en los transformadores de instrumentos, una subestación totalmente digital implementará transformadores de instrumentos no convencionales y estos transmitirán por medio de fibra óptica los *Sample values* a las *Merging Units* se pueden considerar como IED y que para este caso aplican las mismas vulnerabilidades presentadas en los IEDs de subestaciones convencionales, incluso, la marca SIEMENS presenta soluciones de *Merging Unit* que pertenecen a la familia de SIPROTEC 5 que ya se evaluó en la tabla de cumplimiento (TOC), del estándar IEEE 1686, presentada en la sección de anexos del presente trabajo de investigación.

Es importante mencionar que en Guatemala actualmente no existe la implementación de subestaciones totalmente digitales, existen subestaciones convencionales que poco a poco adoptan criterios a la digitalización como es el uso total del protocolo IEC 61850 para trabajar con mensajes GOOSE para el

envío de eventos en la red LAN propia de la subestación, o el uso parcial de *Merging Unit* para la realización de pruebas en algunos casos cuando se implementan equipos de medición no convencionales. La jerarquía de niveles de una subestación digital puede apreciarse en la siguiente figura:

Figura 53. Niveles de mando de una subestación digital



Fuente: elaboración propia, empleando Microsoft Visio 2016.

En cuanto a la diferencia más notoria entre una subestación digital y una convencional es la implementación del bus de proceso; está formado por los múltiples IEDs de toda la subestación, esta topología de red aún no es

implementada por las empresas debido a que el uso de esta topología requiere que los IEDs contengan la suficiente cantidad de puertos, para interactuar a nivel de bus de proceso y para que puedan reportar directamente al bus de estación.

La cantidad de *switches* de comunicación se convierte en un factor importante, estos elementos son los encargados de formar el bus de proceso y de hacer posible la interconexión de todos los IEDs de manera que la comunicación sea del tipo horizontal con paquetes Ethernet etiquetados y con mensajes del tipo Multicast de capa 2.

Las normas que aplican para implementar ciberseguridad en este tipo de configuración son:

- Para IEDs, Relevadores de protección y *Merging Units*: IEEE 1686
- Para el bus de proceso en su totalidad
 - Para proteger los mensajes GOOSE enviados por los relevadores de protección para enviar eventos al bus de proceso y Sampled Values enviados por los transformadores de instrumentos producto de señales análogas de voltaje y corriente, aplica la IEC 62351-6, que es la que determina protección para el estándar IEC 61850.
- Consideración del buen uso de MACsec de acuerdo con lo estipulado en IEEE 802.1AE para proteger el tráfico de direcciones MAC en todo el bus de proceso a nivel de enlace.

Para la parte entre el bus de proceso y el bus de estación es importante tomar en cuenta que en este nivel de la subestación digital se encuentran los mismos equipos que se encuentran en un bus de estación de una subestación

convencional. Por lo tanto, es necesario proteger toda la información que se envíe por MMS que se intercambian entre estos dos niveles para la arquitectura de cliente servidor que se implementa, siendo este tipo de comunicación del tipo vertical y que para implementar la seguridad en este tipo de información es lo estipulado en el estándar IEC 62351-4, donde se definen los tamaños de llaves y el proceso de autenticación entre dispositivos de manera que si la autenticación no es válida no se tenga acceso a la información que transita entre ambos niveles.

Para el resto de los elementos es posible la aplicación de las medidas de ciberseguridad presentadas para las subestaciones convencionales incluyendo la implementación de una DMZ en el bus de estación y las recomendaciones para enviar por tunelización toda la información del bus de estación de la subestación, pasando por el *firewall* hacia el Centro de Control, que de igual manera se deben seguir las recomendaciones indicadas en la sección de subestaciones convencionales.

4.4. Estudio económico

Para fines de consideración de inversión de implementación de ciberseguridad en las subestaciones eléctricas, es necesario realizar un estudio económico; permitirá conocer los precios estimados necesarios para aplicar las diversas medidas de seguridad en las subestaciones de las diversas empresas de transmisión, quienes serán los inversionistas y se determinarán la rentabilidad del mismo. Se toma el caso de estudio de la figura 50 como base para determinar las premisas, cantidades de equipos y los servicios necesarios para implementar ciberseguridad.

El valor del dólar de Estados Unidos se respalda de acuerdo con el tipo de cambio de dicha moneda (USD), a quetzal de Guatemala (GTQ), indicado por el Banco de Guatemala, y en el presente estudio se utiliza el siguiente:

- Tipo de cambio a la fecha 19 de abril de 2022: 7,65599

El análisis se realizará en un primer caso, para la implementación de mejores prácticas de ciberseguridad, como se muestra para cada nivel.

Para el nivel 0 o también conocido como nivel de patio, se están considerando las recomendaciones del estándar IEEE C37.240 para la seguridad física de la subestación.

Tabla XVI. **Costos para la implementación de ciberseguridad en nivel de patio nivel 0**

Seguridad para equipo de patio	Precio unitario en USD	Cantidad	Precio total en USD
Costo del sistema de cámaras de video vigilancia con 15 cámaras (sujeto a cambios dependiendo de las cantidades de accesos y dimensiones de las instalaciones de la subestación), e instalación: <ul style="list-style-type: none"> • Cámara tipo domo, marca EPCON • 2 discos duros de 4TB para video vigilancia • 1 PC 	6 147,98	1	6 147,98
Instalación de sensores de movimiento en los diversos puntos de acceso para 5 puntos de acceso	102,85	5	514,26
TOTAL en USD			6 662,24

Fuente: elaboración propia.

Para el nivel 1 que corresponde a los IEDs, se toma en cuenta la siguiente tabla.

Tabla XVII. **Costos para la implementación de ciberseguridad en nivel 1**

Seguridad para nivel 1	Precio unitario en USD	Cantidad	Precio total en USD
Costos por realización de configuración de las diversas funciones en los Relevadores marca SEL y SIEMENS: <ul style="list-style-type: none"> • Configuración de acuerdo con el control de acceso basado en roles RBAC y asignación de cada rol. • Habilitar el control permisivo de supervisión. • Configuración del seguimiento de auditoría en el IED • Configuración de multifactor para autenticación de usuarios en los IEDs • Configuración para en los IEDs • Configuración de todas las alarmas recomendadas por la IEEE 1686 • Configuración de eventos que se recomienda registrar por la IEEE 1686 • Configuración de funciones criptográficas según IEEE 1686 • Configuración para deshabilitar puertos físicos y lógicos que no se están utilizando 	255,00	6	1 530,00
Configuración del software para gestión de actualización de contraseñas en relevadores de protección	500,00	1	500,00
Costos por actualización de <i>firmware</i> en relevadores de protección	200,00	1	200,00
Configuración de funciones de ciberseguridad en medidor multifuncional	255,00	3	765,00
PRECIO TOTAL			2 995,00

Fuente: elaboración propia.

Donde se están considerando precios de los equipos que mejor se adaptan a los requerimientos especificados en los estándares IEEE C37.240 e IEEE 1686, sin embargo, lo más recomendable es no tomarlos en cuenta.

La sustitución de los equipos conlleva a un gasto mucho mayor de reconfiguración y montaje de los nuevos equipos, y desmontaje de los equipos actualmente instalados.

Se recomienda tomar en cuenta únicamente los precios de las licencias que no se encuentran instaladas y los precios por configuración de los equipos ya instalados, y para el nivel de control y monitoreo, nivel 2, se considera lo siguiente:

Tabla XVIII. **Costos para la implementación de ciberseguridad en nivel 2**

Seguridad para nivel 2	Precio unitario en USD	Cantidad	Precio total en USD
Configuración de funciones de ciberseguridad en <i>switches</i> de comunicación: <ul style="list-style-type: none"> • Deshabilitar puertos de comunicación que no están en uso • Configuración para el uso de los Protocolos de comunicación correctos para el cifrado de datos y protocolos de administración de grupos para el filtrado Multicast. • Configuración de puertos <i>mirror ports</i> • Configuración de direcciones IP nuevos equipos instalados • Deshabilitación de protocolos Telnet y TFTP • Organización de sesiones simultáneas de servidor web • Configuración de cifrados de TLS • Configuración correcta para el filtrado de entrada para controlar el flujo de tráfico. • habilitación de todas las alarmas disponibles para detectar todos los eventos ocurridos en la red. 	255,00	2	510,00
Configuración del software para gestión de actualización de contraseñas en <i>switch</i> de comunicación	500,00	1	500,00
Para configuración de VLAN en <i>switch</i> de comunicación (Por subestación), que incluye: <ul style="list-style-type: none"> • Segmentación de red • Implementación de todo el tráfico de datos de la red LAN hacia el bus de estación de manera que todo se incluya en el <i>firewall</i> 	510,00	1	510,00
Licencia para la Implementación de PKI para la autenticación de usuarios	2000	1	2 000,00
Costos por la configuración de acuerdo con el control de acceso basado en roles RBAC	255,00	2	510,00
Costos por la implementación de plan de auditoría de usuarios y contraseñas	1 000,00	1	1 000,00
Costos de configuración de funciones de ciberseguridad para RTU y HMI	255,00	2	510,00

Continuación de la tabla XVIII.

Costos de configuración de <i>firewall</i>	255,00	1	255,00
Integración de Sistema de Detección de Intrusión (IDS)	3 000,00	1	3 000,00
Servidores de la DMZ	4 100,00	3	12 300,00
Configuración de servidores DMZ - Servidor de Acceso - Servidor para RBAC - Administrado de certificados	255,00	2	510,00
PC de servicio en DMZ	2 800,00	1	2 800,00
PRECIO TOTAL			24,405.00

Fuente: elaboración propia.

Se está incluyendo los costos aproximados por la implementación de la zona desmilitarizada DMZ, actualmente las subestaciones no lo tienen instalado como medida y aplicaciones de ciberseguridad.

Para los precios de actualización de *firmware* se están considerando precios aproximados, esto va a depender de la marca del equipo que se esté analizando y tomando en cuenta que en algunos equipos la actualización de *firmware* no tiene costo (lo incluye dentro del plazo de garantía de los mismos).

Para el Centro de Control, nivel 3, se plantea lo siguiente:

Tabla XIX. **Costos para la implementación de ciberseguridad en nivel 3**

Seguridad para nivel 3	Precio unitario en USD	Cantidad	Precio total en USD
Licencia para la implementación de PKI para la autenticación de usuarios	2 000	1	2000
Costos por la configuración de acuerdo con el control de acceso basado en roles RBAC	255	1	255
Costos de configuración de <i>firewall</i> para seguridad de capas	255	1	255
Costos por la implementación de las diversas VPNs provenientes de las funciones de la subestación	255	2	510
Costo por configuración en servidores para la implementación de diversas zonas	255	2	510
Integración de Sistema de Detección de Intrusión (IDS)	3 000	1	3 000
Entrenamiento para el personal encargado del monitoreo en el Centro de Control	1 500	1	1 500
Adquisición de los <i>firewall</i> para implementar protección de capas (Cualquier marca)	5 000	2	10 000
PRECIO TOTAL			18 030,00

Fuente: elaboración propia.

Únicamente se están tomando en cuenta precios por servicios de implementación de ciberseguridad y las licencias necesarias, no se toma en cuenta el intercambio de equipos nuevos, dado que no es solución factible en precio, y no corresponde al alcance de estudio del presente documento.

De las tablas XVI, XVII, XVIII y XIX se obtiene un total de USD 52,092.24 para la implementación de seguridad física, configuración de las funciones recomendadas de ciberseguridad en los equipos de protección y comunicación ya instalados en una subestación, implementación de una DMZ y los trabajos en el Centro de Control.

Para fines de estudio se enlistan los equipos que conforman cada nivel de la subestación, y es importante tomar en cuenta que según el estudio técnico los equipos que cumplen a mayor conformidad respecto la norma IEEE 1686 objeto del estudio de este documento son los de marca SIEMENS y según los apéndices 1, 3 y 4. Es necesario tomar en cuenta que, si se considera reemplazar equipos que sean muy antiguos dentro de alguna subestación, dado que éstos no posean opciones para configurar funciones de ciberseguridad, y se considere cambiarlos por equipos más actualizados, esta opción no es viable.

Además de considerar el precio de cada equipo nuevo, se debe considerar los cambios físicos que se tendrían que realizar en los tableros y en los planos de ingenierías ya elaborados, por lo que estos montos no se están considerando en este análisis y tampoco costos por instalación, configuración, montaje ni puesta en marcha de estos.

Tabla XX. **Costos de equipos que incluyen funciones de ciberseguridad**

Equipos de subestación	Precio unitario en USD
Siprotec 5 marca SIEMENS para protección de transformador 7UT85	14 500,00
Siprotec 5 marca SIEMENS para protección de Línea 7SL87	11 500,00
Relevador marca SEL 411L	10 143,00
Relevador marca SEL RTU 311L	6 216,00
Ruggedcom RSG 2100	7 000,00
SICAM PAS + SICAM SCC	13 000,00
HMI SIMATIC IPC 477D, 19"	6 000,00
Ruggedcom RX1500	9 500,00
RTU 3555 SEL	7 560,00
GPS SEL	6 100,00
GPS Arbitrer B	3 500,00
Medidor ION 8650B	5 800,00

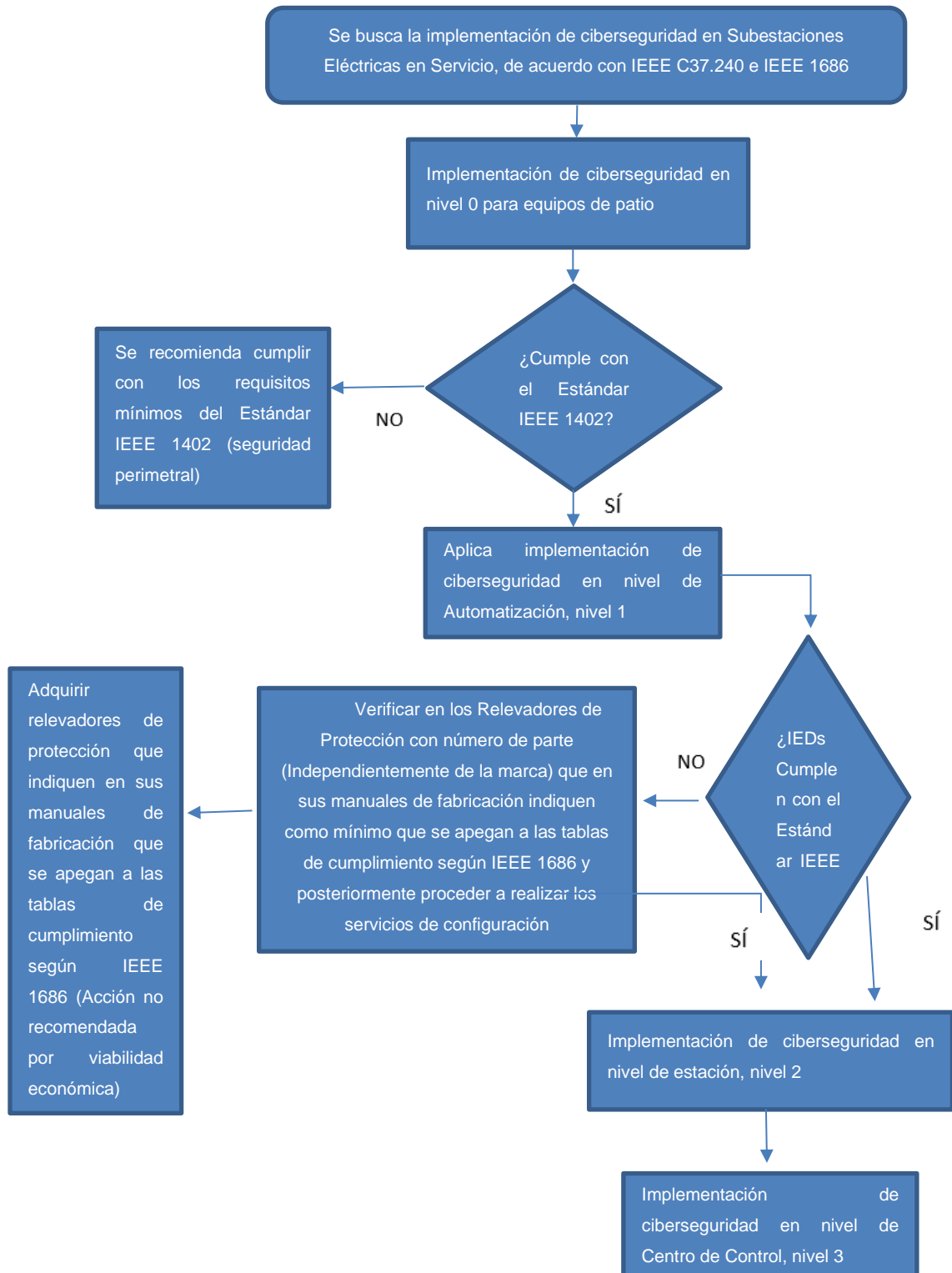
Fuente: elaboración propia.

Tabla XXI. **Costos para la implementación de ciberseguridad en su totalidad para subestaciones eléctricas en servicio (basado en las características técnicas indicadas en el caso propuesto del presente estudio de prefactibilidad)**

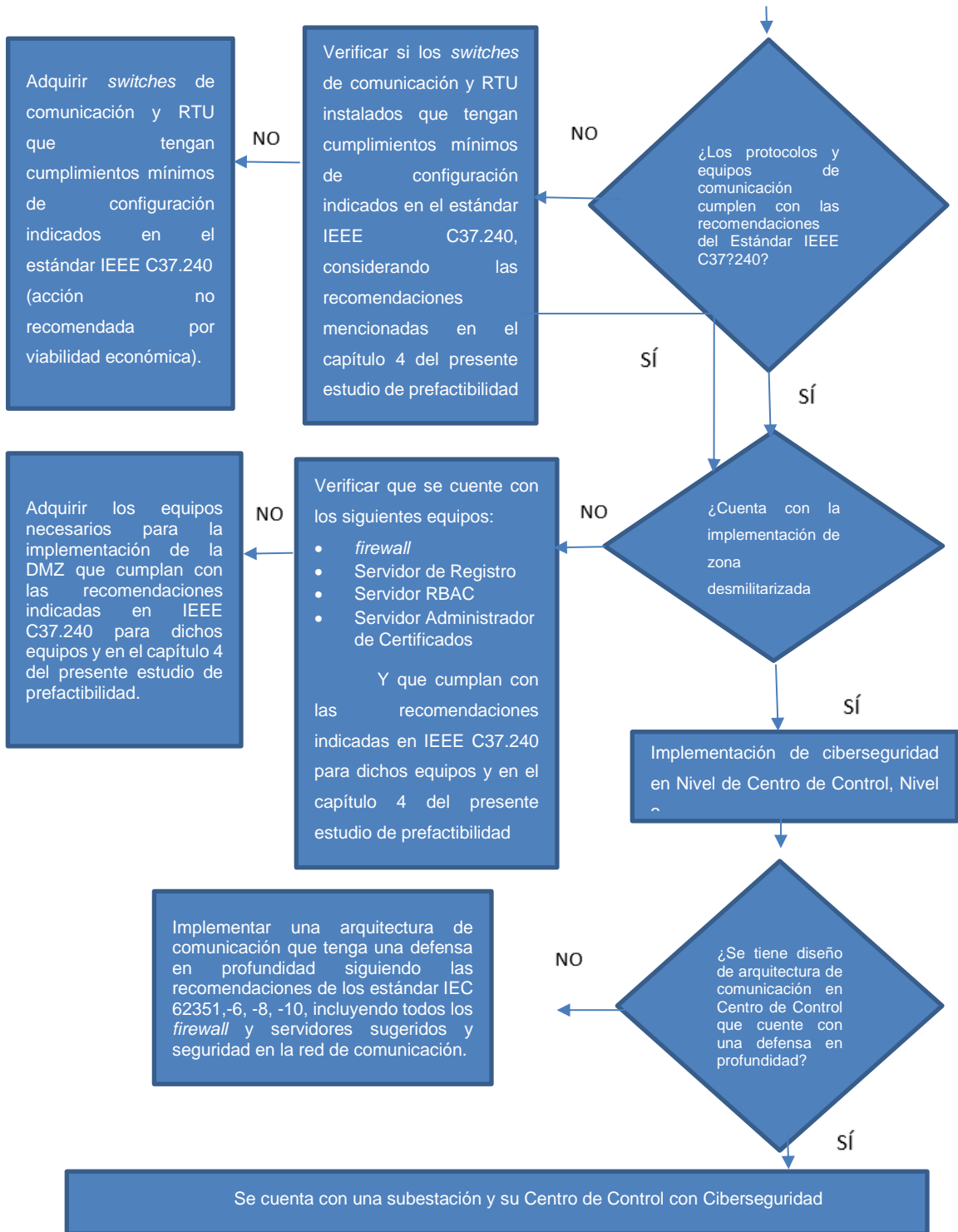
Implementación de ciberseguridad	Precio total en USD
Ciberseguridad en Nivel 0	6 662,24
Ciberseguridad en Nivel 1 (Configuración de equipos ya instalados y en servicio)	2 995,00
Ciberseguridad en Nivel 2	24 405,00
Ciberseguridad en Nivel 3	18 030,00
PRECIO TOTAL EN USD	45 430,00

Fuente: elaboración propia.

Figura 54. Diagrama de flujo de la implementación en subestaciones



Continuación de la figura 54.



Fuente: elaboración propia, empleando Visio 2016.

CONCLUSIONES

1. De acuerdo con el estudio de prefactibilidad realizado, para la implementar una correcta ciberseguridad en las subestaciones de transmisión del SNI, se determina que se obtienen beneficios técnicos de funcionalidad y de configuración en los dispositivos de protección, control, medición y comunicación; así como la correspondiente protección física de *hardware* y *software* de todos los equipos dentro de una subestación, tomando en cuenta lo referido en las siguientes normas: IEEE C37.240, IEEE 1686 y todas las normas recomendadas dentro de estas para los equipos en los niveles 0, 1 y 2 de la subestación. La IEC 62351, -6, -8, -10, IEEE 802.1 AE y la NERC CIP-007-6 para el nivel 3; de la IEC 62443-3-3 para la implementación de defensa en profundidad y *hardening* en los niveles 2 y 3, y de la IEC 62351-1 a la IEC 62351-10 para los protocolos de comunicación en todos los niveles de la subestación.
2. Tomando en cuenta la información contenida en el estudio causa raíz, se determina que las principales causas de falta de la adecuada implementación de ciberseguridad en subestaciones de transmisión en Guatemala, se debe a que las empresas implementaron las tecnologías operativas (OT), de manera separada a las tecnologías de la información (IT), sin considerar que la evolución de las tecnologías haría que estas dependieran una de la otra compartiendo vulnerabilidades. Al mismo tiempo, el hecho que ningún ciberataque se ha realizado hasta el momento en el SNI hace que las empresas no tomen acciones inmediatas para la implementación.

3. Respecto al crecimiento del PIB observado en el estudio de mercado, la economía para el sector eléctrico de Guatemala se recupera tras la caída que tuvo en el año 2020 debido a la pandemia Covid 19, se evidencia que a partir del año 2022 y su tendencia para el año 2023, la actividad económica se recupera de manera consecutiva, lo que hace posible la probabilidad de contar con mayor presupuesto en las empresas transportistas para invertir en proyectos de ciberseguridad en subestaciones.
4. Para el estudio económico realizado, se ha obtenido el monto aproximado de implementar ciberseguridad en una subestación y Centro de Control, el cual es de USD 52 092,24 de acuerdo con las premisas de este estudio. El monto relativamente bajo indicado, es de beneficio para las empresas transportistas porque de ocurrir un ciberataque en el SNI se tendrían pérdidas económicas de mayor valor. El beneficio aplica para dos casos, el primero, para las medidas y condiciones que se tomen desde el dimensionamiento de equipos objeto de la construcción de las subestaciones, y el segundo, para subestaciones que se encuentren en funcionamiento y que posean equipos de protección, control y medición que contengan en sus características de configuración la posibilidad de implementar medidas de ciberseguridad.
5. El principal método para contar con ciberseguridad en todos los niveles de una subestación y su Centro de Control, es la implementación de la zona desmilitarizada en el perímetro de la subestación, la realización de la configuración de las funciones de seguridad en los equipos de control, protección, medición y comunicaciones, y la protección física perimetral de acuerdo con lo recomendado en el estudio técnico.

6. La mejor configuración de una arquitectura de red en una subestación con ciberseguridad puede implementarse de buena manera considerando lo especificado en las normas IEEE C37.240, IEC 62351-3, -10 e IEC 62443-3, de manera que quede protegida toda la red LAN de la subestación que en conjunto con la implementación de la DMZ ofrecen *hardening* a los dispositivos de OT e IT.

7. Según el análisis que se realizó conforme a las tablas de cumplimiento de requisitos de ciberseguridad según norma IEEE 1686, las cuales se encuentran en la sección de anexos del presente estudio, se ha determinado que los equipos propuestos cumplen con la mayoría de requisitos técnicos recomendados por la norma, siendo éstos los equipos SIPROTEC 5, al igual que en la familia de *RTUs* para el SICAM PAS ambos de la marca SIEMENS, dejando pendientes únicamente algunas funciones de configuración que deben ser realizadas en sitio directamente, y son especificadas en el estudio técnico de acuerdo con la norma aplicada. Al mismo tiempo, se tiene buen cumplimiento por parte de los equipos de protección y control, así también como de las unidades terminales remotas de la marca SEL, y se listan en el estudio técnico las configuraciones que se deben realizar en sitio.

RECOMENDACIONES

1. Aplicar ciberseguridad en subestaciones eléctricas de transmisión, tomando como guía el presente estudio de prefactibilidad y aplicarlo de manera completa de acuerdo con las normas correspondientes.
2. Implementar métodos para la planeación del inicio de ejecución de programas de ciberseguridad al personal de las empresas que actualmente fungen como transmisores en el SNI, principalmente para personal que tiene acceso a las IT en la intersección de la subestación y Centro de Control, y de igual manera, sin restar importancia a los usuarios de ingeniería encargados del control y monitoreo de funciones de OT.
3. Evaluar el costo-beneficio para el caso en que ocurriera un ataque cibernético en el SIN, y que este provoque una falla a gran escala interrumpiendo la continuidad del suministro de energía por el tiempo que definan los atacantes. Se recomienda a las empresas transportistas analizar las pérdidas económicas relacionadas con la energía no entregada a los usuarios, esto, al dejar deshabilitado el sistema de control local y remoto, teniendo posibles demandas por consecuencias económicas negativas para las empresas generadoras y distribuidoras, así como para el resto de los agentes del Mercado Mayorista. Para las empresas transportistas se tendrían pérdidas de activos en las subestaciones atacadas, tanto en *hardware*, *software* de control y comunicaciones por ser alterados en su configuración y programación. Asimismo, según lo indicado en la Ley General de Electricidad, por parte de la Comisión Nacional de Energía Eléctrica se impondrían las sanciones

indicadas en la resolución CNEE-37-2020 para las Normas Técnicas de Calidad del Servicio de Transporte y Sanciones -NTCSTS-, y adicional, el incumplimiento de las responsabilidades indicadas en la Resolución 157-13, que corresponde a la norma de la Coordinación de la Operación en Tiempo Real en el numeral 2.2.6 Responsabilidades y obligaciones para la seguridad del SIN, del Administrador del Mercado Mayorista.

4. Analizar para la implementación de ciberseguridad en subestaciones, cada empresa de transmisión debe habilitar la configuración de los equipos respectivos con los protocolos adecuados para la protección de la información y eventos que se transmiten en el nivel 1, nivel 2 y nivel 3 de la subestación donde radica la importancia de protección en la comunicación.
5. Adoptar lo antes posible métodos de autenticación, auditoría y el control de acceso basado en roles, para limitar los accesos al sistema de las subestaciones.
6. Instalar defensa en profundidad para la arquitectura de red en una subestación considerando lo especificado en la norma IEC 62443-3.
7. Cambiar los equipos antiguos ya instalados en las subestaciones para cumplir con requerimientos de ciberseguridad y sustituirlos por equipos nuevos no es lo recomendable como acción inmediata. En todo caso, se debe reforzar la arquitectura de comunicación para que disminuyan vulnerabilidades en la subestación. Sin embargo, se recomienda cambiar a equipo nuevo con características de ciberseguridad en el momento de realizar una modernización o *retrofit*.

BIBLIOGRAFÍA

1. Banco de Guatemala. *Estudio de la Economía Nacional 2019*. Guatemala: BG, 2019. 178 p.
2. _____ . *Estudio de la Economía Nacional*. [en línea]. <<https://www.banguat.gob.gt/es/page/estudio-de-la-economia-nacional>>. [Consulta: 2 de octubre de 2021].
3. _____ . *Producto Interno Bruto (Tasas de variación)*. [en línea]. <<https://www.banguat.gob.gt/es/page/producto-interno-bruto-tasas-de-variacion>>. [Consulta: 1 de octubre de 2021].
4. _____ . *Producto Interno Bruto Trimestral. Estadísticas macroeconómicas cuentas nacionales*, año de referencia 2013. Guatemala: BG. 2013. 14 p.
5. Banco Mundial. *El Banco Mundial en Guatemala*. [en línea]. <<https://www.bancomundial.org/es/country/guatemala/overview#1>>. [Consulta: 2 de octubre de 2021].
6. Bastify.com *¿Qué es SHH y cómo funciona?* [en línea]. <<https://www.bastify.com/que-es-ssh-y-como-funciona/>>. [Consulta: 9 de octubre de 2021].

7. BEAMONTE, Paloma. *Grupo de hackers rusos se ha infiltrado en la red eléctrica de Estados Unidos*. [en línea]. <<https://hipertextual.com/2018/07/hackers-rusos-red-eeuu>>. [Consulta: 13 de noviembre de 2021].
8. CISCO. *Métodos de comunicación en switches CISCO*. [en línea]. <<https://netwgeeks.com/metodos-de-conmutacion-en-switches-cisco/>>. [Consulta: 16 de septiembre de 2021].
9. Comisión Federal de Electricidad. *Procedimiento para el análisis causa raíz (ACR), de fallas relevantes en equipos, accidentes e incidentes, ocurridos en las instalaciones de CFE*. México: CFE. 2008. 75 p.
10. DE LUZ, Sergio. *Mejora la seguridad de tu VPN con el protocolo IPsec*. [en línea]. <<https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/>>. [Consulta: 9 de octubre de 2021].
11. Deloitte. *Ciberseguridad en el sector eléctrico: amenazas para sistemas TI y OT*. Guatemala: Deloitte. 2020. 28 p.
12. Digital Guide IONOS. *Qué es SSH Todo sobre el protocolo de cifrado*. [en línea]. <<https://www.ionos.mx/digitalguide/servidores/herramientas/protocolo-ssh/>>. [Consulta: 10 de octubre de 2021].
13. EcuRed. *Puerta de enlace*. [en línea]. <https://www.ecured.cu/Puerta_de_enlace>. [Consulta: 17 de septiembre de 2021].
14. Expansión.com. *Ciberataque masivo contra empresas energéticas de Europa y EEUU: España es el país más afectado*. [en línea].

<<https://www.expansion.com/2014/07/01/empresas/energia/1404200654.html>>. [Consulta: 13 de noviembre de 2021].

15. FINN, John; KRIEG, Terry. *Study Committee B3: Substations*. Francia: International Council on Large Electric Systems (CIGRE). 2019. 1 079 p.
16. Fs.com. *Switch capa 3 vs el router: cuál es tu mejor alternativa*. [en línea]. <<https://community.fs.com/es/blog/layer-3-switch-vs-router-what-is-your-best-bet.html>>. [Consulta: 16 de septiembre de 2021].
17. GORDON, Clarke; REYNDERS, Deon; WRIGHT, Edwin. *Practical modern SCADA protocols: DNP3.0, 60870.5 y related systems*. 1a ed. 2004. 530 p.
18. GUIJARRO, Alfonso; YPEZ, Holdin; PERALTA, Tania. y ORTIZ, Mirella. *Defensa en profundidad aplicado a un entorno empresarial*. Venezuela: Revista Espacios, 2018. 9 p.
19. HIRSCHMANN, WP 1004HE-Part 5. *Cyber security in substation communication network*. Chicago: White Paper - Data Communication in Substation Automation System (SAS) 2012. 6 p.
20. HIRSCHMANN, WP00002. *Cyber security in electrical substations*. Chicago: White paper. 2015. 8 p.
21. Incibe-cert. *Cyber Kill Chain en sistemas de control industrial*. [en línea]. <<https://www.incibe-cert.es/blog/cyber-kill-chain-sistemas-control-industrial>>. [Consulta: 13 de noviembre de 2021].

22. Incibe-cert. *Protocolos AAA y control de acceso a red: Radius*. [en línea]. <<https://www.incibe-cert.es/blog/protocolos-aaa-radius>>. [Consulta: 23 de octubre de 2021].
23. Infotecs. *Gateway*. [en línea]. <<https://infotecs.mx/blog/gateway.html>>. [Consulta: 17 de septiembre de 2021].
24. Institute of Electrical and Electronics Engineers, Inc. *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*. New York: IEEE 1686. 2013. 29 p.
25. _____. *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection Automation, Protection, and Control Systems*. New York: IEEE Std C37.240. 2015. 40 p.
26. _____. *Media Access Control (MAC) Security. IEEE Std 802.1AE-2006*. USA: IEEE. 2018. 239 p.
27. _____. *Substation physical and electronic security*. IEEE Std 1402-2000, 3. Park Avenue New York, USA: IEEE. 2000. 24 p.
28. Instituto Nacional de Electrificación –INDE. *Empresa de transporte y control de energía eléctrica -ETCEE-*. [en línea]. <<http://www.inde.gob.gt/etcee/>>. [Consulta: 2 de octubre de 2021].
29. International Electrotechnical Commission. *Industrial communication networks – Network and System Security Part 1-1: Terminology, concepts and models*. Londres: International Standard IEC 62443-1-1. 2009. 86 p.

30. _____ . *Industrial communication networks – Network and System Security Part 1-1: Terminology, concepts and models*. Londres: International Standard IEC 62443-3-3. 2013. 170 p.
31. _____ . *Industrial Communication networks – High Availability Automation Networks – Part 3: Parallel redundancy protocol (PRP) and high – availability seamless redundancy (HSR)*. New York: Standard IEC 62439-3. 2018. 176 p.
32. _____ . *Industrial communication Networks-Network and System Security-Part 3-3: System security requirements and security levels*. New York: Standard IEC 2013. 58 p.
33. _____ . *Instrument Transformers-Part 8: Electronic current transformer*. New York. International Standard IEC 60044-8. 2002. 128 p.
34. _____ . *Power systems management and associated information exchange - data and communications security – Part 10: Security architecture guidelines*. Londres: Standard IEC. 62351-10. 2012. 54 p.
35. IST La Recoleta. *Topologías de red*. [en línea]. <<https://www.studocu.com/pe/document/universidad-tecnologica-del-peru/redes-y-comunicacion-de-datos-2/unidad-03-resumen-redes-y-comunicacion-de-datos-2/5118755>>. [Consulta: 25 de septiembre de 2021].

36. JIANG JUN; Ma, Guoming. *Optical sensing in power transformers*. Inglaterra: John Wiley & Sons Ltd, 2021. 256 p.
37. JIMENEZ MEZA, Obed Renato. *Protección de sistemas eléctricos de potencia*. México: Academia de Iluminación y Alta Tensión FIME UANL. 110 p.
38. LEE, Robert M; ASSANTE, Michael; CONWAY Tim. *Analysis of the Cyber Attack on the Ukrainian power grid*. Washington: Electricity Information Sharing and Analysis Center, E-ISAC. TLP: White Defense Use Case, 2016. 29 p.
39. LEVY, Alberto. *El impacto de COVID-19 en el sector eléctrico guatemalteco*. [en línea]. <<https://blogs.iadb.org/energia/es/el-impacto-de-covid-19-en-el-sector-electrico-guatemalteco/>>. [Consulta: 1 de octubre de 2021].
40. MIKOVÁ, Tímea. *Cyber Attack on Ukrainian power grid*. Trabajo de graduación en Relaciones Internacionales. Facultad de Ciencias Políticas, Universidad de Masaryk. 2018. 42 p.
41. Ministerio de Energía y Minas. *Dirección General de Energía. Estadísticas Subsector Eléctrico 2018*. Guatemala: MEM, 2019. 6 p.
42. MOUSSAMIR, Mohamed; DOLEZILEK, David. *The demands and implications of it and ot collaboration*. Sud Africa: Schweizer Engineering Laboratories, Inc. 2013. 13 p.

43. Oficina de Seguridad Interna. *Qué son los ataques DoS y DDoS*. [en línea]. <<https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos>>. [Consulta: 24 de septiembre de 2021].
44. PADILLA, Evelio. *Substation automation systems design and implementation*. 2016. Venezuela: Wiley. 272 p.
45. RAMIREZ, Carlos Felipe. *Subestaciones de alta y extra alta tensión*. 2a ed. Colombia: Impresiones Gráficas, LTDA. 1991. 767 p.
46. RAULL MARTÍN, José. *Diseño de subestaciones eléctricas*. 2a ed. México: UNAM, 2000. 545 p.
47. Redes Telemáticas. *El switch: cómo funciona y sus principales características*. [en línea]. <http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf/>. [Consulta: 16 de septiembre de 2021].
48. RODRÍGUEZ, Nubia; GUTIÉRREZ, Luis. *Caracterización de las subestaciones eléctricas de transmisión y distribución que hagan parte del SIN, del STR o del SDL dentro de la región central*. Colombia: Universidad Distrital Francisco José de Caldas. 2020. 138 p.
49. Schneider Electric. *Energy and power quality meter*. Estados Unidos: SE. 2021. 118 p.

50. Schweitzer Engineering Laboratories, Inc. *SEL-3555-2 Real-Time Automation Controller (RTAC). Instruction manual*. Washington: SEL. 2015. 16 p.
51. _____. *SEL-411L. Advanced line differential protection, automation, and control system*. Washington: SEL. 2015. 1624 p.
52. SIEMENS. *SICAM/SIPROTEC. System Hardening for Substation Automation and Protection. User Guide V01.30*. Alemania: SIEMENS. 2019. 72 p.
53. _____. *Secure Substation, Declaration of Security Conformance IEC 62443-3. Manual V1.00*. Alemania: SIEMENS. 2020. 31 p.
54. _____. *SIMATIC NET Rugged Ethernet Switches RUGGEDCOM ROS V5.5 for RSG2100, RSG2100P*. Alemania: SIEMENS. 2021. 408 p.
55. _____. *SIMATIC NET Rugged multi service platforms RUGGEDCOM ROX II V2.14 CLI for RX1500, RX1501, RX1510, RX1511, RX1512, RX1524, RX1536. RUGGEDCOM RX1500. Configuration Manual*. Alemania: SIEMENS. 2022. 1074 p.
56. SPURGEON Charles; ZIMMERMAN, Joann. *Ethernet, the definitive guide: designing and managing Local Area Networks*. 2a ed. Texas, USA: O'Reilly. 2014. 508 p.

57. Tecnología-informática. *Que es un firewall o cortafuegos. tipos.* [en línea]. <<https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/>>. [Consulta: 16 de septiembre de 2021].

58. UNLP. *Switch, routers y acces point, conceptos generales.* [en línea]. <http://www.trabajosocial.unlp.edu.ar/uploads/docs/switch__routers_y_acces_point__conceptos_generales.pdf/>. [Consulta: 16 de septiembre de 2021].

ANEXOS

Requerimientos de Ciberseguridad en IEDs Según Estándar IEEE 1686.

Anexo 1. **Tabla de cumplimiento según IEEE 1686 para relevador de protección modelo SIPROTEC 5 marca SIEMENS**

Requerimiento del Estándar	Cumplimiento del IED marca SIEMENS SIPROTEC 5
Características de ciberseguridad en el IED	Contiene tabla de cumplimiento de acuerdo con el estándar IEEE 1686:2013
Control de acceso electrónico	Se cumple Se desarrolla en los renglones siguientes:
Control de acceso al IED El acceso local estará protegido por una identificación de usuario única (ID) y combinaciones de contraseña	En la interfaz local del equipo el acceso se puede proteger utilizando ID de confirmación, o bien, activar la función de control de acceso basado en roles (RBAC) y de esta manera autenticar y autorizar usuarios para realizar operaciones críticas con escritura/control de acceso a el dispositivo
Mecanismos de anulación de contraseña El IED no tendrá ningún medio por el cual el control de ID o contraseña creado por el usuario pueda ser anulado o eludido.	Se cumple, El control ID y las contraseñas no puede ser anuladas o eludidas. No es posible ver ninguna de las configuraciones confidenciales, como la contraseña de conexión, el RADIUS precompartido clave, o la contraseña de la cuenta de emergencia con cualquier medio.
El mínimo número de usuarios individuales admitidos por el IED deberá ser de 10	Excede
Construcción de contraseña: Al menos 8 caracteres con las siguientes características: <ul style="list-style-type: none"> - Al menos una letra mayúscula y una minúscula - Al menos un número - Al menos un carácter no alfanumérico El IED no admitirá otro tipo de contraseña	Se cumple Tiene de 8 a 30 caracteres y debe incluir letras mayúsculas y minúsculas, dígitos y caracteres especiales

Continuación del anexo 1.

<p>Control de acceso al IED</p>	<p>Amplia funcionalidad de ciberseguridad, como control de acceso basado en roles (RBAC) a partir de V7.8, registro de eventos relacionados con la seguridad, <i>firmware</i> firmado o acceso a la red IEEE 802.1x autenticado, y como se detalla en los próximos dos ítems.</p>
<p>Niveles de autorización por contraseña</p>	<p>Se cumple con lo siguiente: Todo el sistema admitirá un control de acceso granular a los datos y los recursos. Con este fin, deberá Apoyar el concepto de usuario que cubre al menos los siguientes roles de usuario:</p> <ul style="list-style-type: none"> • Administrador • Usuario • Usuario de solo lectura
<p>Autorización mediante el control de acceso basado en roles (RBAC) El IED tendrá la capacidad de definir al menos cuatro roles definidos por el usuario, cada rol tendrá la capacidad de combinar las funciones enumeradas a continuación:</p>	<p>Con excepción: Se designa el concepto de usuario que cubre al menos los siguientes roles de usuario:</p> <ul style="list-style-type: none"> • Administrador • Usuario • Usuario de solo lectura
<p>Principales funciones de seguridad en IED:</p> <ul style="list-style-type: none"> • Ver datos operativos • Ver ajustes de configuración • Valores de fuerza • Cambio de configuración • Cambio de <i>firmware</i> • La gestión de ID/contraseña o RBAC • Contener Pista de auditoría (Audit Trail) 	<p>Se cumplen todos de acuerdo con:</p> <ul style="list-style-type: none"> • Para poder ver los datos operativos, se cumple para el rol de Administrador y usuario. • Para ver los ajustes de configuración, aplican los roles de administrador y usuario. • Los cambios de los valores de fuerza están relacionados únicamente al Administrador. • El cambio de configuración está permitido únicamente para el administrador. • El cambio de <i>firmware</i> está autorizado únicamente para el rol de administrador. • La gestión de contraseñas es para el rol de administrador, la aplicación utilizará usuarios personales para identificar y autenticar a cada usuario individual. • Pistas de auditoría: Si RBAC está habilitado en el relé SIPROTEC 5, solo los usuarios asignados con el rol de Auditor de seguridad, • El administrador de seguridad o el administrador pueden acceder al búfer de registro de seguridad interno del dispositivo. • Con fines de visualización y archivo

Continuación del anexo 1.

<p>Visualización de contraseña Solo se mostrarán las ID de usuario en las pantallas, las listas de auditoría, el área de memoria o los archivos y otros registros y archivos de configuración.</p>	<p>Se cumple. Solo se muestran registros y archivos de configuración.</p>
<p>Tiempo de espera de Acceso El IED tendrá una función de tiempo de espera que desconecta automáticamente a un usuario que ha iniciado sesión después de un periodo de inactividad del usuario.</p>	<p>Después de 10 minutos de inactividad del usuario en la interfaz local, el dispositivo requiere el suministro del código de identificación de confirmación correspondiente una vez más para cualquier actividad posterior relevante para la seguridad.</p>
<p>Pista de auditoría (Audit Trail)</p>	<p>Se cumple en los renglones desglosados</p>
<p>Antecedentes Audit Trail El IED registrará en una memoria intermedia circular secuencial, no habrá capacidad de borrar o modificar la Audit Trail, ya que debe mantener la integridad</p>	<p>El dispositivo de protección Siprotec 5, brinda un búfer de mensajes operativos, en el que los eventos más relevantes para la aplicación se almacenan en orden cronológico con estampa de tiempo.</p>
<p>Capacidad de almacenamiento La Audit Trail debe almacenar al menos 2048 eventos antes de que la memoria intermedia circular comience a sobrescribir el evento más antiguo con el evento más nuevo.</p>	<p>Las entradas del registro de seguridad se almacenan en un búfer circular no volátil interno del dispositivo protegido con una capacidad de almacenamiento de 2048 entradas.</p>
<p>Registro de almacenamiento (Storage record) Para cada evento de auditoría, se debe registrar la siguiente información:</p> <ul style="list-style-type: none"> • Número de registro de evento • Hora y fecha • Identificación de usuario • Tipo de evento 	<p>El status se presenta que se cumple, incluyendo lo siguiente:</p> <p>El sistema registra las acciones del usuario, así como las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. Durante un período de tiempo mínimo configurable, estos registros registrarán la fecha y la hora, los usuarios y sistemas involucrados, así como el evento real y el resultado.</p>
<p>Tipos de eventos de seguimiento de auditoría</p> <ul style="list-style-type: none"> • Iniciar sesión • Cierre de sesión manual • Cierre de sesión programado • Valor forzado • Configuración de acceso • Cambio de configuración • Cambio de <i>firmware</i> • Creación o modificación de ID/contraseña • Eliminación de IED/contraseña 	<p>Para el dispositivo Siprotec 5, se cumple:</p> <ul style="list-style-type: none"> • Inicio de sesión: Se da cumplimiento con el sistema al registrar las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. • Cierre de sesión manual: Cumple • Cierre de sesión programado: Cumple

Continuación del anexo 1.

<ul style="list-style-type: none"> • Acceso al registro de auditoría • Hora/cambio de fecha • Alarma 	<ul style="list-style-type: none"> • Valor forzado: Acción de un usuario que ha iniciado sesión que anula datos reales con entrada manual y provoca una operación de control. • Configuración de acceso: Cumple • Cambio de configuración: Cumple • Cambio de <i>firmware</i>: Cumple • Creación o modificación de ID/Contraseña: Dependerá de roles de usuario, donde el administrador es quien tiene la posibilidad de cambiar contraseña, y al mismo tiempo se respalda por la Autenticación e inicio de sesión de usuario. • Eliminación de IED/Contraseña: Opción incluida en los Roles de usuario, la cual únicamente el administrador tiene derechos para realizar cambios de este tipo, y para lo cual, sin una autenticación de usuario exitosa, el sistema solo permitirá un rango de acciones definidas. • Acceso al registro de auditoría: Cumple • Hora/cambio de fecha: Cumple • Alarma: Función que se cumple con el inicio de sesión, será posible incluir mensajes relacionados con la seguridad en una gestión de alarmas preexistente.
<p>Supervisión y control de supervisión</p>	<p>Ciberseguridad según NERC CIP y requerimientos BDEW Whitepaper.</p> <p>Las demás funciones se detallan en los siguientes renglones.</p>
<p>Resumen de supervisión y control de supervisión El IED supervisará la actividad relacionada con la seguridad y pondrá la información a disposición de una comunicación en tiempo real para su transmisión a un sistema de supervisión, un SCADA</p>	<p>Cumple En general, solo los estándares y protocolos de comunicación seguros que incluyen protección de integridad Se utilizará la autenticación y cifrado, siempre que la tecnología lo permita. Este es un requisito no negociable para cualquier protocolo utilizado para la administración remota y la parametrización y también se debe tener en cuenta cuando no sea estándar y se utilizan protocolos patentados.</p>
<p>Eventos Actividades que se pueden esperar que ocurran en la rutina de uso y mantenimiento del IED.</p>	<p>Cumple Los IED SIPROTEC 5 transmiten activamente eventos de seguridad y alarmas a través del protocolo Syslog UDP (si esta opción está habilitada).</p>

Continuación del anexo 1.

<p>Alarmas Las alarmas son actividades que pueden identificar una actividad no autorizada,</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido • Reiniciar • Intento de uso de software de configuración no autorizado • Configuración inválida o descarga de firmawre • Configuración no autorizada o archivo de <i>firmware</i> • Señal de tiempo fuera de tolerancia: el IED tendrá que validar el tiempo de sincronización de los mensajes recibidos a través de protocolo o dedicar canales de tiempo de sincronización. • Cambios de hardware de campo no válidos 	<p>Siprotec 5 puede cumplir con lo siguiente:</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido, se cumple • Reiniciar: Cumple con las opciones de inicio de sesión, Será posible incluir mensajes de registro relacionados con la seguridad en una gestión de alarmas preexistente. • Intento de uso de software de configuración no autorizado: • Los dispositivos SIPROTEC 5 pueden configurarse para aceptar únicamente conexiones de instalaciones DIGSI 5 que presenten estos certificados durante el protocolo de enlace TLS inicial. • Configuración inválida o descarga de firmware: Cumple. • Señal de tiempo fuera de tolerancia: Actualmente verificado, pero no registrado • Cambios de hardware de campo no válidos: Actualmente verificado, pero no registrado
<p>Detección de cambio de punto de alarma Los puntos de alarma tendrán la capacidad de detectar momentáneamente la ocurrencia de una alarma.</p>	<p>Cumple con lo siguiente: Será posible incluir mensajes de registro relacionados con la seguridad en una gestión de alarmas preexistente.</p>
<p>Grupos de Eventos y alarmas Se proporcionará un medio que permita al usuario agrupar eventos y alarmas.</p>	<p>Cumple con lo siguiente: Configurable usando como CFC</p>
<p>Control permisivo de supervisión El IED proporcionará un mecanismo que, cuando este habilitado, requiere permiso antes de realizar acciones para la supervisión independiente o requiere en el campo y remotamente.</p>	<p>Con excepción: Se admite el control de supervisión de la operación. No se admite la activación / desactivación del registro de seguridad mediante el sistema de supervisión.</p>
<p>Funciones de ciberseguridad del IED Compromiso de funcionalidad del IED</p>	<p>Se describen en los siguientes renglones El compromiso de funcionalidad del IED se cumple con lo siguiente: Con excepción para aplicación de parches y gestión de parches. Todos los componentes del sistema deben poder parchearse. La integridad de los parches y actualizaciones de seguridad se podrá verificar mediante un mecanismo criptográfico.</p>

Continuación del anexo 1.

<p>Principales características criptográficas:</p> <ul style="list-style-type: none"> • La funcionalidad del servidor web proporcionada por el IED será protocolo HTTPS • Funcionalidad de transferencia de archivos proporcionada por el IED deberá ser SFTP • Facilidades de comunicación orientada al texto usando una conexión terminal virtual a través de una red basada en Ethernet será un Shell seguro (SSH) • Implementación de SNMPv3. • La sincronización del tiempo en la red será NTP, la funcionalidad de la sincronización en la red implementada será NTP v3/4 o SNTP3/4. • Funcionalidad de túnel seguro proporcionada por el IED será una red privada virtual VPN 	<ul style="list-style-type: none"> • Siptorec 5 cuenta con conexión HTTPS a DIGSI 5 y el servidor web HTTPS para el acceso al navegador web están activados en el dispositivo. • La transferencia de archivos segura se logra a través de HTTPS, no SFTP. • Facilidades de comunicación orientada al texto: No se admite la conexión de terminal orientada a texto. Por tanto, este requisito no es aplicable. • Implementación de SNMPv3: • Los relés SIPROTEC 5 brindan información de monitoreo de activos para sus módulos de red a través de protocolos estándar como SNMPv3 e IEC 61850-MMS. • Sincronización del tiempo en la red: Se cumple con UDP se utiliza para la sincronización de la hora a través de NTP • El dispositivo no admite ninguna función de tunelización.
<p>Técnicas criptográficas</p>	<p>Con las siguientes excepciones:</p> <p>Al seleccionar los mecanismos criptográficos, se tendrá en cuenta la legislación nacional. Solo se utilizarán mecanismos aprobados y tamaños mínimos de clave que se consideren seguros para el futuro previsible de acuerdo con los conocimientos tecnológicos más avanzados. El proveedor no utilizará algoritmos criptográficos personalizados.</p> <p>Para productos SIPROTEC 5 y DIGSI 5, el método de cifrado reconocido se utiliza con TLS 1.2.</p>
<p>Encriptación de comunicación serial Los IEDs serán capacitados para emplear comunicación por cualquier aplicación de acceso remota (transferencia de datos, configuración, carga de <i>firmware</i>, entre otros). deberá proporcionar encriptación de acuerdo con IEEE 1711 para todos los puertos designados a permitir acceso remoto.</p>	<p>No se admite la comunicación en serie para acceso remoto</p>
<p>Configuración del Software de IED</p>	<p>Se describen en los renglones siguientes</p>

Continuación del anexo 1.

<p>Autenticación Se evitará que las copias no autorizadas del software de configuración accedan a las funciones del IED.</p>	<p>Este requerimiento es excedido por los dispositivos Siprotec 5, con la siguiente característica:</p> <p>A partir de la versión de <i>firmware</i> SIPROTEC 5 y la versión DIGSI 5 V7.90 y superior, los clientes pueden emitir certificados de cliente X.509 a sus instancias legítimas de DIGSI 5 con su propia PKI / Autoridad de certificación (CA). Pueden configurar los IED SIPROTEC 5 para que solo acepten solicitudes de conexión de las instancias DIGSI 5 legítimas confiando en la CA en los dispositivos, para los siguientes escenarios:</p> <ul style="list-style-type: none"> • Autenticación de servidor para ingeniería web. • Ingeniería basada en PC (DIGSI 5) con autenticación mutua. • Seguridad de acceso al puerto sobre EAP-TLS para módulos de comunicación de instalación (Rol de solicitante IEEE 802.1X)
<p>Firma digital La configuración del software tendrá la capacidad para generar archivos de descarga de configuración y <i>firmware</i> indicando que el archivo ha sido producido por una configuración autorizada de software y por un usuario autorizado. El IED aceptará únicamente archivos debidamente firmados.</p>	<p>Se cumple con lo siguiente:</p> <p>El dispositivo solo acepta <i>firmware</i> y configuración con una firma digital emitida a los archivos de <i>firmware</i> / configuración en nuestras instalaciones de fabricación seguras.</p> <p>Los ficheros del <i>firmware</i> de equipo SIPROTEC 5 están firmados digitalmente. De esta manera, se evita con seguridad una falsificación exterior causada por virus o troyanos, por ejemplo, ficheros de Firmware manipulados.</p> <p>Implica de igual manera, protección contra <i>malware</i>.</p>
<p>Control ID/contraseña La configuración del software será controlada por ID / contraseña para que el software no pueda ser accesado sin la combinación adecuada del ID/contraseña.</p>	<p>Se da cumplimiento con excepciones: Acceso autenticado y autorizado al DIGSI 5 El software de ingeniería es compatible con los usuarios individuales del software DIGSI 5 a través de un usuario central y la gestión de RBAC en Active Directory.</p> <p>El sistema admitirá una política de contraseñas de última generación.</p>

Continuación del anexo 1.

<p>Cambiar datos de configuración Cambiar y guardar datos de configuración y revisión de archivos de <i>firmware</i> que se cargarán en el IED:</p> <ul style="list-style-type: none"> • Acceso completo • Seguimiento de cambios • Monitoreo de uso • Descargas del IED 	<ul style="list-style-type: none"> • Se cumple con el acceso completo y se aplica con el rol de administrador. • Se cumple con el seguimiento de cambios • Se cumple con el monitoreo de uso • Se cumple con las descargas del IED: Para cada archivo de software y <i>firmware</i> descargable, se publica en Internet la huella digital hash SHA256 correspondiente. Los clientes pueden utilizar herramientas como Certutil en Microsoft Windows para generar la huella digital hash SHA256 para un archivo que descargan. Pueden comprobar si es idéntica a la huella dactilar publicada, verificando así la integridad del archivo.
<p>Acceso al Puerto de comunicaciones Todos los puertos de comunicaciones, ya sean físicos o lógicos, otros que el puerto de diagnóstico en los IED tendrá la capacidad para ser habilitados o deshabilitados por medio de la configuración del IED.</p>	<p>Cumple: Segregación de puertos Ethernet</p> <p>En la mayoría de los modos, los puertos Ethernet habilitados admiten tráfico IP y protocolos de capa 2 (es decir, IEC 61850 GOOSE). Si NETMODE = ISOLATEIP, entonces un puerto solo permite el tráfico GOOSE.</p>
<p>Aseguramiento de calidad de Firmware El aseguramiento de calidad del Firmware deberá cumplir con IEEE C37.231, práctica recomendada para el control de <i>firmware</i> de equipos de protección basados en microprocesadores</p>	<p>Excepción: Siemens desarrolla SIPROTEC 5 y DIGSI 5 de acuerdo con el reconocido proceso de desarrollo y garantía de calidad de CMMI. Los estrictos procesos de control de calidad cubren las prácticas recomendadas por IEEE Std. C37.231.</p>

Fuente: SIEMENS. *SIPROTEC 5 / DIGSI 5: Declaration of security conformance. manual v02.01*. pp. 24-29, 35-37.

Anexo 2. **Tabla de cumplimiento según IEEE 1686 para relevador de protección modelo 477L marca SEL**

Requerimiento del Estándar	Cumplimiento del IED marca SEL
Características de ciberseguridad en el IED	Según NERC CIP
Control de acceso electrónico	Cuando tres intentos sucesivos de inicio de sesión fallan como resultado de una entrada de contraseña incorrecta, el relé bloquea los intentos de inicio de sesión en ese puerto durante 30 segundos. También pulsa el bit BADPASS Relay Word.
Control de acceso al IED El acceso local estará protegido por una identificación de usuario única (ID) y combinaciones de contraseña	Los relés de la serie admiten ocho niveles de acceso, como se describe en Niveles de acceso y contraseñas
Mecanismos de anulación de contraseña El IED no tendrá ningún medio por el cual el control ID o contraseña creado por el usuario pueda ser anulado o eludido.	Cumple
El mínimo número de usuarios individuales admitidos por el IED deberá ser de 10	6 usuarios
Construcción de contraseña: Al menos 8 caracteres con las siguientes características: <ul style="list-style-type: none"> • Al menos una letra mayúscula y una minúscula • Al menos un número • Al menos un carácter no alfanumérico El IED no admitirá otro tipo de contraseña	Cada relé admite contraseñas seguras de hasta 12 caracteres, incluido cualquier carácter imprimible, lo que permite a los usuarios seleccionar contraseñas complejas si así lo desean. SEL recomienda que las contraseñas contengan un mínimo de ocho caracteres que contengan al menos uno de cada uno de los siguientes: letra minúscula, letra mayúscula, número y carácter especial.
Control de Acceso al IED <ul style="list-style-type: none"> • Niveles de autorización por contraseña • Autorización mediante el control de acceso basado en roles (RBAC) 	Cumple con nivel de autorización por contraseña, Debe configurarse el control de acceso basado en roles
Niveles de autorización por contraseña	Cumple
Autorización mediante el control de acceso basado en roles (RBAC) El IED tendrá la capacidad de definir al menos cuatro roles definidos por el usuario, cada rol tendrá la capacidad de combinar las funciones enumeradas a continuación:	Se describe en los renglones siguientes

Continuación del anexo 2.

<p>Principales funciones de seguridad en IED:</p> <ul style="list-style-type: none"> • Ver datos operativos • Ver ajustes de configuración • Valores de fuerza • Cambio de configuración • Cambio de <i>firmware</i> • La gestión de ID/contraseña o RBAC • Contener Pista de auditoría (Audit Trail) 	<ul style="list-style-type: none"> • Datos operativos: se ve el status de la información por medio de los niveles de acceso • Ajustes de configuración: Cumple • Valores de fuerza: Se incluye únicamente para DNP3 • Cambio de configuración solo para ciertos niveles de acceso. • No define que usuarios se autorizan para el cambio de <i>firmware</i>, debe configurarse únicamente para rol de administrador • Debe configurarse la gestión de contraseña • No indica que usuario puede configurar pistas de auditoría, se aplica el registrador de eventos secuenciales
<p>Visualización de contraseña Solo se mostrarán las ID de usuario en las pantallas, las listas de auditoría, el área de memoria o los archivos y otros registros y archivos de configuración.</p>	<p>Con registros y archivos de configuración y eventos</p>
<p>Tiempo de espera de Acceso El IED tendrá una función de tiempo de espera que desconecta automáticamente a un usuario que ha iniciado sesión después de un periodo de inactividad del usuario.</p>	<p>Cumple</p>
<p>Pista de auditoría (Audit Trail)</p>	<p>Descripción en los renglones siguientes</p>
<p>Antecedentes Audit Trail El IED registrará en una memoria intermedia circular secuencial, no habrá capacidad de borrar o modificar la Audit Trail, ya que debe mantener la integridad</p>	<p>Con excepción: Memoria no volátil que almacena las últimas 1000 entradas del registrador de eventos secuenciales</p>
<p>Capacidad de almacenamiento La Audit Trail debe almacenar al menos 2048 eventos antes de que la memoria intermedia circular comience a sobrescribir el evento más antiguo con el evento más nuevo.</p>	<p>Con excepción para historial de eventos: El historial de eventos le brinda un vistazo rápido a la actividad reciente de relevos. El relé etiqueta cada nuevo evento con un número único de 10000 a 42767. (En 42767 el relé vuelve a 10000 para el siguiente número de evento y luego continúa incrementándose)</p>

Continuación del anexo 2.

<p>Registro de almacenamiento (Storage record) Para cada evento de auditoría, se debe registrar la siguiente información:</p> <ul style="list-style-type: none"> • Número de registro de evento • Hora y fecha • Identificación de usuario • Tipo de evento 	<p>Con excepción: El registrador de eventos secuenciales, tiene la capacidad de registrar la siguiente información:</p> <ul style="list-style-type: none"> • Encabezado del informe estándar <ul style="list-style-type: none"> ○ Identificación de relés y terminales ○ Fecha y hora del informe • Número • Fecha y Hora • Elemento o condición del relé • Estado del elemento • Estados de puesta en servicio de TIDL.
<p>Tipos de eventos de seguimiento de auditoría</p> <ul style="list-style-type: none"> • Iniciar sesión • Cierre de sesión manual • Cierre de sesión programado • Valor forzado • Configuración de acceso • Cambio de configuración • Cambio de <i>firmware</i> • Creación o modificación de ID/contraseña • Eliminación de IED/contraseña • Acceso al registro de auditoría • Hora/cambio de fecha • Alarma 	<ul style="list-style-type: none"> • Inicio de sesión: por medio del registrador de eventos secuenciales. • Cierre de sesión manual: No configurado. • Cierre de sesión programado: No configurado. • Cambio de configuración: Cumple con el registrador de eventos secuenciales. • Cambio de <i>firmware</i>: Cumple con el registrador de eventos secuenciales. • Creación o modificación de contraseña: Cumple con el registrador de eventos secuenciales. • Eliminación de contraseña: No configurado. • Acceso al registro de auditoría: Cumple con el registrador de eventos secuenciales. • Alarma: Cumple con el registrador de eventos secuenciales.
<p>Supervisión y control de supervisión</p>	<p>Descritos en los renglones siguientes</p>
<p>Resumen de supervisión y control de supervisión El IED supervisará la actividad relacionada con la seguridad y pondrá la información a disposición de una comunicación en tiempo real para su transmisión a un sistema de supervisión, un SCADA</p>	<p>Cumple para enviar la información a una RTU</p>

Continuación del anexo 2.

<p>Eventos Actividades que se pueden esperar que ocurran en la rutina de uso y mantenimiento del IED</p>	<ul style="list-style-type: none"> • Inicio de sesión: por medio del registrador de eventos secuenciales. • Cierre de sesión manual: No configurado. • Cierre de sesión programado: No configurado. • Cambio de configuración: Cumple con el registrador de eventos secuenciales. • Cambio de <i>firmware</i>: Cumple con el registrador de eventos secuenciales • Creación o modificación de contraseña: Cumple con el registrador de eventos secuenciales • Eliminación de contraseña: No configurado • Acceso al registro de auditoría: Cumple con el registrador de eventos secuenciales • Alarma: Cumple con el registrador de eventos secuenciales
<p>Alarmas Las alarmas son actividades que pueden identificar una actividad no autorizada,</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido • Reiniciar • Intento de uso de software de configuración no autorizado • Configuración inválida o descarga de <i>firmware</i> • Configuración no autorizada o archivo de <i>firmware</i> • Señal de tiempo fuera de tolerancia: el IED tendrá que validar el tiempo de sincronización de los mensajes recibidos a través de protocolo o dedicar canales de tiempo de sincronización. • Cambios de hardware de campo no válidos. 	<p>El relé proporciona los siguientes bits de Palabra de relé que son útiles para monitorear el acceso al relé:</p> <ul style="list-style-type: none"> • BADPASS: pulsa durante un segundo si un usuario ingresa tres contraseñas incorrectas sucesivas. • ACCESO: se establece cuando cualquier usuario está conectado al nivel de acceso B o superior. • ACCESSP: pulsa durante un segundo cada vez que un usuario accede a un nivel de acceso de B o superior. • PASSDIS: se establece si está instalado el puente de desactivación de contraseña. • BRKENAB: se establece si está instalado el puente de activación del control del disyuntor. • INK5A, LINK5B, LINK5C, LINK5D: se configura mientras el enlace está activo en el puerto Ethernet respectivo. La pérdida de enlace puede ser una indicación de que se ha desconectado un cable Ethernet.

Continuación del anexo 2.

	<ul style="list-style-type: none"> LNKFAIL: se establece si se pierde el enlace en cualquier puerto de bus de estación activo. Para relés con solo dos puertos Ethernet, LNKFAIL afirma si se pierde el enlace en cualquier puerto. LNKFL2: se establece si se pierde el enlace en el puerto de bus de proceso activo (Ethernet)
Detección de cambio de punto de alarma Los puntos de alarma tendrán la capacidad de detectar momentáneamente la ocurrencia de una alarma.	No configurado
Grupos de Eventos y alarmas Se proporcionará un medio que permita al usuario agrupar eventos y alarmas.	No disponible
Control permisivo de supervisión El IED proporcionará un mecanismo que, cuando este habilitado, requiere permiso antes de realizar acciones para la supervisión independiente o requiere en el campo y remotamente.	No disponible
Funciones de ciberseguridad del IED	Se describen en los renglones siguientes
Compromiso de funcionalidad del IED	Con excepción Funcionalidad de control del IED
Principales características criptográficas: <ul style="list-style-type: none"> La funcionalidad del servidor web proporcionada por el IED será protocolo HTTPS Funcionalidad de transferencia de archivos proporcionada por el IED deberá ser SFTP Facilidades de comunicación orientada al texto usando una conexión terminal virtual a través de una red basada en Ethernet será un Shell seguro (SSH) Implementación de SNMPv3. La sincronización del tiempo en la red será NTP, la funcionalidad de la sincronización en la red implementada será NTP v3/4 o SNTP3/4. Funcionalidad de túnel seguro proporcionada por el IED será una red privada virtual VPN 	<ul style="list-style-type: none"> Servidor web proporcionada por HTTP La transferencia de archivos segura se logra a través de HTTPS, no SFTP. Comunicación por SSH: No configurada. Implementación por SNMPv3: No configurada/no incluida Sincronización del tiempo en la red: Se cumple con UDP se utiliza para la sincronización de la hora a través de NTP No incluida funcionalidad de túnel seguro

Continuación del anexo 2.

<p>Técnicas criptográficas</p>	<ul style="list-style-type: none"> • Cifrado de bloque: cumple • Autenticación de entidad: cumple • Mensaje de autenticación: cumple • Establecimiento de clave: cumple
<p>Encriptación de comunicación serial Los IEDs serán capacitados para emplear comunicación por cualquier aplicación de acceso remota (transferencia de datos, configuración, carga de <i>firmware</i>, entre otros), deberá proporcionar encriptación de acuerdo con IEEE 1711 para todos los puertos designados a permitir acceso remoto.</p>	<p>No aplica en Relevadores SEL</p>
<p>Configuración del Software de IED</p>	<p>Descritos en los renglones siguientes</p>
<p>Autenticación Se evitará que las copias no autorizadas del software de configuración accedan a las funciones del IED.</p>	<p>Se cumple</p>
<p>Firma digital La configuración del software tendrá la capacidad para generar archivos de descarga de configuración y <i>firmware</i> indicando que el archivo ha sido producido por una configuración autorizada de software y por un usuario autorizado. El IED aceptará únicamente archivos debidamente firmados.</p>	<p>Con excepción: No se admiten software de otras marcas y únicamente por usuarios autorizados, habilitar firma digital para actualización de software</p>
<p>Control ID/contraseña La configuración del software será controlado por ID / contraseña para que el software no pueda ser accedido sin la combinación adecuada del ID/contraseña.</p>	<p>Con excepción: Se cumple la contraseña para acceder al software, sin embargo, no se cumple con las combinaciones de contraseña sugeridas.</p>
<p>Cambiar datos de configuración Cambiar y guardar datos de configuración y revisión de archivos de <i>firmware</i> que se cargarán en el IED:</p> <ul style="list-style-type: none"> • Acceso completo • Seguimiento de cambios • Monitoreo de uso • Descargas del IED 	<p>Se cumple</p>
<p>Acceso al Puerto de comunicaciones Todos los puertos de comunicaciones, ya sean físicos o lógicos, otros que el puerto de diagnóstico en los IED tendrá la capacidad para ser habilitados o deshabilitados por medio de la configuración del IED.</p>	<p>Se deben configurar</p>

Continuación del anexo 2.

<p>Aseguramiento de calidad de Firmware El aseguramiento de calidad del Firmware deberá cumplir con IEEE C37.231, práctica recomendada para el control de <i>firmware</i> de equipos de protección basados en microprocesadores</p>	<p>Con excepción: Los relés de la serie SEL-400 son dispositivos integrados que no permiten la instalación de software adicional. Los relés de la serie SEL-400 incluyen una autocomprobación que verifica continuamente el código en ejecución con la versión de referencia del código en buen estado conocido en la memoria no volátil.</p>
--	---

Fuente: SEL-411L. *Advanced line differential protection, automation, and control system.*
pp. 1-5.

Anexo 3. **Tabla de cumplimiento según IEEE 1686 para relevador de protección modelo SIPROTEC 4 marca SIEMENS**

Requerimiento del Estándar	Cumplimiento del IED marca SIEMENS Siprotec 4
Características de ciberseguridad en el IED	Se da cumplimiento de la tabla de acuerdo con IEEE 1686:2013
Control de acceso electrónico	Con Excepción, como se desglosa en los siguientes dos renglones.
<p>Control de acceso al IED El acceso local estará protegido por una identificación de usuario única (ID) y combinaciones de contraseña</p>	<p>Con excepción El control de acceso al IED se da por los siguientes métodos:</p> <ul style="list-style-type: none"> • Niveles de autorización por contraseña • Autorización mediante control de acceso basado en roles
<p>Mecanismos de anulación de contraseña El IED no tendrá ningún medio por el cual el control ID o contraseña creado por el usuario pueda ser anulado o eludido.</p>	<p>Con Excepción: El Siprotec 4 no tiene ningún medio por el cual el control ID y las contraseñas no pueden ser anuladas o eludidas, se requiere la autenticación con un PIN máximo de 8 dígitos antes de transmitir parámetros al dispositivo.</p>
El mínimo número de usuarios individuales admitidos por el IED deberá ser de 10	

Continuación del anexo 3.

<p>Construcción de contraseña: Al menos 8 caracteres con las siguientes características:</p> <ul style="list-style-type: none"> • Al menos una letra mayúscula y una minúscula • Al menos un número • Al menos un carácter no alfanumérico <p>El IED no admitirá otro tipo de contraseña</p>	<p>Con excepción:</p> <p>El Siprotec 4, admite una contraseña de acceso no autorizado, también cuenta con la posibilidad de crear una contraseña que se puede configurar para evitar el acceso remoto no autorizado.</p> <p>Ambas contraseñas admiten de 8 a 24 caracteres ASCII que deben incluir letras mayúsculas y minúsculas, números y caracteres especiales. Si se utilizan caracteres que no son ASCII en estas contraseñas, se aplicará una restricción de longitud de contraseña de 8 a 24 caracteres.</p>
<p>Control de Acceso al IED</p>	<p>Con excepción</p> <p>Todo el sistema admitirá un control de acceso granular a los datos y los recursos. Con este fin, apoyará el concepto de usuario que cubra al menos los siguientes roles de usuario:</p> <ul style="list-style-type: none"> • Administrador • Usuario • Usuario de solo lectura
<p>Niveles de autorización por contraseña</p>	<p>Con excepción:</p> <p>Se otorga la capacidad de asignar autorización para utilizar funciones y características del IED de acuerdo con los roles de usuario que se implementan en el dispositivo.</p>
<p>Autorización mediante el control de acceso baso en roles (RBAC) El IED tendrá la capacidad de definir al menos cuatro roles definidos por el usuario, cada rol tendrá la capacidad de combinar las funciones enumeradas a continuación:</p>	<p>Con excepción:</p> <p>El IED Siprotec 4 apoya el concepto de usuario que cubra al menos los siguientes roles de usuario:</p> <ul style="list-style-type: none"> • Administrador • Usuario • Usuario de solo lectura
<p>Principales funciones de seguridad en IED:</p> <ul style="list-style-type: none"> • Ver datos operativos • Ver ajustes de configuración • Valores de fuerza • Cambio de configuración • Cambio de <i>firmware</i> • La gestión de ID/contraseña o RBAC • Contener Pista de auditoría (Audit Trail) 	<p>Se cumple para caso en particular:</p> <ul style="list-style-type: none"> • Con excepción: Para poder ver los datos operativos, se cumple para el rol de Administrador. • Con excepción: Para ver los ajustes de configuración, aplican los roles de administrador y usuario. • Se cumple: El cambio de los valores de fuerza están relacionados únicamente al Administrador. • Se cumple: El cambio de configuración está permitido únicamente para el administrador.

Continuación del anexo 3.

	<ul style="list-style-type: none"> • Se cumple: El cambio de <i>firmware</i> está autorizado únicamente para el rol de administrador. • La gestión de contraseñas es para el rol de administrador, la aplicación utilizará usuarios personales para identificar y autenticar a cada usuario individual. • Pistas de auditoría: Como excepción.
<p>Visualización de contraseña Solo se mostrarán las ID de usuario en las pantallas, las listas de auditoría, el área de memoria o los archivos y otros registros y archivos de configuración.</p>	Se cumple: Autorización de acciones a nivel de usuario y sistema
<p>Tiempo de espera de Acceso El IED tendrá una función de tiempo de espera que desconecta automáticamente a un usuario.</p>	<p>Con excepción:</p> <p>Autenticación e inicio de sesión de usuario Cuando corresponda, se debe realizar lo siguiente, con especial énfasis en los requisitos para operaciones seguras y disponibilidad:</p> <ul style="list-style-type: none"> • El sistema debe implementar mecanismos que permitan el traspaso seguro y transparente de las sesiones de los usuarios durante las operaciones.
Pista de auditoría (Audit Trail)	Se desglosan en los renglones posteriores
<p>Antecedentes Audit Trail El IED registrará en una memoria intermedia circular secuencial, no habrá capacidad de borrar o modificar la Audit Trail, ya que debe mantener la integridad</p>	El dispositivo de protección Siprotec 4, brinda un búfer de mensajes operativos, en el que los eventos más relevantes para la aplicación se almacenan en orden cronológico con estampa de tiempo.
<p>Capacidad de almacenamiento La Audit Trail debe almacenar al menos 2048 eventos antes de que la memoria intermedia circular comience a sobrescribir el evento más antiguo con el evento más nuevo.</p>	Según el cumplimiento indicado en la tabla 1686:2013, Las entradas más antiguas se sobrescribirán en el desbordamiento del archivo de registro. El sistema enviará una alerta antes de que el almacenamiento de registros se quede sin espacio.
<p>Registro de almacenamiento (Storage record) Para cada evento de auditoría, se debe registrar la siguiente información:</p> <ul style="list-style-type: none"> • Número de registro de evento • Hora y fecha • Identificación de usuario • Tipo de evento 	<p>El status se presenta como excepción, incluyendo lo siguiente:</p> <p>El sistemaregistra las acciones del usuario, así como las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. Durante un período de tiempo mínimo configurable, estos registros registrarán la fecha y la hora, los usuarios y sistemas involucrados, así como el evento real y el resultado.</p>

Continuación del anexo 3.

<p>Tipos de eventos de seguimiento de auditoría</p> <ul style="list-style-type: none"> • Iniciar sesión • Cierre de sesión manual • Cierre de sesión programado • Valor forzado • Configuración de acceso • Cambio de configuración • Cambio de <i>firmware</i> • Creación o modificación de ID/contraseña • Eliminación de IED/contraseña • Acceso al registro de auditoría • Hora/cambio de fecha • Alarma 	<p>El estatus se presenta como excepción, incluyendo lo siguiente:</p> <ul style="list-style-type: none"> • Iniciar Sesión: Se da cumplimiento con el sistema al registrar las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. • Cierre de sesión manual: Actualmente no se admite el cierre de sesión manual del usuario. • Cierre de sesión programado: Actualmente no se admite el cierre de sesión manual del usuario. • Valor forzado: Acción de un usuario que ha iniciado sesión que anula datos reales con entrada manual y provoca una operación de control. • Configuración de acceso: Actualmente no registrado. • Cambio de configuración: Actualmente no registrado • Cambio de <i>firmware</i>: Actualmente no registrado. • Creación o modificación de ID/contraseña: Dependerá de roles de usuario, donde el administrador es quien tiene la posibilidad de cambiar contraseña, y al mismo tiempo se respalda por la Autenticación e inicio de sesión de usuario. • Eliminación de IED/contraseña: Opción incluida en los Roles de usuario. • Acceso al registro de auditoría: Actualmente no registrado. • Hora/cambio de fecha: Actualmente no registrado. • Alarma: Función que se cumple con el inicio de sesión, será posible incluir mensajes relacionados con la seguridad en una gestión de alarmas preexistente.
<p>Supervisión y control de supervisión</p>	<ul style="list-style-type: none"> • El resumen de supervisión y control de supervisión, se cumple con el inicio de sesión (loggin)

Continuación del anexo 3.

<p>Resumen de supervisión y control de supervisión El IED supervisará la actividad relacionada con la seguridad y pondrá la información a disposición de una comunicación en tiempo real para su transmisión a un sistema de supervisión, un SCADA</p>	
<p>Eventos Actividades que se pueden esperar que ocurran en la rutina de uso y mantenimiento del IED.</p>	<p>Con excepción: Aplican las características de inicio de sesión, la cuales son</p> <ul style="list-style-type: none"> • Todo el sistema debe tener una hora uniforme del sistema, así como una opción para sincronizar esta hora del sistema con una fuente de tiempo externa segura. • El sistema debe registrar las acciones del usuario, así como las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. Durante un período de tiempo mínimo configurable, estos registros registrarán la fecha y la hora, los usuarios y sistemas involucrados, así como el evento real y el resultado. • Los archivos de registro se almacenarán de forma centralizada en una ubicación libremente configurable. Deberá estar disponible un mecanismo para la transferencia automática del archivo de registro a los componentes centrales. • El archivo de registro estará protegido contra modificaciones posteriores. • Las entradas más antiguas se sobrescribirán en el desbordamiento del archivo de registro. El sistema enviará una alerta antes de que el almacenamiento de registros se quede sin espacio. • Será posible incluir mensajes de registro relacionados con la seguridad en una gestión de alarmas preexistente.

Continuación del anexo 3.

<p>Alarmas Las alarmas son actividades que pueden identificar una actividad no autorizada,</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido • Reiniciar • Intento de uso de software de configuración no autorizado • Configuración inválida o descarga de <i>firmware</i> • Configuración no autorizada o archivo de <i>firmware</i> • Señal de tiempo fuera de tolerancia: el IED tendrá que validar el tiempo de sincronización de los mensajes recibidos a través de protocolo o dedicar canales de tiempo de sincronización. • Cambios de hardware de campo no válidos 	<p>Siprotec 4 puede cumplir únicamente con lo siguiente:</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido, con excepción: Se registrará cada intento de inicio de sesión fallido. • Reiniciar: Cumple • Intento de uso de software de configuración no autorizado: Actualmente verificado, pero no registrado. • Configuración inválida o descarga de <i>firmware</i>: Actualmente verificado, pero no registrado. • Señal de tiempo fuera de tolerancia: Actualmente verificado, pero no registrado • Cambios de hardware de campo no válidos: Actualmente verificado, pero no registrado
<p>Detección de cambio de punto de alarma Los puntos de alarma tendrán la capacidad de detectar momentáneamente la ocurrencia de una alarma será reportada en el siguiente escáner del IED por el sistema supervisor.</p>	<p>Con excepción: Será posible incluir mensajes de registro relacionados con la seguridad en una gestión de alarmas preexistente.</p>
<p>Grupos de Eventos y alarmas Se proporcionará un medio que permita al usuario agrupar eventos y alarmas.</p>	<p>Este grupo no está disponible</p>
<p>Control permisivo de supervisión El IED proporcionará un mecanismo que, cuando este habilitado, requiere permiso antes de realizar acciones para la supervisión independiente o requiere en el campo y remotamente.</p>	<p>Actualmente no es compatible</p>

Continuación del anexo 3.

<p>Funciones de ciberseguridad del IED</p>	<p>Características Criptográficas específicas:</p> <ul style="list-style-type: none"> • Funcionalidad del servidor Web: Siprotec 4 Cumple y soporta HTTPS • Funcionalidad de transferencia de archivos: Excepción: la función de transferencia de archivos no es compatible • Conexiones de terminales orientadas a texto: No es compatible • Gestión de red SNMP: Siprotec 4 únicamente soporta V1 y V2; V3 no es compatible.
<p>Compromiso de funcionalidad del IED</p>	<p>Compromiso de funcionalidad del IED: Con excepción para aplicación de parches y gestión de parches.</p>
<p>Principales características criptográficas:</p> <ul style="list-style-type: none"> • La funcionalidad del servidor web proporcionada por el IED será protocolo HTTPS • Funcionalidad de transferencia de archivos proporcionada por el IED deberá ser SFTP • Facilidades de comunicación orientada al texto usando una conexión terminal virtual a través de una red basada en Ethernet será un Shell seguro (SSH) • Implementación de SNMPv3. • La sincronización del tiempo en la red será NTP, la funcionalidad de la sincronización en la red implementada será NTP v3/4 o SNTP3/4. • Funcionalidad de túnel seguro proporcionada por el IED será una red privada virtual VPN 	<p>Características Criptográficas específicas:</p> <ul style="list-style-type: none"> • Funcionalidad del servidor Web: Siprotec 4 Cumple y soporta HTTPS • Funcionalidad de transferencia de archivos: Excepción: la función de transferencia de archivos no es compatible • Conexiones de terminales orientadas a texto: No es compatible • Gestión de red SNMP: Siprotec 4 únicamente soporta V1 y V2; V3 no es compatible. • Sincronización de la hora de red: Siprotec 4 cumple Las operaciones de ingeniería y mantenimiento a través de protocolos UDP y HTTP solo son compatibles con EN100 • Se admite NTP sobre UDP para la sincronización horaria. Otros protocolos de comunicación como IEC 61850 se configuran de acuerdo con las normas correspondientes

Continuación del anexo 3.

<p>Técnicas criptográficas</p>	<p>Con excepción:</p> <p>Al seleccionar los mecanismos criptográficos, se tendrá en cuenta la legislación nacional. Solo se utilizarán mecanismos aprobados y tamaños mínimos de clave que se consideren seguros para el futuro previsible de acuerdo con los conocimientos tecnológicos más avanzados. El proveedor no utilizará algoritmos criptográficos personalizados.</p> <p>Teniendo en cuenta las limitaciones de los dispositivos en el rendimiento operativo en el entorno de la subestación, se admiten los siguientes conjuntos de cifrado DTLS (para ingeniería con DIGSI 4) y TLS (para acceso web EN100)</p>
<p>Encriptación de comunicación serial Los IEDs serán capacitados para emplear comunicación por cualquier aplicación de acceso remota (transferencia de datos, configuración, carga de <i>firmware</i>, entre otros), deberá proporcionar encriptación de acuerdo con IEEE 1711 para todos los puertos designados a permitir acceso remoto.</p>	<p>No se admite la comunicación en serie para acceso remoto.</p>
<p>Configuración del Software de IED</p>	<p>Ver desglosados abajo</p> <p>Actualmente es conocido y con excepciones.</p>
<p>Autenticación Se evitará que las copias no autorizadas del software de configuración accedan a las funciones del IED.</p>	<p>Actualmente, el dispositivo comprueba si la configuración</p> <p>El software es el software oficial de Siemens. No es posible que el dispositivo verifique actualmente si la instancia de software ha sido autorizada por el usuario.</p>
<p>Firma digital La configuración del software tendrá la capacidad para generar archivos de descarga de configuración y <i>firmware</i> indicando que el archivo ha sido producido por una configuración autorizada de software y por un usuario autorizado. El IED aceptará únicamente archivos debidamente firmados.</p>	<p>Con excepción:</p> <p>Todos los dispositivos se protegerán contra <i>malware</i> en la ubicación adecuada. Como alternativa a la protección contra <i>malware</i> proporcionada en todos los componentes del sistema, el proveedor puede presentar un concepto integral de protección contra <i>malware</i> que proporcione la misma protección.</p>

Continuación del anexo 3.

<p>Control ID/contraseña</p> <p>La configuración del software será controlada por ID / contraseña para que el software no pueda ser accedido sin la combinación adecuada del ID/contraseña.</p>	<p>Con Excepción:</p> <p>Ciertas acciones relacionadas con la seguridad o críticas para la seguridad requerirán la autorización previa del usuario solicitante respecto del componente del sistema solicitante.</p> <p>Ambas contraseñas se pueden administrar solo a través de la interfaz web protegida por HTTPS EN100. Ambas contraseñas admiten de 8 a 24 caracteres ASCII que deben incluir letras mayúsculas y minúsculas, números y caracteres especiales.</p>
<p>Cambiar datos de configuración</p> <p>Cambiar y guardar datos de configuración y revisión de archivos de <i>firmware</i> que se cargarán en el IED:</p> <ul style="list-style-type: none"> • Acceso completo • Seguimiento de cambios • Monitoreo de uso • Descargas del IED 	<p>Para el acceso completo: Este modo es compatible. Sin embargo, la asignación de usuarios</p> <p>Seguimiento de cambios: Los niveles actualmente no son compatibles. Actualmente no está soportado.</p> <p>Monitoreo de uso: Actualmente, no se realiza un seguimiento de la acción de cierre de sesión.</p> <p>Descargas del IED: Actualmente no registrado.</p>
<p>Acceso al Puerto de comunicaciones</p> <p>Todos los puertos de comunicaciones, ya sean físicos o lógicos, otros que el puerto de diagnóstico en los IED tendrá la capacidad para ser habilitados o deshabilitados por medio de la configuración del IED.</p>	<p>Se cumple con lo siguiente:</p> <p>En general, solo los estándares y protocolos de comunicación seguros que incluyen protección de integridad</p>
<p>Aseguramiento de calidad de Firmware</p> <p>El aseguramiento de calidad del Firmware deberá cumplir con IEEE C37.231, práctica recomendada para el control de <i>firmware</i> de equipos de protección basados en microprocesadores</p>	<p>Con excepción de lo siguiente:</p> <p>Estándares de desarrollo seguros, gestión de la calidad y procesos de aprobación</p> <p>Siemens desarrolla SIPROTEC 4 / DIGSI 4 y EN100 de acuerdo con el reconocido proceso de desarrollo y garantía de calidad de CMMI. Los procesos de control de calidad cubren las prácticas recomendadas por IEEE Std. C37.231.</p>

Fuente: SIEMENS. *SIPROTEC 4 / SIPROTEC Compact / DIGSI 4 / EN100. Declaration of security conformance. Manual V02.00.* pp. 13, 34-53, 62-64.

Anexo 4. **Tabla de cumplimiento según IEEE 1686 para Unidad Terminal Remota modelo SICAM PAS marca SIEMENS**

Requerimiento del Estándar	Cumplimiento del IED marca SIEMENS SICAM PAS / SICAM SCC
Características de ciberseguridad en el IED	Contiene tabla de cumplimiento de acuerdo con el estándar IEEE 1686:2013
Control de acceso electrónico <ul style="list-style-type: none"> • Control de acceso al IED • Mecanismos de anulación de contraseña 	Con excepciones
Control de acceso al IED El acceso local estará protegido por una identificación de usuario única (ID) y combinaciones de contraseña	SICAM PAS no proporciona una interfaz abierta para usar productos de terceros
Mecanismos de anulación de contraseña El IED no tendrá ningún medio por el cual el control ID o contraseña creado por el usuario pueda ser anulado o eludido.	NA
El mínimo número de usuarios individuales admitidos por el IED deberá ser de 10	SICAM PAS soporta más de 10 usuarios.
Construcción de contraseña: Al menos 8 caracteres con las siguientes características: <ul style="list-style-type: none"> • Al menos una letra mayúscula y una minúscula • Al menos un número • Al menos un carácter no alfanumérico El IED no admitirá otro tipo de contraseña	Con excepción: SICAM PAS no sigue ninguna regla para las contraseñas creadas por el usuario.
Control de Acceso al IED	N.A.
Niveles de autorización por contraseña	N.A.
Autorización mediante el control de acceso basado en roles (RBAC) El IED tendrá la capacidad de definir al menos cuatro roles definidos por el usuario, cada rol tendrá la capacidad de combinar las funciones enumeradas a continuación:	Con excepción: SICAM PAS no admite roles definidos por el usuario.

Continuación del anexo 4.

<p>Principales funciones de seguridad en IED:</p> <ul style="list-style-type: none"> • Ver datos operativos • Ver ajustes de configuración • Valores de fuerza • Cambio de configuración • Cambio de <i>firmware</i> • La gestión de ID/contraseña o RBAC • Contener Pista de auditoría (Audit Trail) 	<p>Cumple únicamente para lo siguiente:</p> <ul style="list-style-type: none"> • La gestión de ID/Contraseña o RBAC: A los usuarios se les pueden asignar 8 roles predefinidos en SICAM PAS: <ul style="list-style-type: none"> ○ Administrador ○ Ingeniero de sistemas ○ Ingeniero de datos ○ Cambiar de operador ○ Huésped ○ Administrador de seguridad ○ Gerente de RBAC ○ Auditor de seguridad <p>Al asignar estos roles, el uso del sistema por parte de los usuarios individuales puede restringirse dependiendo de sus responsabilidades.</p> <p>El sistema admitirá una política de contraseñas de última generación.</p> <ul style="list-style-type: none"> • Pista de auditoría (Adit Trail): SICAM PAS mantienen un registro de eventos separado para eventos relevantes para la seguridad. <p>SICAM SCC registra los eventos relevantes para la seguridad en su base de datos de registro de auditoría con la opción WinCC Audit habilitada.</p>
<p>Visualización de contraseña Solo se mostrarán las ID de usuario en las pantallas, las listas de auditoría, el área de memoria o los archivos y otros registros y archivos de configuración.</p>	<p>Cumple con lo siguiente:</p> <p>SICAM PAS mantiene un registro de eventos separado para eventos relevantes para la seguridad.</p> <p>SICAM SCC registra los eventos relevantes para la seguridad en su base de datos de registro de auditoría con la opción WinCC Audit habilitada.</p> <p>Las operaciones críticas están protegidas contra entradas involuntarias del usuario a través de cuadros de diálogo. Se requieren derechos de usuario de Windows.</p>

Continuación del anexo 4.

<p>Tiempo de espera de Acceso El IED tendrá una función de tiempo de espera que desconecta automáticamente a un usuario que ha iniciado sesión después de un periodo de inactividad del usuario.</p>	<p>Se cumple con lo siguiente:</p> <p>Los productos de software SICAM, así como los sistemas operativos Windows utilizados, admiten la gestión de usuarios como se describe anteriormente. El cliente es responsable de su implementación para la operación diaria.</p> <p>Los productos de software de SICAM han implementado un servicio de registro para el registro de intentos de inicio de sesión fallidos y exitosos en un registro. Durante la integración de la función de gestión de usuarios proporcionada por el sistema operativo, también es posible configurar funciones adicionales como autenticación de 2 factores o políticas de contraseña específicas de la organización.</p>
<p>Pista de auditoría (Audit Trail)</p>	<p>Se cumple con las excepciones mencionadas en los renglones correspondientes.</p>
<p>Antecedentes Audit Trail El IED registrará en una memoria intermedia circular secuencial, no habrá capacidad de borrar o modificar la Audit Trail, ya que debe mantener la integridad</p>	<p>Con excepción: Se utiliza un mecanismo de búfer circular de Windows; no es alarmante.</p>
<p>Capacidad de almacenamiento La Audit Trail debe almacenar al menos 2048 eventos antes de que la memoria intermedia circular comience a sobrescribir el evento más antiguo con el evento más nuevo.</p>	<p>Se cumple con lo siguiente: El sistema debe registrar las acciones del usuario, así como las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. Durante un período de tiempo mínimo configurable, estos registros registrarán la fecha y la hora, los usuarios y sistemas involucrados, así como el evento real y el resultado.</p>
<p>Registro de almacenamiento (Storage record) Para cada evento de auditoría, se debe registrar la siguiente información:</p> <ul style="list-style-type: none"> • Número de registro de evento • Hora y fecha • Identificación de usuario • Tipo de evento 	<p>Se Cumple con lo siguiente: El sistema de SICAM PAS registrará las acciones del usuario, así como las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. Durante un período de tiempo mínimo configurable, estos registros registrarán la fecha y la hora, los usuarios y sistemas involucrados, así como el evento real y el resultado.</p>

Continuación del anexo 4.

<p>Tipos de eventos de seguimiento de auditoría</p> <ul style="list-style-type: none"> • Iniciar sesión • Cierre de sesión manual • Cierre de sesión programado • Valor forzado • Configuración de acceso • Cambio de configuración • Cambio de <i>firmware</i> • Creación o modificación de ID/contraseña • Eliminación de IED/contraseña • Acceso al registro de auditoría • Hora/cambio de fecha • Alarma 	<p>Para el dispositivo SICAM PAS, se cumple:</p> <ul style="list-style-type: none"> • Inicio de sesión: Se da cumplimiento con el sistema al registrar las acciones, eventos y errores relacionados con la seguridad en un formato adecuado para un procesamiento posterior y centralizado. • Cierre de sesión manual: Cumple • Cierre de sesión programado: N.A. • Valor forzado: N.A. • Configuración de acceso: N.A. • Cambio de configuración: N.A. • Cambio de <i>firmware</i>: N.A. • Creación o modificación de ID/Contraseña: Dependerá de roles de usuario, donde el administrador es quien tiene la posibilidad de cambiar contraseña, y al mismo tiempo se respalda por la Autenticación e inicio de sesión de usuario. • Eliminación de IED/Contraseña: Opción incluida en los Roles de usuario, la cual únicamente el administrador tiene derechos para realizar cambios de este tipo, y para lo cual, sin una autenticación de usuario exitosa, el sistema solo permitirá un rango de acciones definidas. • Acceso al registro de auditoría: con excepción. Actualmente no registrado. • Hora/cambio de fecha: N.A. • Alarma: Función que se cumple con el inicio de sesión, será posible incluir mensajes relacionados con la seguridad en una gestión de alarmas preexistente.
<p>Supervisión y control de supervisión</p>	<ul style="list-style-type: none"> • Resumen de supervisión y control de supervisión: N.A. • Eventos: En su mayoría, únicamente no se registran los eventos que no aplican para eventos de auditoría. • Alarmas: se define en renglones correspondientes • Detección de cambio de punto de alarma: N.A. • Grupos de eventos y alarmas: N.A. • Control permisivo de supervisión: N.A.

Continuación del anexo 4.

Resumen de supervisión y control de supervisión	N.A.
Eventos Actividades que se pueden esperar que ocurran en la rutina de uso y mantenimiento del IED.	Se cumple en su mayoría, únicamente no se registran los eventos que no aplican para eventos de auditoría.
Alarmas Las alarmas son actividades que pueden identificar una actividad no autorizada, <ul style="list-style-type: none"> • Intento de inicio de sesión fallido • Reiniciar • Intento de uso de software de configuración no autorizado • Configuración inválida o descarga de firmawre • Configuración no autorizada o archivo de <i>firmware</i> • Señal de tiempo fuera de tolerancia: el IED tendrá que validar el tiempo de sincronización de los mensajes recibidos a través de protocolo o dedicar canales de tiempo de sincronización. • Cambios de hardware de campo no válidos 	SICAM PAS puede cumplir con lo siguiente: <ul style="list-style-type: none"> • Intento de inicio de sesión fallido: se cumple, se registrará cada intento de inicio de sesión fallido. • Reiniciar: Cumple con las opciones de inicio de sesión, será posible incluir mensajes de registro relacionados con la seguridad en una gestión de alarmas preexistente. • Intento de uso de software de configuración no autorizado: N.A. • Configuración inválida o descarga de <i>firmware</i>: N.A. • Señal de tiempo fuera de tolerancia: N.A. • Cambios de hardware de campo no válidos: N.A.
Detección de cambio de punto de alarma	N.A.
Grupos de Eventos y alarmas Se proporcionará un medio que permita al usuario agrupar eventos y alarmas.	N.A.
Control permisivo de supervisión	N.A.
Funciones de ciberseguridad del IED	Para algunos casos descritos en los renglones correspondientes.
Compromiso de funcionalidad del IED	N.A.
Principales características criptográficas: <ul style="list-style-type: none"> • La funcionalidad del servidor web proporcionada por el IED será protocolo HTTPS • Funcionalidad de transferencia de archivos proporcionada por el IED deberá ser SFTP 	<ul style="list-style-type: none"> • Funcionalidad del servidor Web: N.A. • La transferencia de archivos: N.A. • Facilidades de comunicación orientada al texto: N.A. • Implementación de SNMP: Se cumple con SNMPv3, el cual se utiliza como protocolo de red. Las interfaces de administración están protegidas mediante ACL. La red

Continuación del anexo 4.

<ul style="list-style-type: none"> • Facilidades de comunicación orientada al texto usando una conexión terminal virtual a través de una red basada en Ethernet será un Shell seguro (SSH) • Implementación de SNMPv3. • La sincronización del tiempo en la red será NTP, la funcionalidad de la sincronización en la red implementada será NTP v3/4 o SNTP3/4. • Funcionalidad de túnel seguro proporcionada por el IED será una red privada virtual VPN. 	<ul style="list-style-type: none"> • los componentes de SICAM PAS y SICAM PQS están en modo hardened; los servicios y protocolos innecesarios están desactivados. • Sincronización del tiempo en la red: Se cumple con UDP se utiliza para la sincronización de la hora a través de NTP • El dispositivo no admite ninguna función de tunelización.
<p>Técnicas criptográficas</p>	<p>Con las siguientes excepciones:</p> <p>Al seleccionar los mecanismos criptográficos, se tendrá en cuenta la legislación nacional. Solo se utilizarán mecanismos aprobados y tamaños mínimos de clave que se consideren seguros para el futuro previsible de acuerdo con los conocimientos tecnológicos más avanzados. El proveedor no utilizará algoritmos criptográficos personalizados.</p>
<p>Encriptación de comunicación serial</p>	<p>N.A.</p>
<p>Configuración del Software de IED</p>	<p>Se describen en los renglones siguientes</p>
<p>Autenticación Se evitará que las copias no autorizadas del software de configuración accedan a las funciones del IED.</p>	<p>N.A.</p>
<p>Firma digital</p>	<p>N.A.</p>
<p>Control ID/contraseña</p>	<p>N.A.</p>
<p>Cambiar datos de configuración a)</p>	<p>N.A.</p>
<p>Acceso al Puerto de comunicaciones</p>	<p>N.A.</p>
<p>Aseguramiento de calidad de Firmware</p>	<p>N.A.</p>

Fuente: SIEMENS. SICAM PAS/PQS, SICAM SCC, SICAM PQ Analyzer: Declaration of security conformance. Manual V02.00. Edition 03.2020. pp.12-28, 50-51.

Anexo 5. **Tabla de cumplimiento según IEEE 1686 para unidad terminal remota modelo 3555 marca SEL**

Requerimiento del Estándar	Cumplimiento del IED marca SEL 3555
Características de ciberseguridad en el IED	No contiene tabla de cumplimiento de acuerdo con el estándar IEEE 1686:2013
Control de acceso electrónico <ul style="list-style-type: none"> Control de acceso al IED Mecanismos de anulación de contraseña 	El control de acceso obligatorio ajusta la política de seguridad del sistema para que los programas y servicios estén limitados a los privilegios de acceso mínimos absolutos necesarios para funcionar.
Control de acceso al IED El acceso local estará protegido por una identificación de usuario única (ID) y combinaciones de contraseña	Si, por contraseña
Mecanismos de anulación de contraseña El IED no tendrá ningún medio por el cual el control ID o contraseña creado por el usuario pueda ser anulado o eludido.	N.A.
El mínimo número de usuarios individuales admitidos por el IED deberá ser de 10	6 usuarios
Construcción de contraseña: Al menos 8 caracteres con las siguientes características: <ul style="list-style-type: none"> Al menos una letra mayúscula y una minúscula Al menos un número Al menos un carácter no alfanumérico El IED no admitirá otro tipo de contraseña	Con los siguientes criterios: Una contraseña segura debe cumplir con los siguientes criterios: <ul style="list-style-type: none"> mínimo ocho caracteres al menos un dígito al menos un carácter especial (!, \$, entre otros). al menos una letra en mayúscula al menos una letra minúscula
Control de Acceso al IED	N.A.
Niveles de autorización por contraseña	N.A.
Autorización mediante el control de acceso basado en roles (RBAC) El IED tendrá la capacidad de definir al menos cuatro roles definidos por el usuario, cada rol tendrá la capacidad de combinar las funciones enumeradas a continuación:	Se cumple para servicios de DNP3 Esta API es para ver y administrar roles de usuario de RTAC. Los roles de usuario personalizados pueden ser agregado y otorgado permisos que otorguen acceso a datos RTAC específicos y comportamiento. La lista completa de permisos se puede encontrar en la sección Funciones de usuario de la interfaz web RTAC agregando un nuevo rol de usuario. El usuario predeterminado de fábrica.

Continuación del anexo 5.

	<p>Los roles y sus respectivos permisos no se pueden eliminar ni editar, pero se pueden visto usando esta API</p>
<p>Principales funciones de seguridad en IED:</p> <ul style="list-style-type: none"> • Ver datos operativos • Ver ajustes de configuración • Valores de fuerza • Cambio de configuración • Cambio de <i>firmware</i> • La gestión de ID/contraseña o RBAC • Contener Pista de auditoría (Audit Trail) 	<p>Cumple únicamente para lo siguiente:</p> <ul style="list-style-type: none"> • Ver datos operativos: En HMI • Ajustes de configuración: Se cumple. • Valores de fuerza: Aplica para el rol de administrador e ingeniero. • La API de configuración ofrece la posibilidad de realizar un seguimiento de los cambios de configuración de RTAC exportando un valor de huella digital hexadecimal de 40 dígitos. Este valor se crea basado en la configuración del proyecto, aplicaciones de motor lógico, configuración avanzada, licencia características, ID de <i>firmware</i> (FID) y el número de serie. Cambios realizados en estos parámetros causarán cambios en el valor de la huella digital • Para la actualización de <i>firmware</i> • Para gestión de RBAC • El registro proporciona un método para auditar el acceso autorizado y no autorizado y cambios en el sistema. Puede registrar cambios en el RTAC colocando una variable en el procesador de etiquetas y habilitando el registro de esa variable. <p>LA interface web de la RTAC, tiene la posibilidad de crear los siguientes roles:</p> <ul style="list-style-type: none"> • Administrador • Gerente de cuenta de usuario • Ingeniero monitor • Operador HMI • Transferencia de archivos
<p>Visualización de contraseña Solo se mostrarán las ID de usuario en las pantallas, las listas de auditoría, el área de memoria o los archivos y otros registros y archivos de configuración.</p>	<p>Se cumple con lo siguiente: Se registran archivos de eventos y auditoría.</p>

Continuación del anexo 5.

<p>Tiempo de espera de Acceso El IED tendrá una función de tiempo de espera que desconecta automáticamente a un usuario que ha iniciado sesión después de un periodo de inactividad del usuario.</p>	<p>Los ajustes en el panel de RTAC le permiten configurar cuando la interfaz web debe cerrar la sesión de un usuario debido a la inactividad.</p>
<p>Pista de auditoría (Audit Trail)</p>	<p>Se cumple con las excepciones mencionadas en los renglones correspondientes.</p>
<p>Antecedentes Audit Trail El IED registrará en una memoria intermedia circular secuencial, no habrá capacidad de borrar o modificar la Audit Trail, ya que debe mantener la integridad</p>	<p>Con excepción: El RTAC conserva la llegada más reciente para cada uno de los 150 suscripciones. Si llega un GOOSE posterior para una suscripción que ya tiene un mensaje almacenado en búfer, el RTAC descarta la llegada anterior.</p>
<p>Capacidad de almacenamiento La Audit Trail debe almacenar al menos 2048 eventos antes de que la memoria intermedia circular comience a sobrescribir el evento más antiguo con el evento más nuevo.</p>	<p>No indicado.</p>
<p>Registro de almacenamiento (Storage record) Para cada evento de auditoría, se debe registrar la siguiente información:</p> <ul style="list-style-type: none"> • Número de registro de evento • Hora y fecha • Identificación de usuario • Tipo de evento 	<p>Esta API proporciona información sobre el proyecto en el RTAC, incluida la memoria. uso, uso de almacenamiento y usuarios conectados. La siguiente información se devuelve en esta API.</p> <ul style="list-style-type: none"> • Nombre del proyecto activo • Estadísticas de memoria actual • Estadísticas de almacenamiento actual • Estadísticas de usuarios registrados <p>Las utilidades de auditoría de red solo son compatibles con SEL-3555. Las auditorías están restringidas solo a las redes de área local y no pueden realizado en la red 127.0.0.0/8.</p>
<p>Tipos de eventos de seguimiento de auditoría</p> <ul style="list-style-type: none"> • Iniciar sesión • Cierre de sesión manual • Cierre de sesión programado • Valor forzado • Configuración de acceso • Cambio de configuración • Cambio de <i>firmware</i> 	<p>Para el dispositivo se cumple:</p> <ul style="list-style-type: none"> • Inicio de sesión: El registro proporciona un método para auditar el acceso autorizado y no autorizado y cambios en el sistema. • Cierre de sesión manual: La aplicación Cerrar sesión está disponible cuando un usuario ha iniciado sesión correctamente en dispositivo.

Continuación del anexo 5.

<ul style="list-style-type: none"> • Creación o modificación de ID/contraseña • Eliminación de IED/contraseña • Acceso al registro de auditoría • Hora/cambio de fecha • Alarma 	<ul style="list-style-type: none"> • Cierre de sesión programado: N.A. • Valor forzado: N.A. • Configuración de acceso: N.A. • Cambio de configuración: N.A. • Cambio de <i>firmware</i>: N.A. • Creación o modificación de ID/Contraseña: Dependerá de roles de usuario, donde el administrador es quien tiene la posibilidad de cambiar contraseña, y al mismo tiempo se respalda por la Autenticación e inicio de sesión de usuario. • Eliminación de IED/Contraseña: Opción incluida en los Roles de usuario, la cual únicamente el administrador tiene derechos para realizar cambios de este tipo. • Acceso al registro de auditoría: No cumple • Hora/cambio de fecha: N.A. • Alarma: No cumple
<p>Supervisión y control de supervisión</p>	<ul style="list-style-type: none"> • Resumen de supervisión y control de supervisión: N.A. • Eventos: En su mayoría, únicamente no se registran los eventos que no aplican para eventos de auditoría. • Alarmas: se define en renglones correspondientes • Detección de cambio de punto de alarma: N.A. • Grupos de eventos y alarmas: N.A. • Control permisivo de supervisión: N.A.
<p>Resumen de supervisión y control de supervisión</p>	<p>N.A.</p>
<p>Eventos</p> <p>Actividades que se pueden esperar que ocurran en la rutina de uso y mantenimiento del IED.</p>	<p>Se cumple en su mayoría, únicamente no se registran los eventos que no aplican para eventos de auditoría.</p>

Continuación del anexo 5.

<p>Alarmas</p> <p>Las alarmas son actividades que pueden identificar una actividad no autorizada,</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido • Reiniciar • Intento de uso de software de configuración no autorizado • Configuración inválida o descarga de <i>firmware</i> • Configuración no autorizada o archivo de <i>firmware</i> • Señal de tiempo fuera de tolerancia: el IED tendrá que validar el tiempo de sincronización de los mensajes recibidos a través de protocolo o dedicar canales de tiempo de sincronización. • Cambios de hardware de campo no válidos 	<p>Puede cumplir con lo siguiente:</p> <ul style="list-style-type: none"> • Intento de inicio de sesión fallido: se cumple, un mensaje de cadena que indica que hubo intentos de inicio de sesión fallidos. • El nombre de usuario no se proporciona hasta el tercer intento consecutivo. • Reiniciar: Cumple para algún cambio no autorizado. • Intento de uso de software de configuración no autorizado: N.A. • Configuración inválida o descarga de <i>firmware</i>: N.A. • Señal de tiempo fuera de tolerancia: N.A. • Cambios de hardware de campo no válidos: N.A.
<p>Detección de cambio de punto de alarma</p>	<p>N.A.</p>
<p>Grupos de Eventos y alarmas</p> <p>Se proporcionará un medio que permita al usuario agrupar eventos y alarmas.</p>	<p>N.A.</p>
<p>Control permisivo de supervisión</p>	<p>N.A.</p>
<p>Funciones de ciberseguridad del IED</p>	<p>Para algunos casos descritos en los renglones correspondientes.</p>
<p>Compromiso de funcionalidad del IED</p>	<p>N.A.</p>
<p>Principales características criptográficas:</p> <ul style="list-style-type: none"> • La funcionalidad del servidor web proporcionada por el IED será protocolo HTTPS • Funcionalidad de transferencia de archivos proporcionada por el IED deberá ser SFTP • Facilidades de comunicación orientada al texto usando una conexión terminal virtual a través de una red basada en Ethernet será un Shell seguro (SSH) • Implementación de SNMPv3. 	<ul style="list-style-type: none"> • Funcionalidad del servidor Web: Los mismos mecanismos que se utilizan para establecer una conexión HTTPS con el servidor web RTAC también se utilizan para cifrar una sesión de comunicaciones tunelizadas mediante TLS / SSL. • La transferencia de archivos: La autenticación de clave pública se puede utilizar con SFTP como alternativa a proporcionar una contraseña. Al colocar la clave SSH pública de RTAC en el servidor SFTP, el servidor SFTP puede autenticar el RTAC para la transferencia de archivos y cifrar el comunicación.

Continuación del anexo 5.

<ul style="list-style-type: none"> • La sincronización del tiempo en la red será NTP, la funcionalidad de la sincronización en la red implementada será NTP v3/4 o SNTP3/4. • Funcionalidad de túnel seguro proporcionada por el IED será una red privada virtual VPN. 	<ul style="list-style-type: none"> • Facilidades de comunicación orientada al texto: N.A. • Implementación de SNMP: No cumple para encriptación. • Sincronización del tiempo en la red: Se cumple con UDP se utiliza para la sincronización de la hora a través de NTP • Cifrado serial tunelizado: Cifrado de datos en conexiones seriales tunelizadas. Acceso de ingeniería seguro y otras comunicaciones seriales de túnel Ethernet • en la red de automatización con cifrado SSL / TLS o SSH.
Técnicas criptográficas	Con las siguientes excepciones: DNP Secure Authentication utiliza técnicas de hash criptográfico para una infraestructura de desafío y respuesta que sirve para autenticar comandos y servicios críticos. IEEE 1815 (estándar DNP) define comandos y servicios que son críticos y que deben desafiarse.
Encriptación de comunicación serial	N.A.
Configuración del Software de IED	Se describen en los renglones siguientes
<ul style="list-style-type: none"> • Autenticación • Firma digital • Control de ID/Contraseña • Característica de control de ID/contraseña: ver datos de configuración y cambiar los datos de configuración 	
Autenticación	N.A.
Firma digital	N.A.
Control ID/contraseña	N.A.
Cambiar datos de configuración b)	N.A.
Acceso al Puerto de comunicaciones	N.A.
Aseguramiento de calidad de Firmware	N.A.

Fuente: SEL-3555-2. *Real-Time Automation Controller (RTAC). Instruction manual. Schweitzer Engineering Laboratories, Inc. 1.3-1.15. pp. 499-527.*

