CARACTERIZACIÓN DE AMENAZAS CIBERNETICAS EN SISTEMAS DE TRANSMISION DE ENERGÍA ELÉCTRICA

Grupo Energía Bogotá

Mejoramos vidas con energía sostenible y competitiva

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

CONTENIDO

- INFRAESTRUCTURA CRÍTICA.
- CONCEPTOS GENERALES.
- METODOLOGÍA.
- ESTUDIO DE CASO.
- PREGUNTAS.

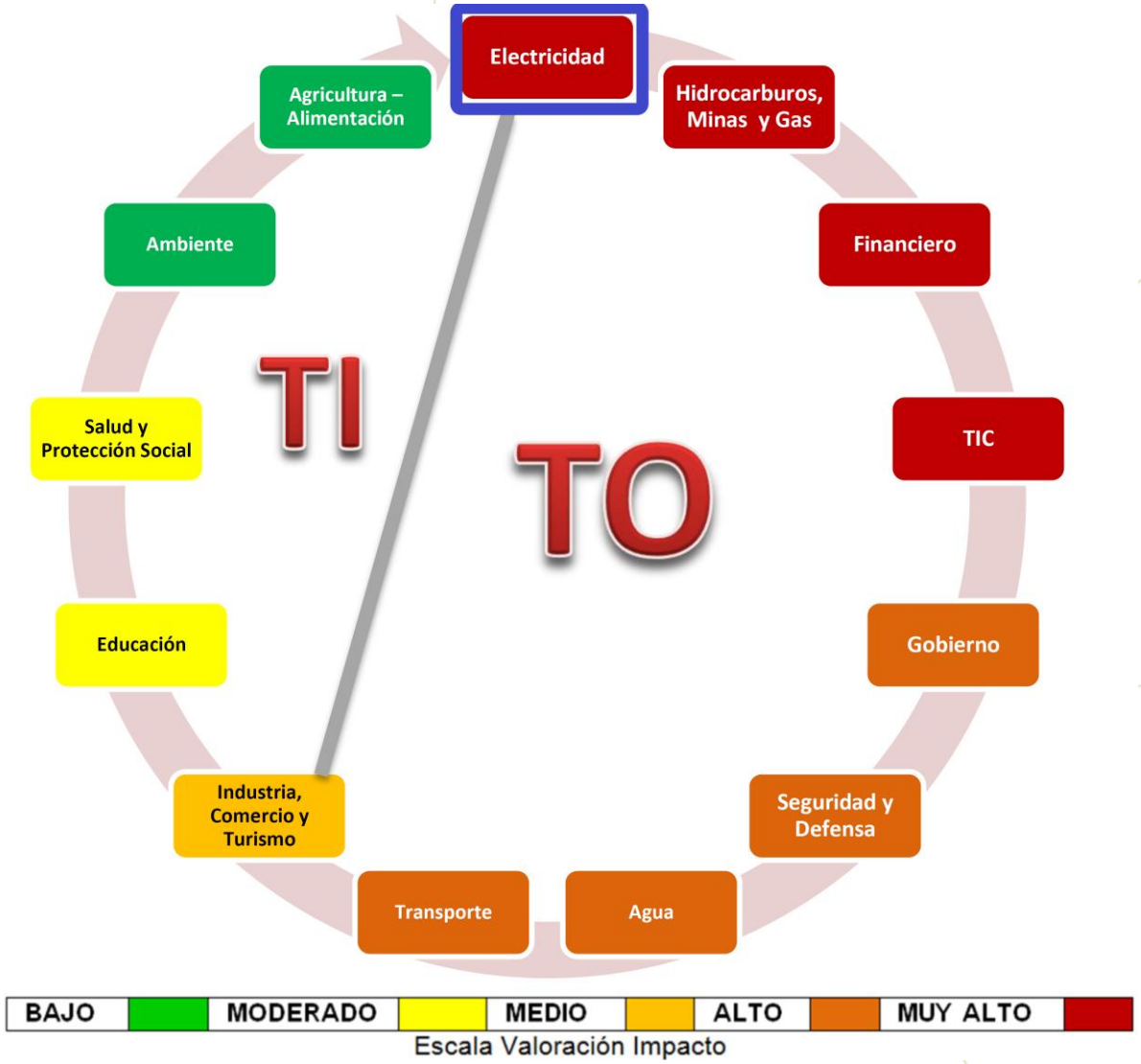
Grupo Energía Bogotá

Mejoramos vidas con energía sostenible y competitiva

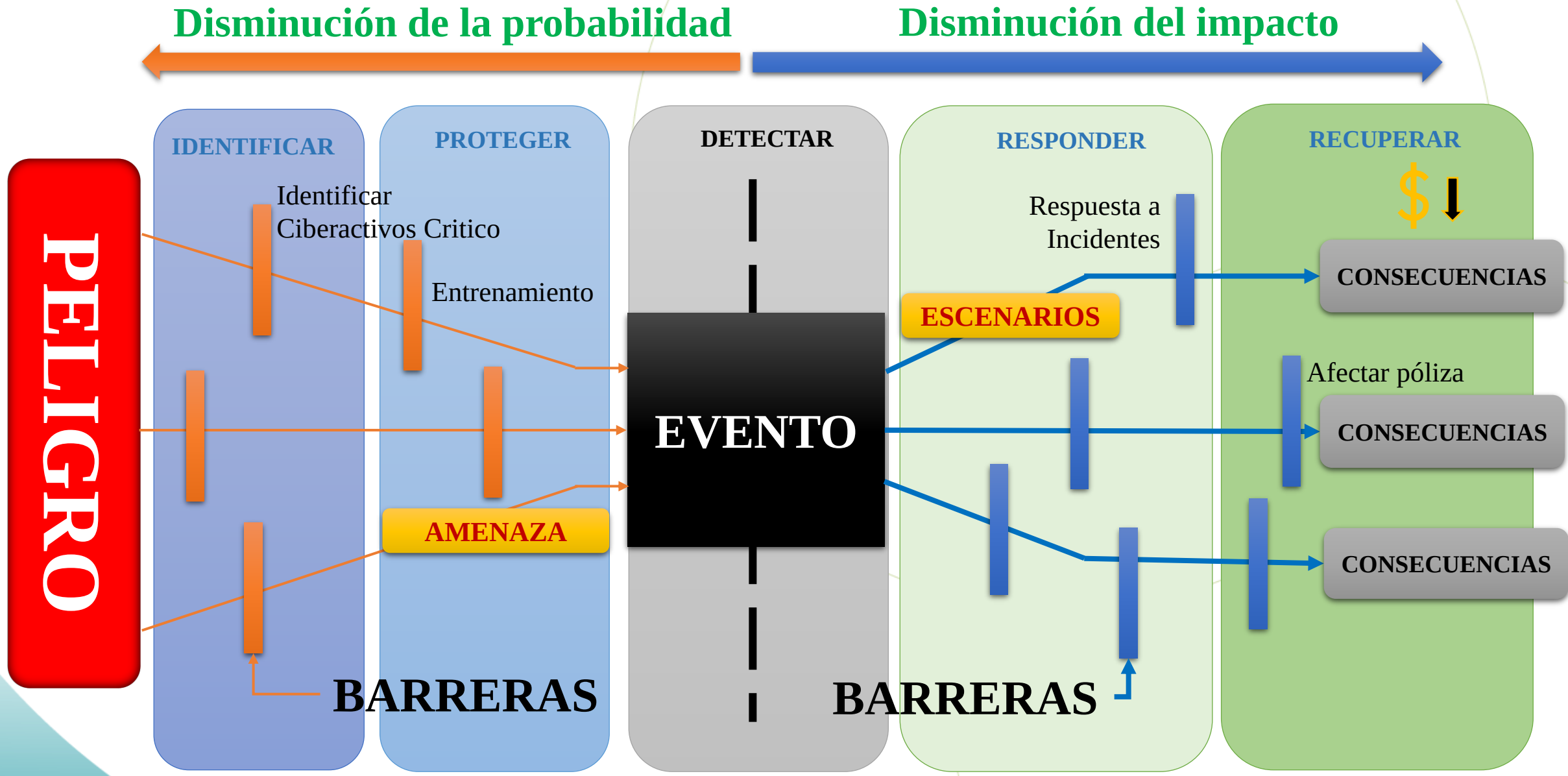
UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS
Acreditación Institucional de Alta Calidad

AMENAZAS CIBERNÉTICAS

INFRAESTRUCTURA CRÍTICA



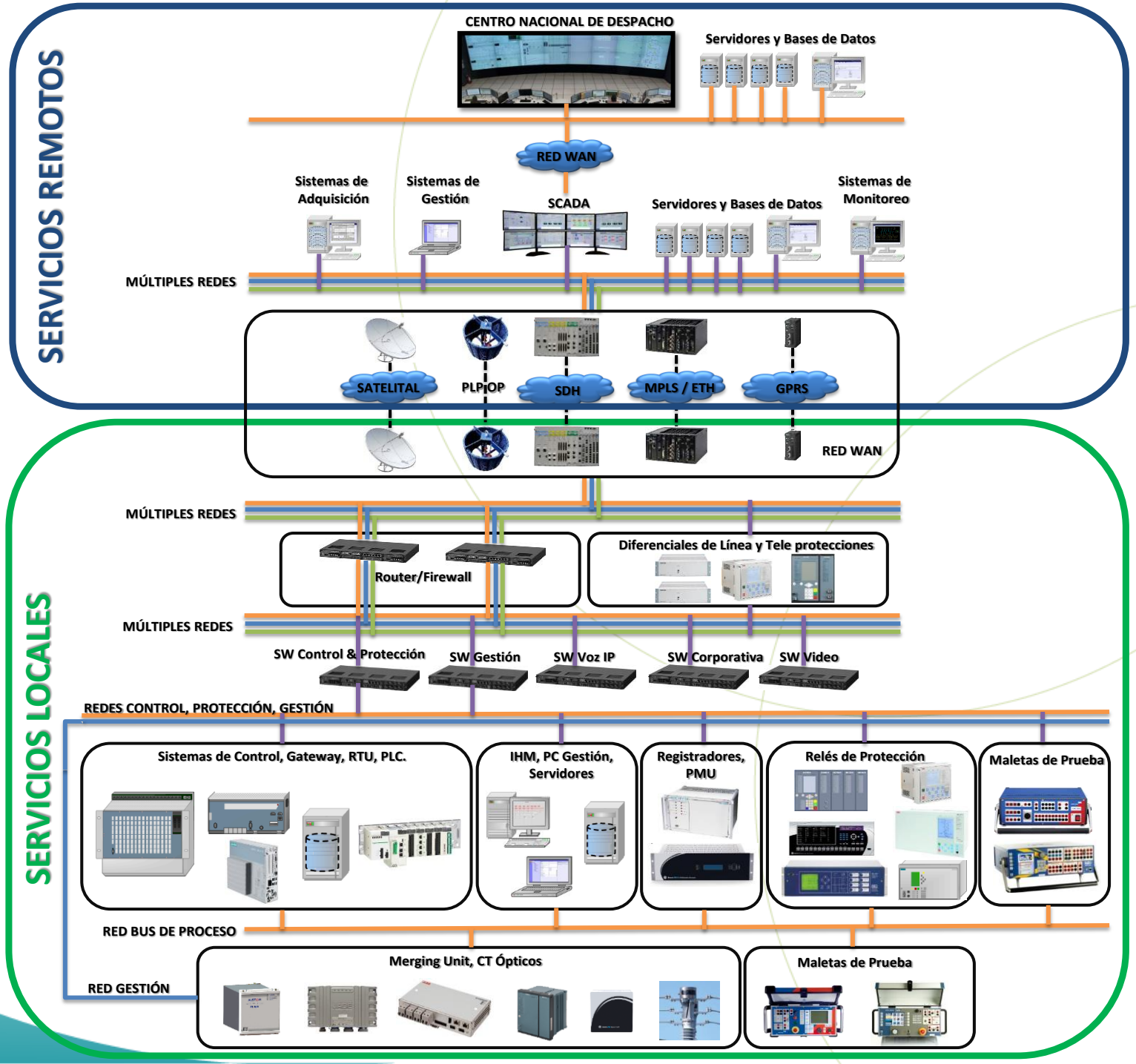
Grupo Energía Bogotá



Grupo Energía Bogotá

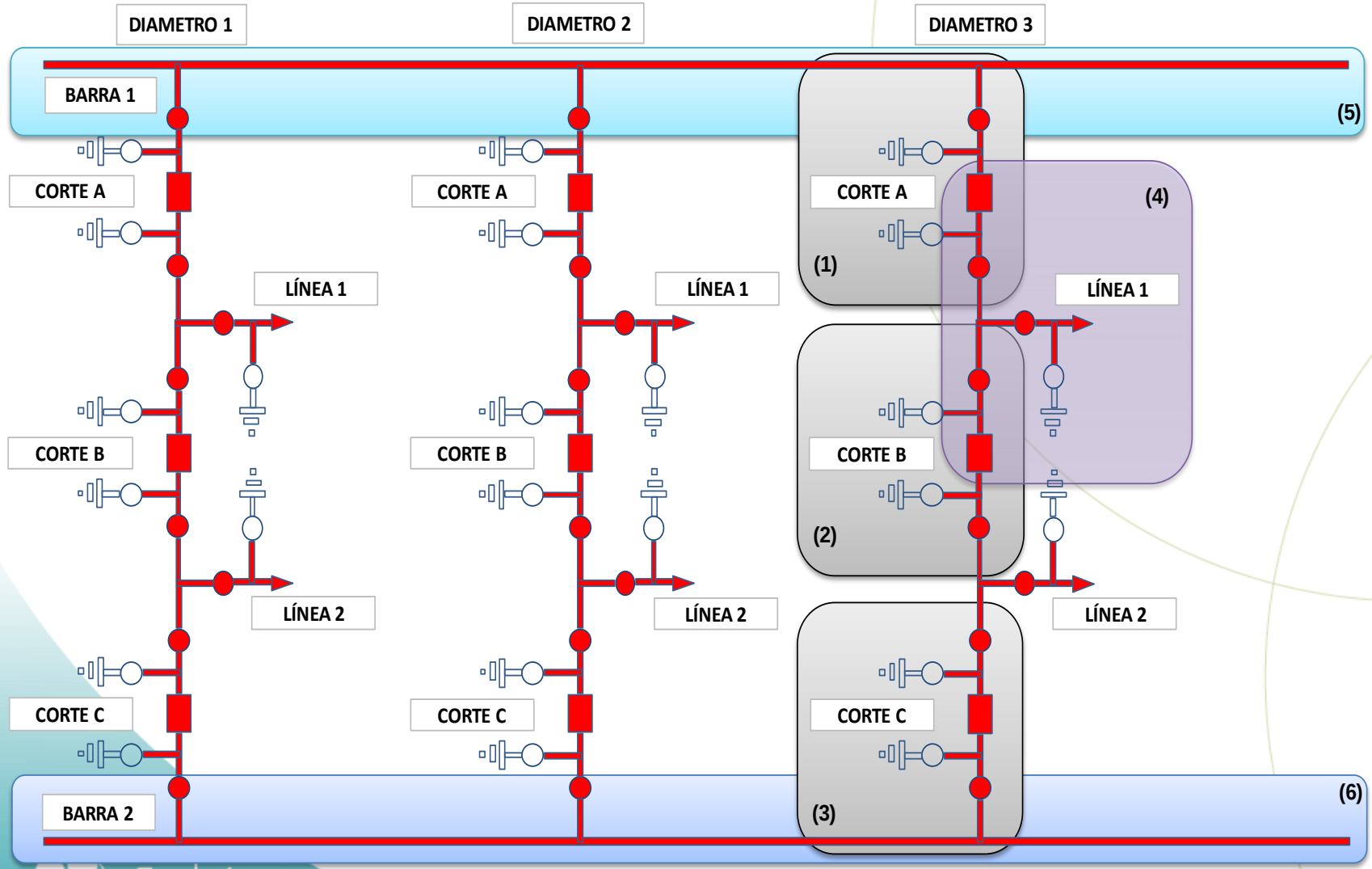
MODELO DE FUNCIONAMIENTO

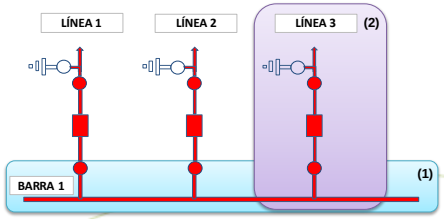
ESQUEMA DE ARQUITECTURA DE COMUNICACIONES EN SISTEMAS DE TRANSMISIÓN

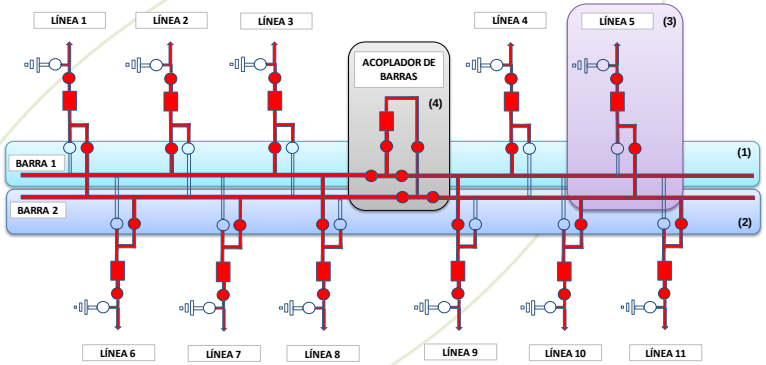


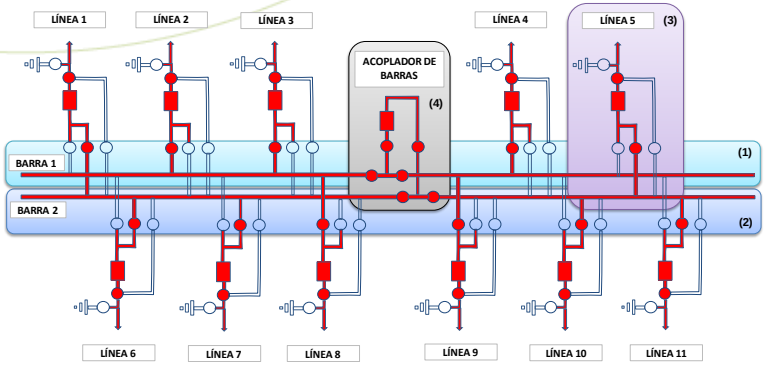
Grupo Energía Bogotá

ACTIVOS PRIMARIOS



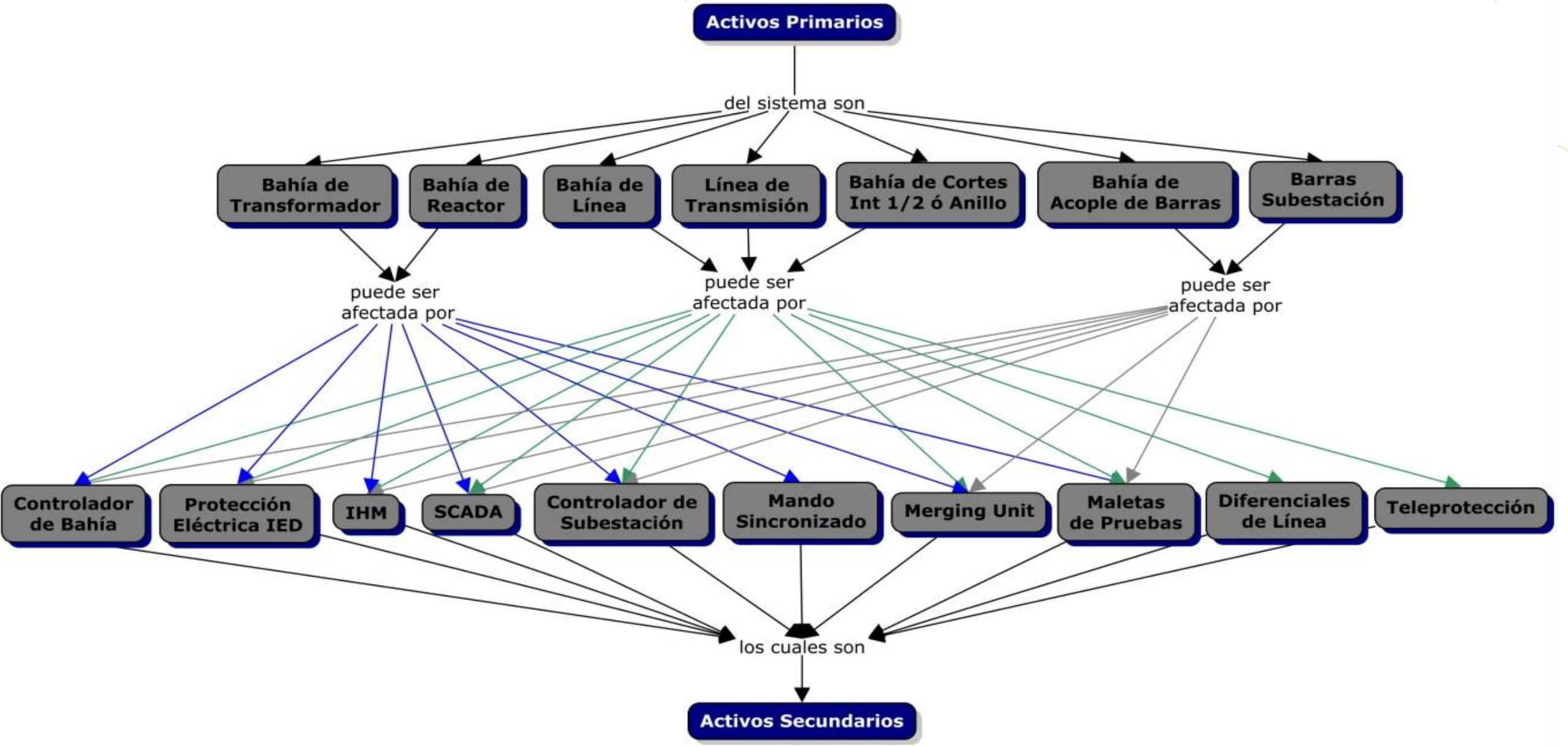




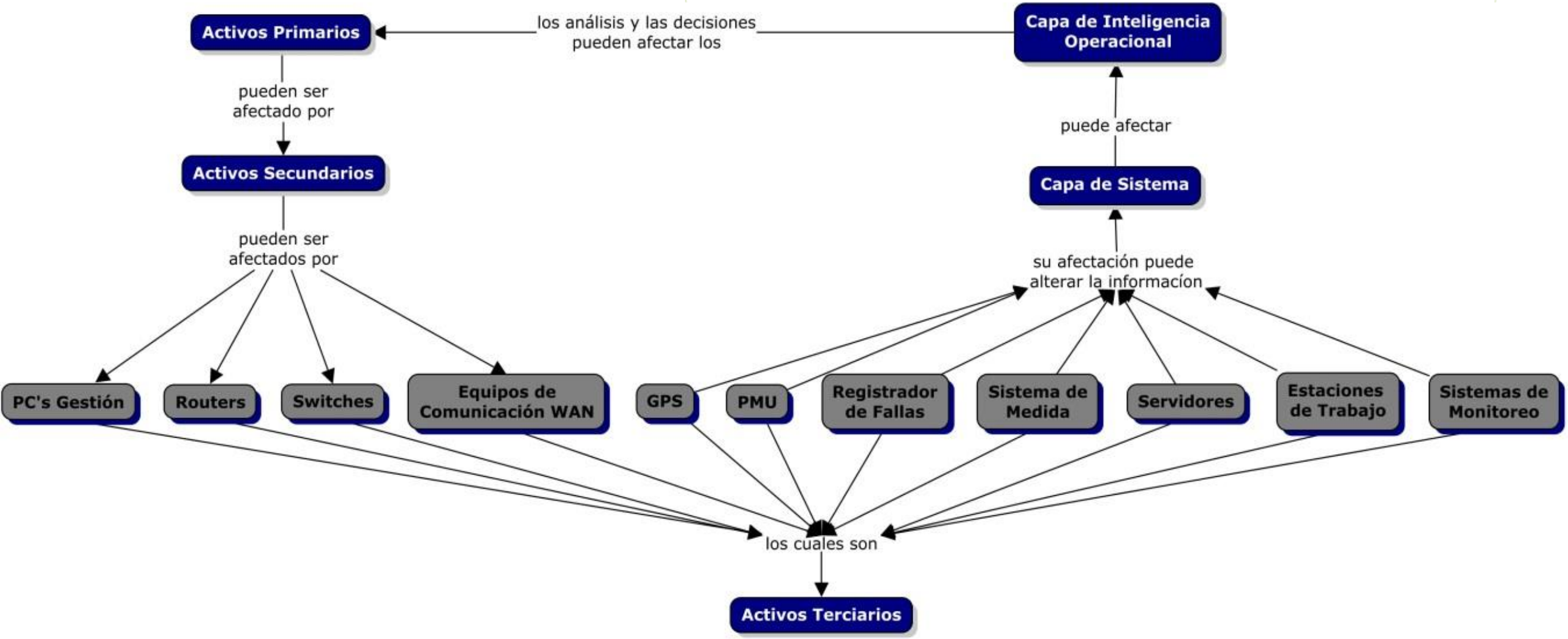


Energía Bogotá

ACTIVOS SECUNDARIOS

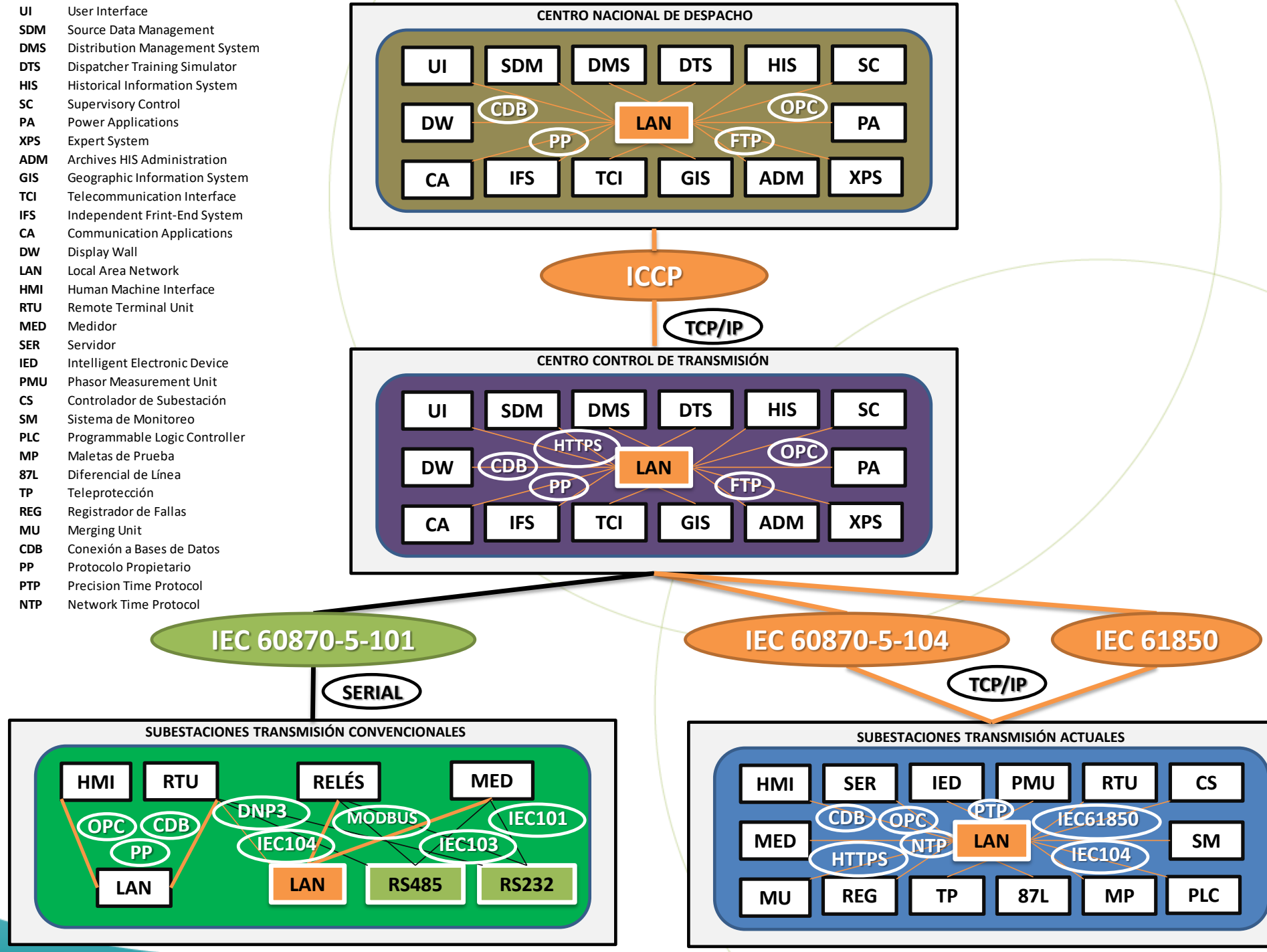


ACTIVOS TERCIARIOS

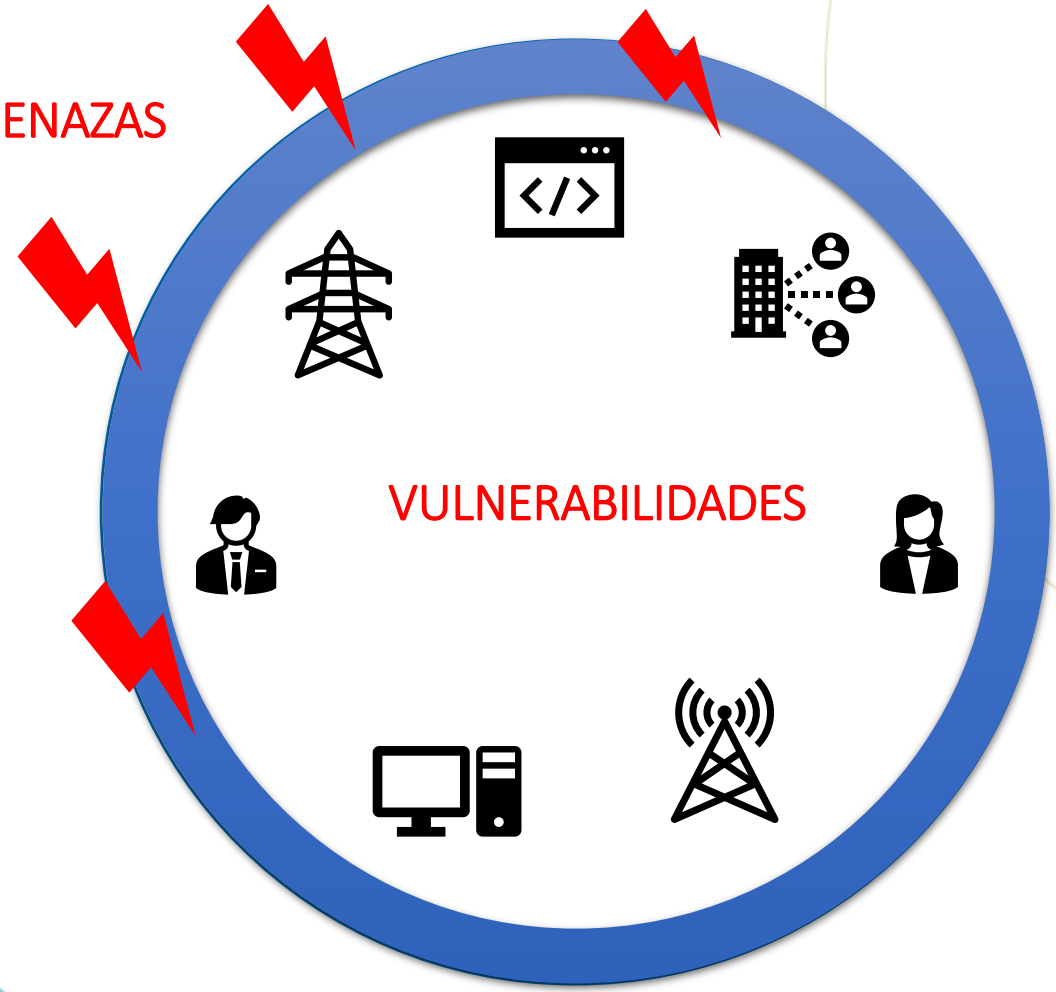


Servicio	Protocolo	Puerto
IEC 60870-5-104	TCP	2404 - 2405
OPC	TCP	135
OPC XML DA	TCP	8081
Modbus	TCP	502
DNP 3.0	TCP	20000
IEC 61850 Server	TCP	102
Propietario Registradores	TCP	4847
NTP	UDP	123
Remote Server	TCP	7912
Propietario IHM	TCP	10501 - 10502
Propietario Gestion Siemens	TCP	508-509
Propietario Gestion ABB	TCP	5555 - 5556
IPSec	UDP	500
PTP IEEE 1588	UDP	319 - 320
HTTPS	TCP	443
ICCP	TCP	102
SNMP	UDP	161
FTP	TCP	20 - 21
SSH	TCP	22

UI	User Interface
SDM	Source Data Management
DMS	Distribution Management System
DTS	Dispatcher Training Simulator
HIS	Historical Information System
SC	Supervisory Control
PA	Power Applications
XPS	Expert System
ADM	Archives HIS Administration
GIS	Geographic Information System
TCI	Telecommunication Interface
IFS	Independent Frint-End System
CA	Communication Applications
DW	Display Wall
LAN	Local Area Network
HMI	Human Machine Interface
RTU	Remote Terminal Unit
MED	Medidor
SER	Servidor
IED	Intelligent Electronic Device
PMU	Phasor Measurement Unit
CS	Controlador de Subestación
SM	Sistema de Monitoreo
PLC	Programmable Logic Controller
MP	Maletas de Prueba
87L	Diferencial de Línea
TP	Teleprotección
REG	Registrador de Fallas
MU	Merging Unit
CDB	Conexión a Bases de Datos
PP	Protocolo Propietario
PTP	Precision Time Protocol
NTP	Network Time Protocol



Grupo Energía Bogotá



SISTEMA DE TRANSMISION DE ENERGÍA

ANÁLISIS DE PROBABILIDAD

+

VALORACIÓN DE IMPACTO

↓

NIVEL DE RIESGO

↓

IMPLEMENTACIÓN DE CONTROLES

Grupo Energía Bogotá

LISTA DE VULNERABILIDADES METODOLOGÍA Y SU RESPECTIVA CLASIFICACIÓN

Amenaza	Propiedad Afectada	Vulnerabilidad	Categoria de riesgo	Tipo de Riesgo	Impacto	Probabilidad
Sitio web malicioso	Confidencialidad	Protección de límites	Riesgos de control	Riesgos conocidos	Moderado	Probable
Virus	Confidencialidad	Protección de límites	Riesgos de peligro	Riesgos conocidos	Menor	Probable
Trojan Horse	Integridad	Mínima funcionalidad	Riesgos de peligro	Riesgos conocidos	Menor	Probable
Gusano (worm)	Confidencialidad	Mínima funcionalidad	Riesgos de peligro	Riesgos conocidos	Moderado	Probable
Spyware	Confidencialidad	Monitoreo del sistema de información	Riesgos de peligro	Riesgos emergentes	Moderado	Probable
Keystroke Logger	Confidencialidad	Gestión de cuentas	Riesgos de control	Riesgos conocidos	Mayor	Probable
Malware	Integridad	Mínima funcionalidad	Riesgos de peligro	Riesgos emergentes	Mayor	Casi seguro
DOS/DDOS	Disponibilidad	Identificación y Autenticación	Riesgos de control	Riesgos conocidos	Severo	Casi seguro
Bot	Integridad	Acceso remoto	Riesgos de control	Riesgos conocidos	Severo	Casi seguro
Hack	No-repudio	Protección de límites	Riesgos de control	Riesgos latentes	Mayor	Probable
Phishing	Confidencialidad	Identificación y Autenticación	Riesgos de control	Riesgos focalizados	Mayor	Probable
Spoofing	No-repudio	Entrenamiento en conciencia de seguridad	Riesgos de control	Riesgos emergentes	Moderado	Probable
Spoofing DNS	Confidencialidad	Confidencialidad e integridad de la transmisión	Riesgos de control	Riesgos conocidos	Moderado	Probable
Exploit	Integridad	Remediación de defectos	Riesgos de control	Riesgos emergentes	Severo	Probable
Clickjacking	No-repudio	Entrenamiento en conciencia de seguridad	Riesgos de control	Riesgos conocidos	Moderado	Casi seguro
Inyección SQL	Confidencialidad	Monitoreo del sistema de información	Riesgos de peligro	Riesgos latentes	Mayor	Probable
Ingeniería social	No-repudio	Entrenamiento en conciencia de seguridad	Riesgos de oportunidad	Riesgos focalizados	Menor	Casi seguro
Ransomware	Integridad	Protección de la información en reposo	Riesgos de peligro	Riesgos latentes	Mayor	Improbable
Ciberterorismo	Integridad	Control de acceso físico	Riesgos de control	Riesgos latentes	Severo	Posible
Ciberespionaje	Confidencialidad	Confidencialidad e integridad de la transmisión	Riesgos de control	Riesgos latentes	Mayor	Improbable
Vulnerabilidades en TO	Disponibilidad	Mínima funcionalidad	Riesgos de oportunidad	Riesgos focalizados	Severo	Probable
Rootkits en PLC	Integridad	Mínima funcionalidad	Riesgos de control	Riesgos focalizados	Severo	Posible
USB Driveby	Integridad	Uso de dispositivos media	Riesgos de peligro	Riesgos conocidos	Moderado	Posible
Man in the middle	Integridad	Protección de límites	Riesgos de peligro	Riesgos emergentes	Mayor	Posible
Suplantación de señales de control	Integridad	Mínima funcionalidad	Riesgos de peligro	Riesgos focalizados	Severo	Posible
Configuraciones inadecuadas	Disponibilidad	Asignación de recursos	Riesgos de control	Riesgos conocidos	Mayor	Probable
Controles de acceso débiles	Confidencialidad	Bajos privilegios	Riesgos de control	Riesgos conocidos	Mayor	Probable
Obsolecencia tecnológica	Disponibilidad	Análisis de impacto de seguridad	Riesgos de peligro	Riesgos focalizados	Moderado	Posible
Convergencia TI TO	Disponibilidad	Asignación de recursos	Riesgos de peligro	Riesgos emergentes	Mayor	Probable
Sistemas no actualizados	Integridad	Configuración de ajustes	Riesgos de control	Riesgos focalizados	Moderado	Probable
Puertos lógicos no controlados	Confidencialidad	Configuración de ajustes	Riesgos de control	Riesgos conocidos	Moderado	Probable
Bajo conocimiento especializado	Integridad	Asignación de recursos	Riesgos de control	Riesgos conocidos	Menor	Probable
Falta de conciencia situacional	Disponibilidad	Entrenamiento en conciencia de seguridad	Riesgos de peligro	Riesgos conocidos	Moderado	Probable
Ataques a sistemas de protecciones	Integridad	Protección de límites	Riesgos de control	Riesgos focalizados	Severo	Posible
Ataques a dispositivos de safety	Integridad	Protección de límites	Riesgos de control	Riesgos focalizados	Mayor	Posible
Ataques a sistemas control y RTUs	Integridad	Protección de límites	Riesgos de control	Riesgos focalizados	Severo	Posible
Ataques a sistemas de comunicaciones	Integridad	Protección de límites	Riesgos de control	Riesgos latentes	Mayor	Probable

(ISID - Industrial Security Incident Database)
(ICS-CERT - Cyber Emergency Response Team)
(NCCIC - National Cybersecurity and Communications Integration Center)
(Hopkin, 2017), (Schlegel, Obermeier, & Schneider, 2016), (Santander, 2017), (Maglaras, y otros, 2018), (Cano, 2017)

INDICADOR DE VULNERABILIDAD OPERATIVA

$$IVO = 0{,}4 * DNAn + 0{,}4 * PC + 0{,}2 * PSn$$

Demanda No Atendida (DNA):

$$DNA \leq 1000MWh = 0{,}1 + \left(0{,}6 * \frac{DNA\ [MWh]}{1000\ [MWh]}\right)$$

$$DNA > 1000MWh = 0{,}7 + \left(0{,}3 * \frac{DNA\ [MWh]}{5000\ [MWh]}\right)$$

Pérdida de Conectividad (PC):

$$\mathrm{PL} = 1 - \mathrm{KL}'/\mathrm{KL}$$

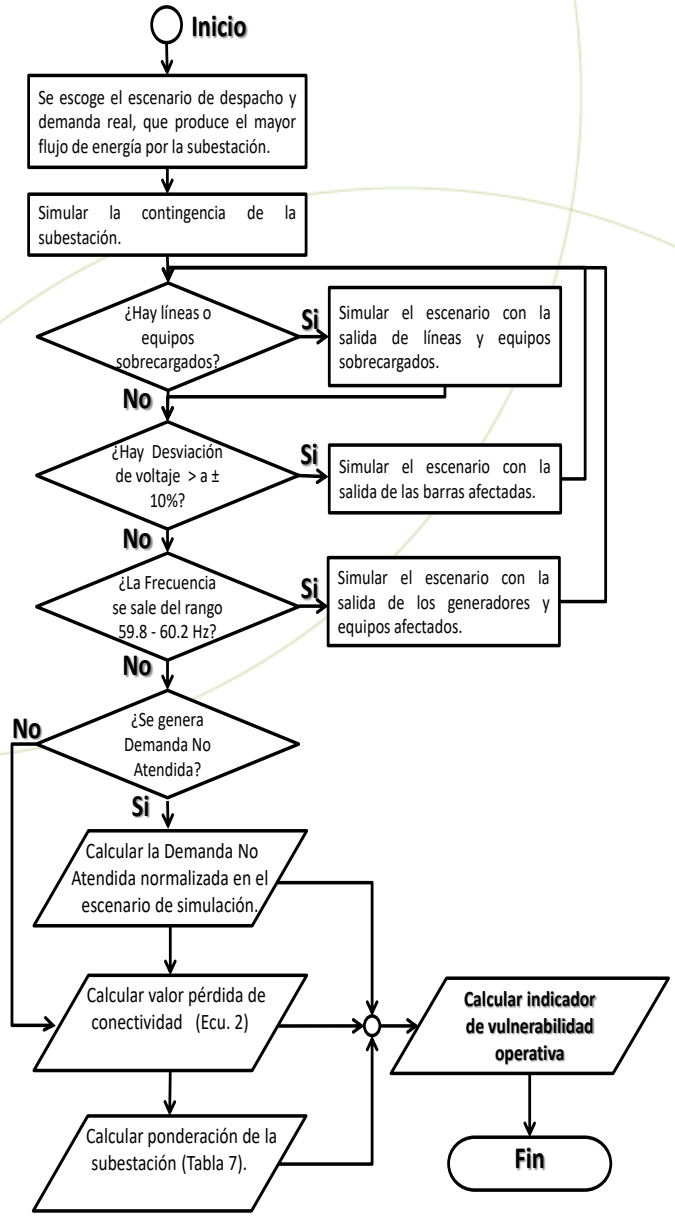
Donde KL es el número de líneas disponibles antes del ataque y KL' representa el número de líneas disponibles luego del ataque.

Ponderación de Subestación (PS):

$$PSn \rightarrow PS \leq 3000\ (De\ Tabla\ 7) = 0{,}1 + \left(0{,}6 * \frac{PS}{3000}\right)$$

$$PSn \rightarrow PS > 3000\ (De\ Tabla\ 7) = 0{,}7 + \left(0{,}3 * \frac{PS}{10000}\right)$$

Tensión de Línea	Valor de Peso por Línea
100kV a 199kV	300
200kV a 299kV	700
300kV a 499kV	1300
>= 500kV	1500



Rango Bajo: >=0,3; Rango Medio 0,3> & <=0,7 ; Rango Alto >0,7

INDICADOR DE VULNERABILIDAD DE SISTEMA

$$IAC = \frac{(\#+)*2+(\#\pm)}{16}$$

CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN (IAC)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se tiene identificación y autenticación única para todos los usuarios.			
Se tiene múltiple factor de autenticación para todas las redes.			
Se realiza gestión de cuentas unificada.			
Se cuenta con Hardware de seguridad para identificar credenciales mediante procesos de software.			
Se cuenta con identificación y autenticación única para los accesos inalámbricos.			
Se tiene metodología definida para la generación de contraseñas.			
Se realiza restricciones en tiempo de vida para las contraseñas de usuarios.			
Se realiza bloqueos por Intentos de login fallidos.			

MÉTODO PARA EVALUAR LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN

$$UC = \frac{(\#+)*2+(\#\pm)}{14}$$

CONTROL DE USO (UC)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se tiene aplicación de autorización para todos los usuarios.			
Se realiza mapeo de permisos por roles.			
Se cuenta con sincronización interna de tiempo para todos los equipos.			
Se cuenta con sistemas de gestión centralizada.			
Se puede identificar y reportar dispositivos no autorizados.			
Se usa certificados de seguridad para los accesos remotos a dispositivos.			
Se puede identificar y reportar personal no autorizado en las instalaciones físicas.			

MÉTODO PARA EVALUAR LOS CONTROLES DE USO

DISPONIBILIDAD DE RECURSOS (RA)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se realiza gestión de la carga en las comunicaciones.			
Se tiene política de verificación de backup.			
Se tiene sistema de automatización de backup.			
Se cuenta con sistemas de respaldo de energía.			
Se cuenta con reportes de ajustes de seguridad actuales legibles.			
Se cuenta con inventario de componentes del sistemas de control.			
Se realizan pruebas de verificación de configuración del sistema periodicamente.			
Se cuenta con gestor de actualizaciones e inventario de versiones.			
Se cuenta con los especialistas para el manejo y operación de los sistemas de control y protección.			

MÉTODO PARA EVALUAR LA DISPONIBILIDAD DE RECURSO

$$RA = \frac{(\#+)*2+(\#\pm)}{18}$$

$$TRE = \frac{(\#+)*2+(\#\pm)}{6}$$

TIEMPO DE RESPUESTA A EVENTOS (TRE)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se puede tener accesibilidad a logs de todos los equipos y software.			
Se tiene sistema de monitoreo continuo.			
Se tiene plan de entrenamiento continuo para el personal, en conciencia de seguridad .			

MÉTODO PARA EVALUAR TIEMPOS DE RESPUESTA A EVENTOS

$$DC = \frac{(\#+)*2+(\#\pm)}{8}$$

CONFIDENCIALIDAD DE LOS DATOS (DC)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se tiene protección de la confidencialidad de la información alojada o en tránsito por redes.			
Se tiene protección de la confidencialidad a través de los límites de las zonas.			
Se usa criptografía para proteger la integridad de los datos.			
Se realiza purga de recursos de memoria compartida.			

MÉTODO PARA EVALUAR LA CONFIDENCIALIDAD DE LOS DATOS

$$RDF = \frac{(\#+)*2+(\#\pm)}{12}$$

FLUJO DE DATOS RESTRINGIDO (RDF)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se tiene segmentación física de redes.			
Se tiene aislamiento lógico y físico de redes criticas.			
Se realiza denegar por defecto, permitir por excepción.			
Se cuenta con sistema de gestión centralizada para el monitoreo de flujos de datos.			
Se encuentran habilitados los puertos lógicos utilizados por el sistema y restringidos los demas.			
Se cuenta definidos los anchos de banda de acuerdo a los servicios que se utilizan.			

MÉTODO PARA EVALUAR EL FLUJO DE DATOS RESTRINGIDO

$$SI = \frac{(\#+)*2+(\#\pm)}{10}$$

INTEGRIDAD DEL SISTEMA (SI)			
Descripción	Impacto		
	+: Implementado	±: Parcial	-:No existe
Se usa criptografía para proteger la integridad de los datos.			
Se usa protección contra código malicioso en los puntos de entrada y salida.			
Se cuenta con sistema de gestión centralizada para protección contra código malicioso.			
Se cuenta con mecanismos para verificar funcionalidades de seguridad.			
Se tiene sistema de notificaciones automáticas sobre violaciones de integridad.			

MÉTODO PARA EVALUAR LA INTEGRIDAD DEL SISTEMA

$$IVS = 1 - \left(\frac{1}{7}*IAC + \frac{1}{7}*TRE + \frac{1}{7}*UC + \frac{1}{7}*SI + \frac{1}{7}*DC + \frac{1}{7}*RDF + \frac{1}{7}*RA\right)$$

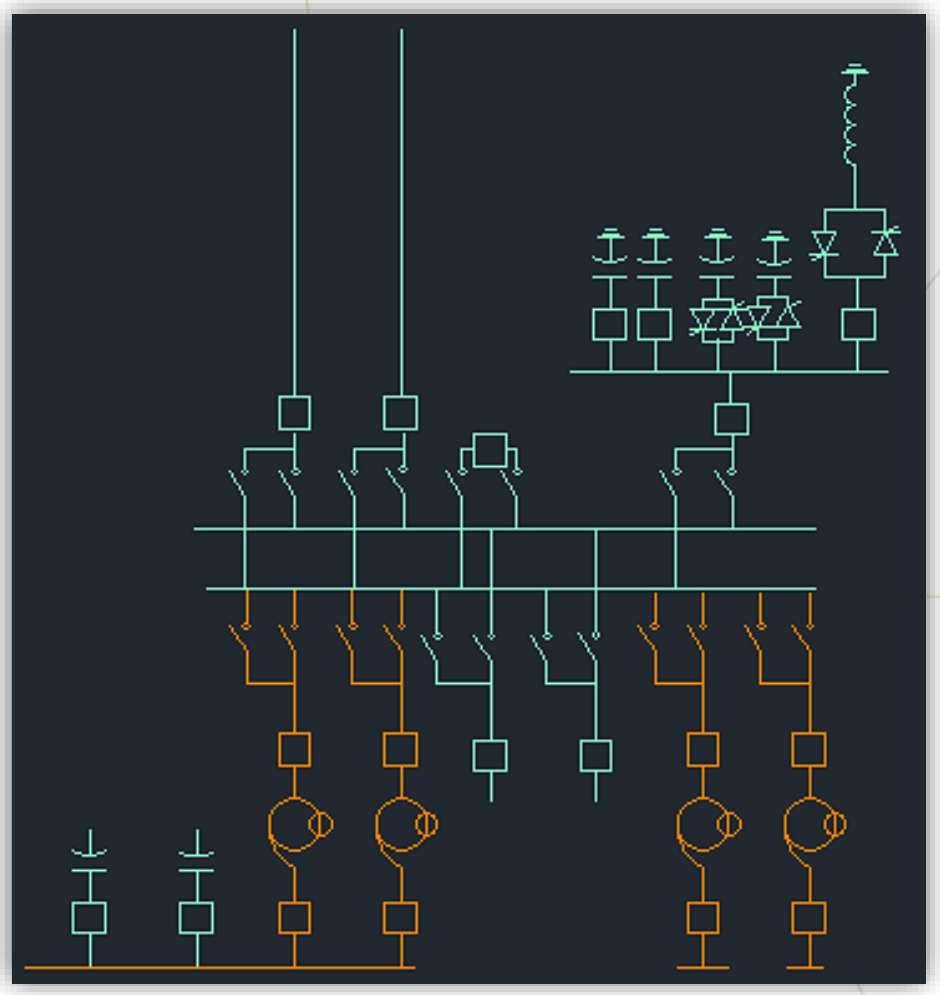
Rango Bajo: >=0,3; Rango Medio 0,3> & <=0,7 ; Rango Alto >0,7

Grupo Energía Bogotá


¿ PERO SI ES POSIBLE AFECTAR UN ACTIVO?

ESTUDIO DE CASO

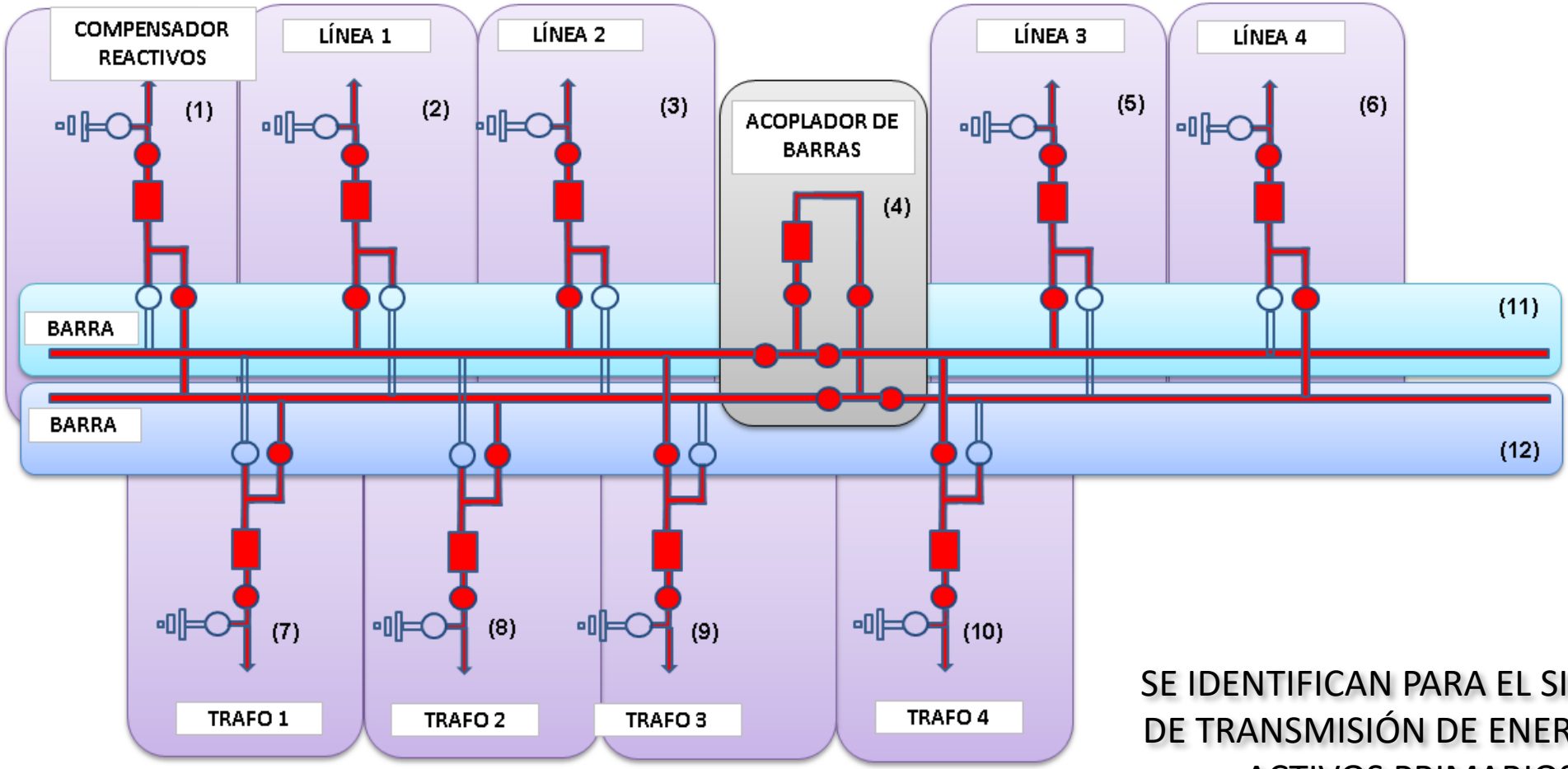
LA SUBESTACIÓN ESTA INTERCONECTADO A 230 kV



Grupo Energía Bogotá

ESTUDIO DE CASO

Identificación de activos primarios

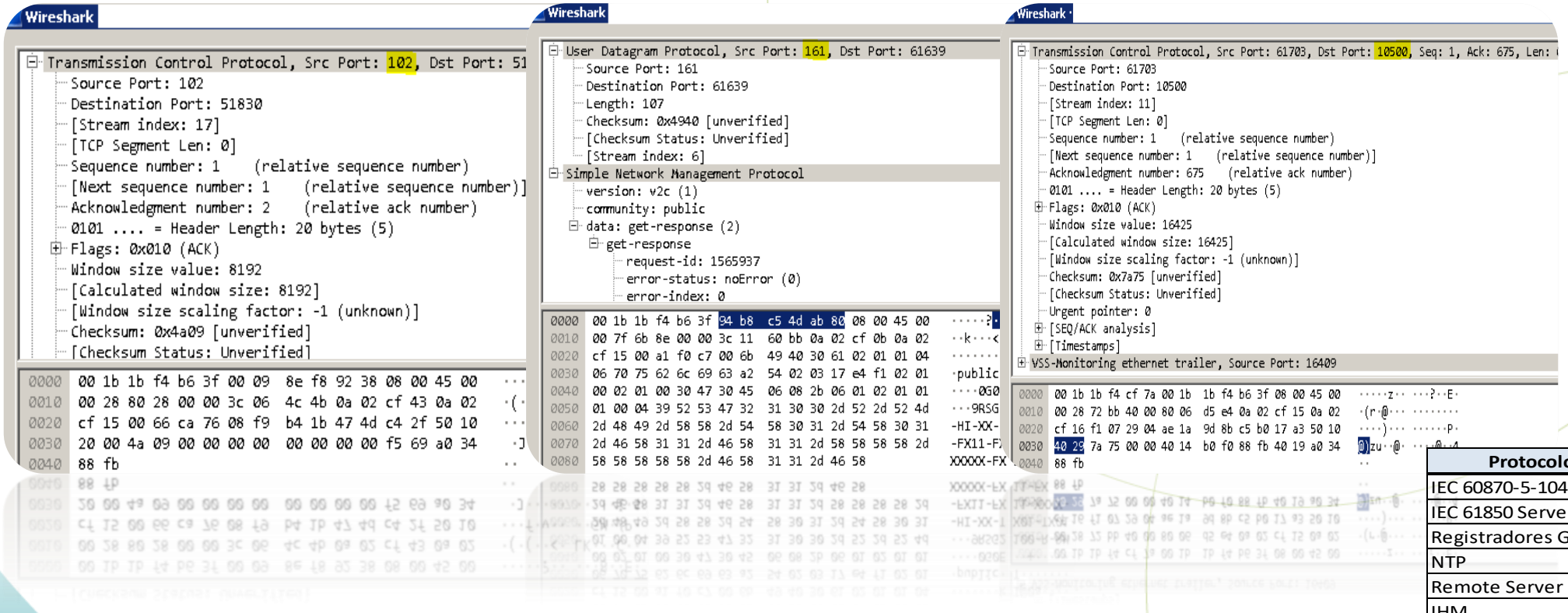


SE IDENTIFICAN PARA EL SISTEMA DE TRANSMISIÓN DE ENERGÍA 12 ACTIVOS PRIMARIOS

Grupo Energía Bogotá

ESTUDIO DE CASO

Escaneo de protocolos



Protocolo de red	Tipo	Puerto
IEC 60870-5-104	TCP	2404 - 2405
IEC 61850 Server	TCP	102
Registradores GE	TCP	4847
NTP	UDP	123
Remote Server	TCP	7912
IHM	TCP	10501
Redundancia Gateway		10500
Propietario Gestion Siemens	TCP	508-509
Propietario Gestion ABB	TCP	5555 - 5556
HTTPS	TCP	443
HTTP	TCP	80
FTP	TCP	20 - 21
ICCP	TCP	102
SNMP	UDP	161
IRIG-B	SERIAL	P2P
IEC 60870-5-101	SERIAL	RS232

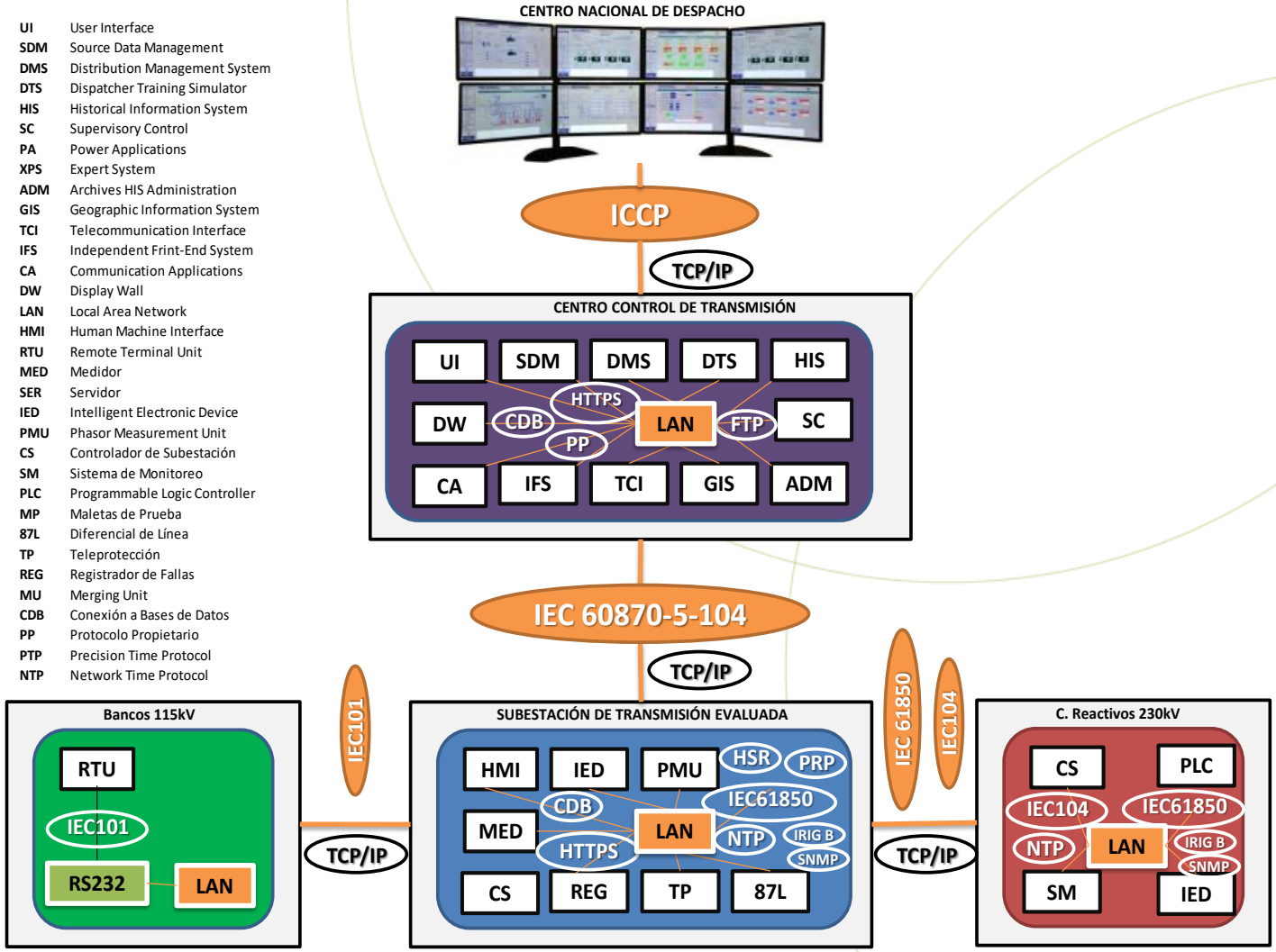
Grupo Energía Bogotá

ESTUDIO DE CASO

Identificación de protocolos y aplicaciones

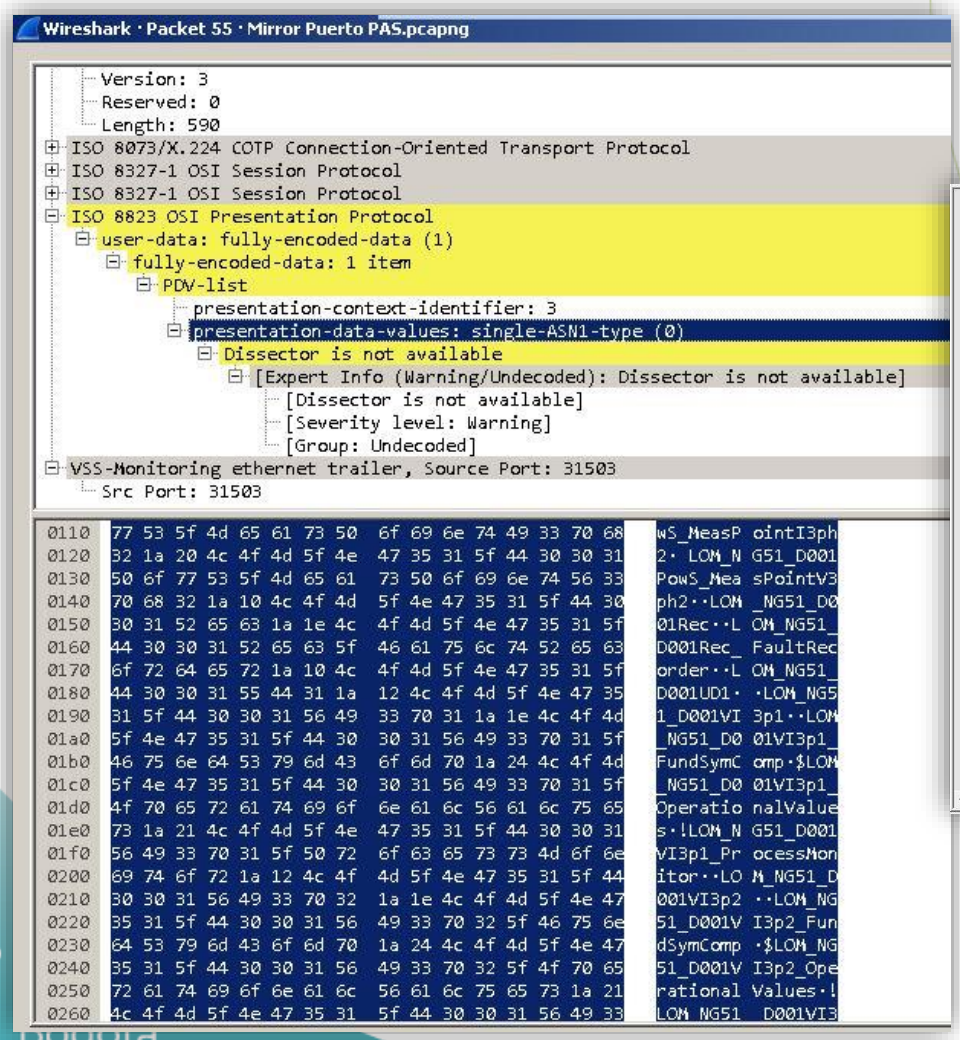
FUNCIONAN LOS PROTOCOLOS DE COMUNICACIÓN IEC 61850, IEC 60870-5-104, IEC 60870-5-101, IRIG-B, HSR, PRP, SNMP

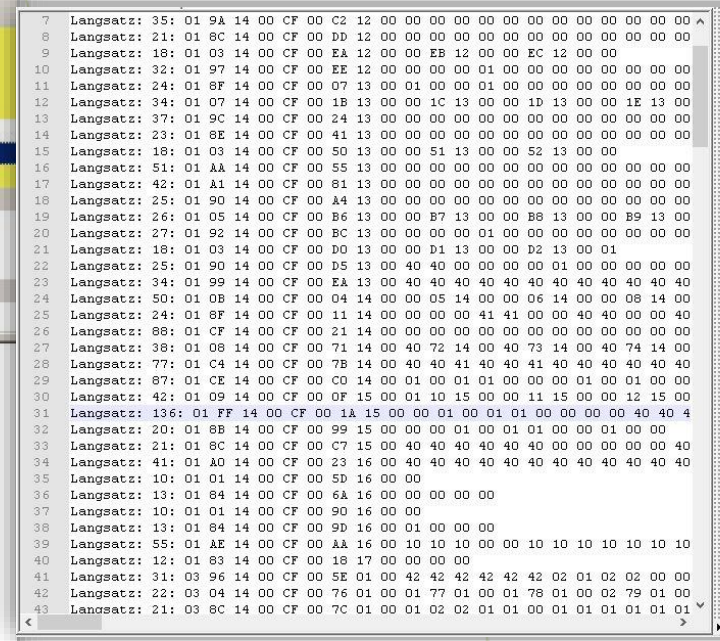
UI	User Interface
SDM	Source Data Management
DMS	Distribution Management System
DTS	Dispatcher Training Simulator
HIS	Historical Information System
SC	Supervisory Control
PA	Power Applications
XPS	Expert System
ADM	Archives HIS Administration
GIS	Geographic Information System
TCI	Telecommunication Interface
IFS	Independent Frint-End System
CA	Communication Applications
DW	Display Wall
LAN	Local Area Network
HMI	Human Machine Interface
RTU	Remote Terminal Unit
MED	Medidor
SER	Servidor
IED	Intelligent Electronic Device
PMU	Phasor Measurement Unit
CS	Controlador de Subestación
SM	Sistema de Monitoreo
PLC	Programmable Logic Controller
MP	Maletas de Prueba
87L	Diferencial de Línea
TP	Teleprotección
REG	Registrador de Fallas
MU	Merging Unit
CDB	Conexión a Bases de Datos
PP	Protocolo Propietario
PTP	Precision Time Protocol
NTP	Network Time Protocol

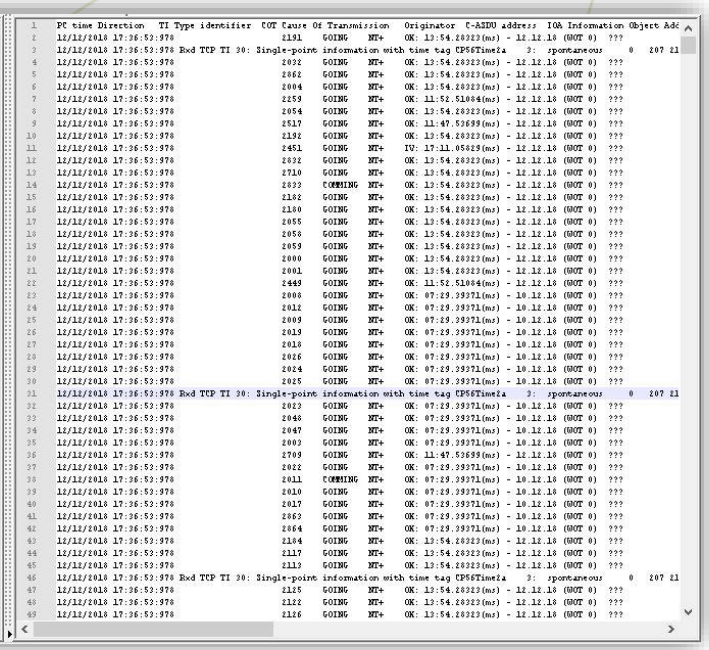


ESTUDIO DE CASO

Interpretación de tramas



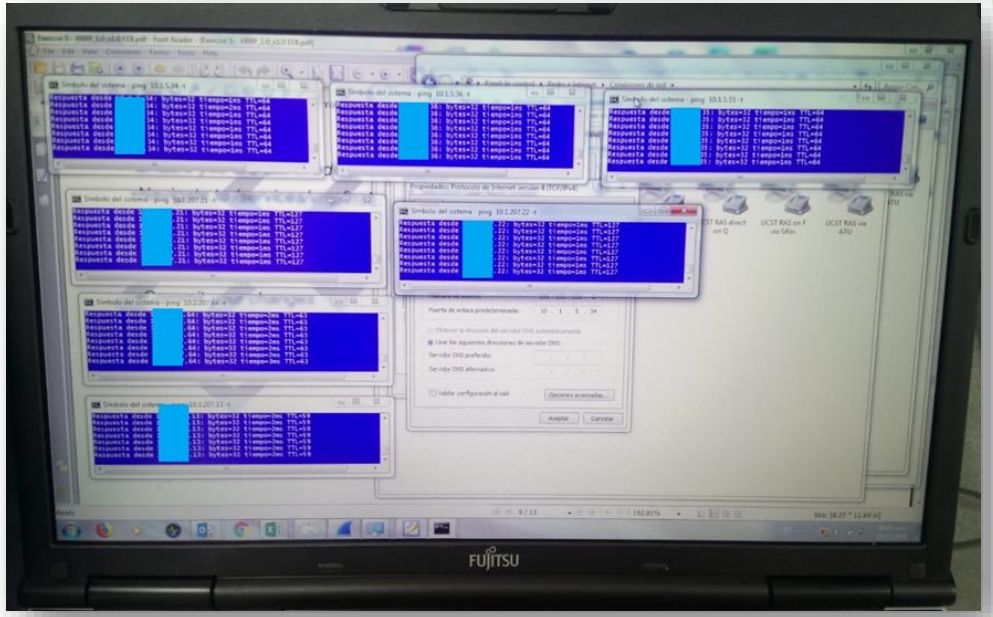




Bogotá

ESTUDIO DE CASO

Descubrimiento de red con ping




```
for i in $(seq 1 2);
    do
    for j in $(seq 1 254);
        do
            result=$(fping -A 192.168.$i.$j  | awk '{print $3}');
            if [ "$result" =  "alive" ];
                then
                    echo  "192.168.$i.$j GOOD is $result"

                else
                    echo "192.168.$i.$j BAD is $result"
                fi
        done
    done
```

Grupo Energía Bogotá

ESTUDIO DE CASO

Descubrimiento de red con ping

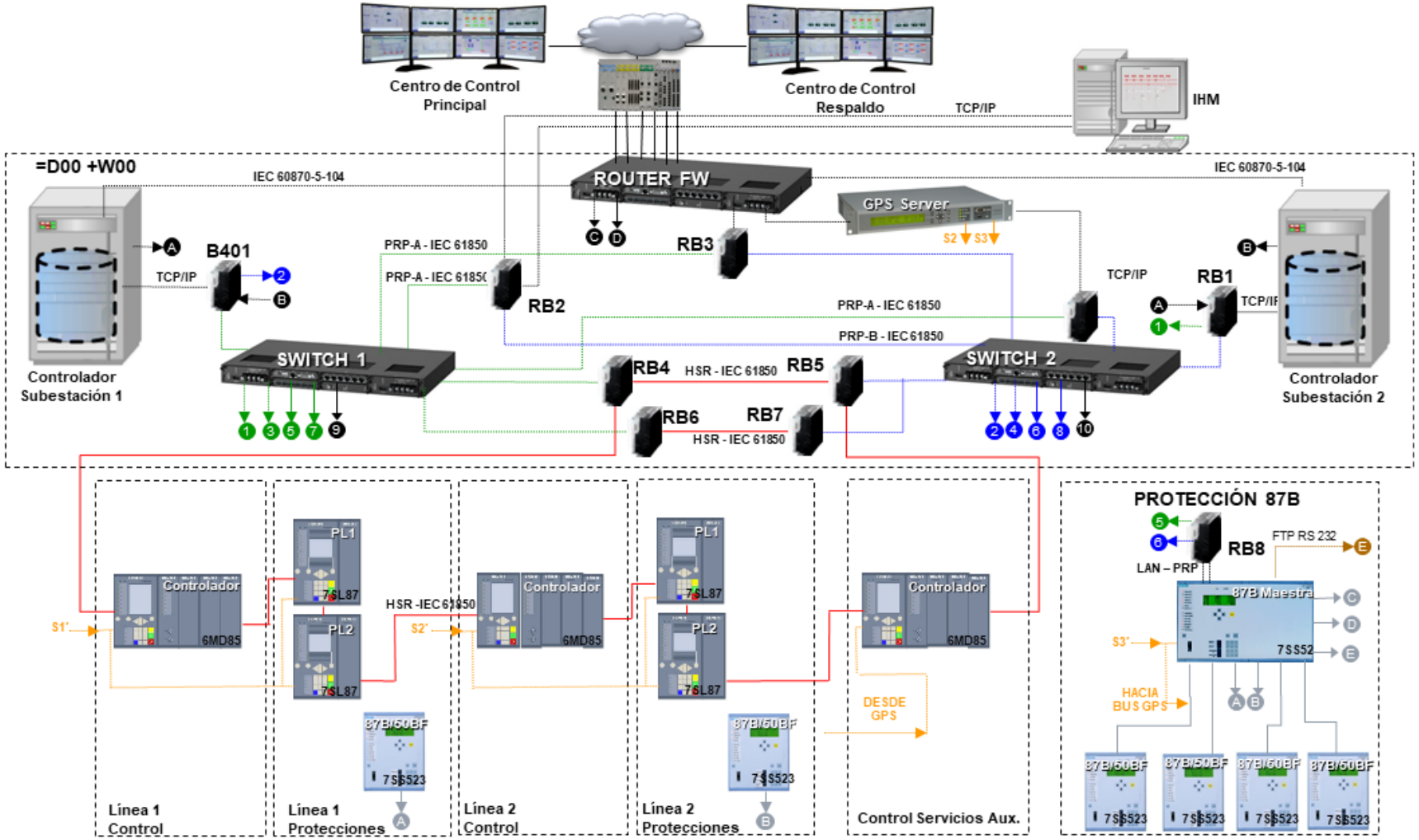
IP IDENTIFICADA	NOMBRE IED	GATEWAY	SUBRED	TIEMPO PING	VERSION SNMP	DESCRIPCION	TIPO EQUIPO	MAC	LINK CANAL 1	LINK CANAL 2	PROTOCOLO	SERVIDOR SNTP	SERIAL	REFERENCIA
XX.X.XXX.61	2D2_R02_F003	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.54.01995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025962	C53207A 602B110 1
XX.X.XXX.62	2D2_R02_F004	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC 5	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1802072804	C53207A 602B110 2
XX.X.XXX.63	2D3_R03_F003	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025956	C53207A 602B110 1
XX.X.XXX.64	2D3_R03_F004	XX.X.XXX.1	255.255.255.0	1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D3/SIP098EFFCF94	00 09 8E FF CF 94	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.65	2D4_R04_F003	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025963	C53207A 602B110 1
XX.X.XXX.66	2D4_R04_F004	XX.X.XXX.1	255.255.255.0	<1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D4/SIP098EFFCE2F	00 09 8E FF CE 2F	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.67	2D5_R05_F003	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1512061443	C53207A 602B110 1
XX.X.XXX.68	2D5_R05_F004	XX.X.XXX.1	255.255.255.0	1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D5/SIP098EFFCE32	00 09 8E FF CE 32	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.69	2D6_R06_F003	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025942	C53207A 602B110 1
XX.X.XXX.70	2D7_R07_F003	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.54.01995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025950	C53207A 602B110 1
XX.X.XXX.71	2D7_R07_F004	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC 5	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1802072821	C53207A 602B110 2
XX.X.XXX.72	2D9_R09_F003	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1510048742	C53207A 602B110 1
XX.X.XXX.73	2D9_R09_F004	XX.X.XXX.1	255.255.255.0	1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D9/SIP098EFFCF98	00 09 8E FF CF 98	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.74	2D10_R10_F003	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025964	C53207A 602B110 1
XX.X.XXX.75	2D10_R10_F004	XX.X.XXX.1	255.255.255.0	1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D10/SIP098EFFCE30	00 09 8E FF CE 30	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.76	2D12_R12_F003	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025965	C53207A 602B110 1
XX.X.XXX.77	2D12_R12_F004	XX.X.XXX.1	255.255.255.0	<1ms	V2	SIPROTEC4 EN100_O V04.29.01_01 Ed2	EN100_O F004_D12/SIP098EFFCE2D	00 09 8E FF CE 2D	Up	Up	HSR	XX.X.XXX.161	N/E	N/E
XX.X.XXX.121	2D2_w02_D001	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025966	C53207A 602B110 1
XX.X.XXX.122	2D3_w03_D001	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410061244	C53207A 602B110 1
XX.X.XXX.123	2D4_w04_D001	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410061221	C53207A 602B110 1
XX.X.XXX.124	2D5_W05_D001	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410061235	C53207A 602B110 1
XX.X.XXX.125	2D6_W06_D001	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410039613	C53207A 602B110 1
XX.X.XXX.126	2D7_W07_D001	XX.X.XXX.1	255.255.255.0	2 ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410061223	C53207A 602B110 1
XX.X.XXX.127	2D9_W09_D001	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410061228	C53207A 602B110 1
XX.X.XXX.128	2D10_W10_D001	XX.X.XXX.1	255.255.255.0	1ms	V3	SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.3103.995	sip5com	00 00 7A CC 00 14	Up	Up	HSR	XX.X.XXX.161	BF1410025930	C53207A 602B110 1

Grupo Energía Bogotá

ESTUDIO DE CASO

Arquitectura de red e identificación de activos secundarios y terciarios

EN TOTAL SE IDENTIFICARON 87 ACTIVOS SECUNDARIOS Y TERCIARIOS EN EL SISTEMA



Grupo Energía Bogotá

ESTUDIO DE CASO

Escaneo de servicios abiertos equipos de cómputo

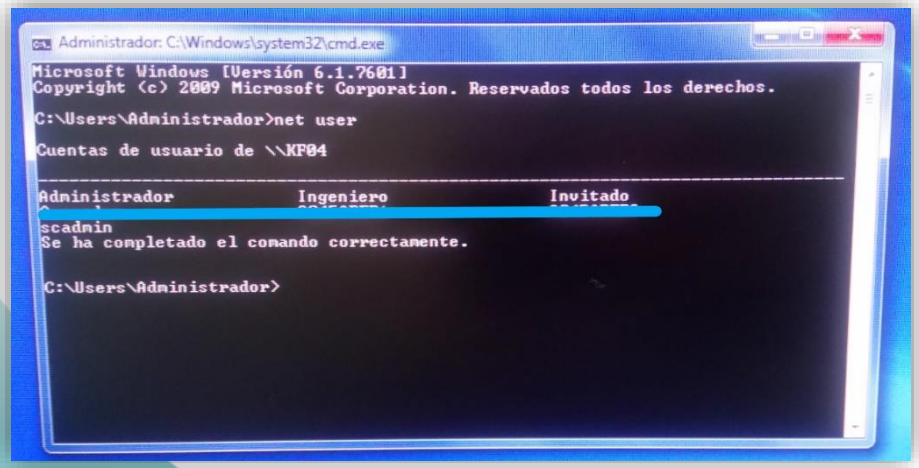
```
Nmap scan report for [redacted]
Host is up (0.89s latency).
Not shown: 998 open|filtered ports, 991 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
111/tcp   open     rpcbind
587/tcp   filtered submission
5900/tcp  open     vnc
6666/tcp  filtered irc
6667/tcp  filtered irc
6668/tcp  filtered irc
6669/tcp  filtered irc
111/udp   open     rpcbind
123/udp   open     ntp
```

Grupo Energía Bogotá

ESTUDIO DE CASO

Ataque de fuerza bruta para identificar credenciales RDP

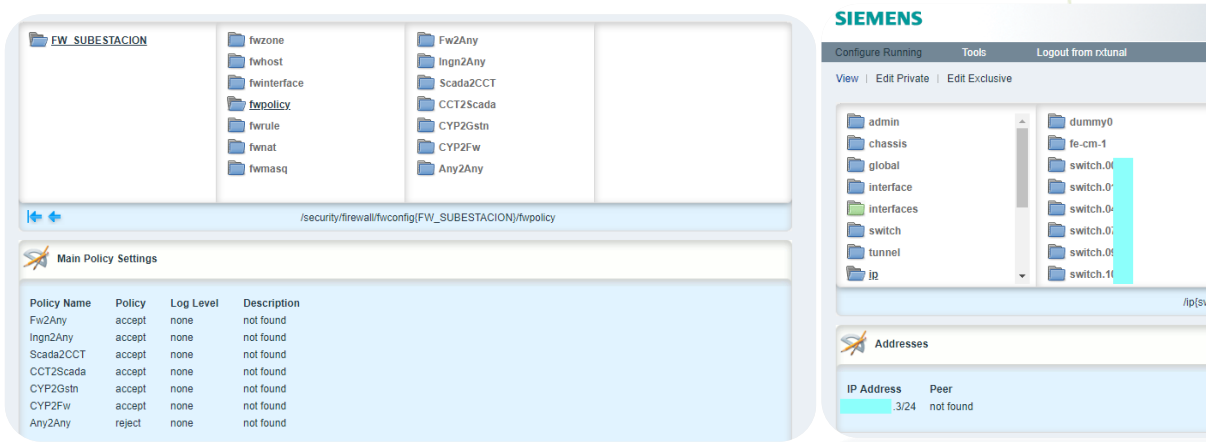
```
root@kali:~/Escritorio/[redacted]# nbtscan [redacted].41
Doing NBT name scan for addresses from [redacted].41

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
[redacted].41    [redacted]IHM    <server>  <unknown>        2c:44:fd:0c:b3:cd
root@kali:~/Escritorio/[redacted]# nbtscan [redacted].2-50
Doing NBT name scan for addresses from [redacted].2-50

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
[redacted].22    [redacted]GW2    <server>  <unknown>        00:1b:1b:83:67:df
```

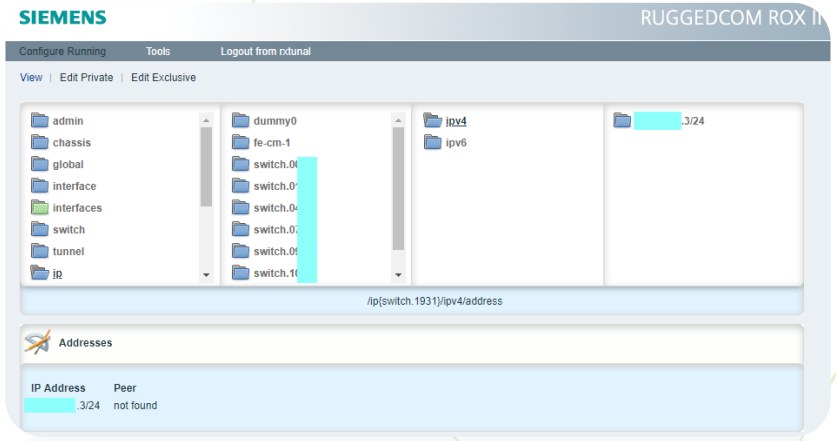


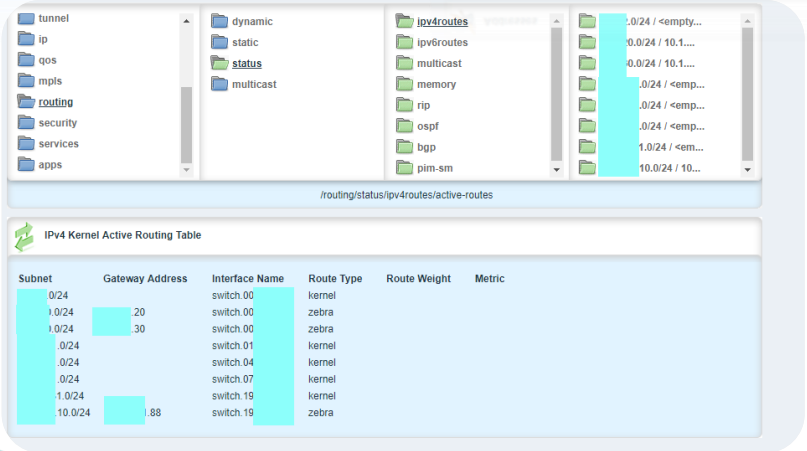
Grupo Energía Bogotá

ESTUDIO DE CASO

Descubrimiento de configuración de Router/Firewall







PUERTO ROUTER	DESTINO
LM1/1	RESERVA
LM1/2	104 SU1
LM1/3	Gestion CYP
LM1/4	104 SU2
LM1/5	Gestion -RF y SVC
LM1/6	RESERVA
LM2/1	RESERVA
LM2/2	RESERVA
LM2/3	RESERVA
LM2/4	RESERVA
LM2/5	RESERVA
LM2/6	RESERVA
LM3/1	SDH - P1 VIDEO
LM3/2	SDH Corporativa
LM3/3	SDH - TELEFONO
LM3/4	SDH - CCT
LM4/1	Gestion -RF y SVC
LM4/2	SDH - Gestion CYP
LM4/3	SDH - Teleprotección - Gestion
LM4/4	SDH - Gestion CYP

Grupo Energía Bogotá

ESTUDIO DE CASO

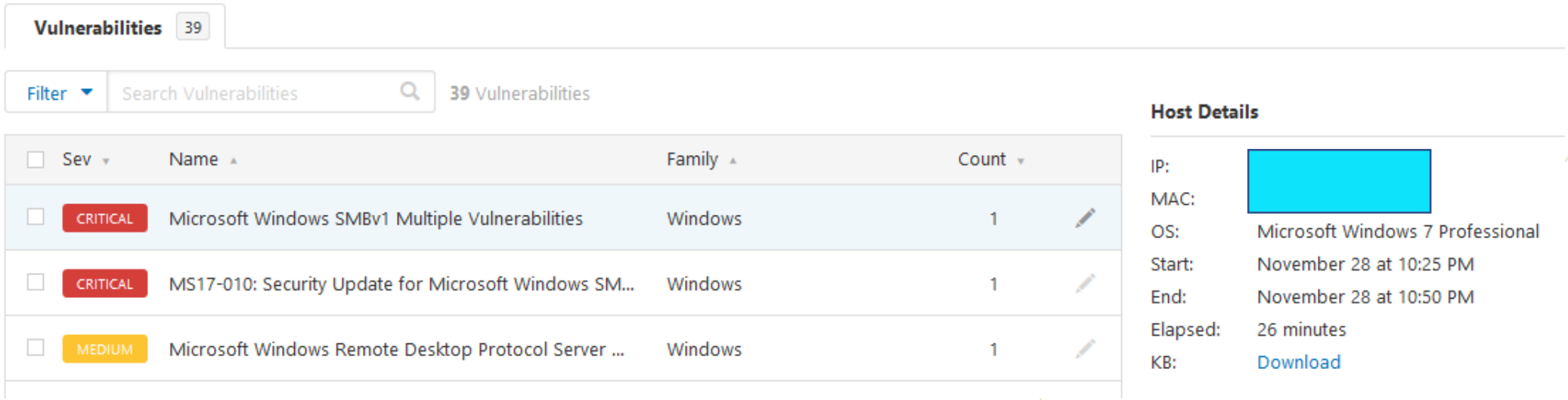
Ingreso equipo de comunicación remoto desde el Router local

```
Welcome to Rugged CLI
admin connected from [redacted].105 using http on rx[redacted]
rx[redacted]# ssh host 10.1.6.1
The authenticity of host[redacted].1 ([redacted].1)' can't be established.
DSA key fingerprint is b6:7e:d8:a0:fd:ac:82:74:47:20:e5:9b:b6:6f:47:1a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added [redacted].1' (DSA) to the list of known hosts.
admin@[redacted].1's password:
Welcome to Rugged CLI
admin connected from [redacted].3 using ssh on rx1gestion
rx1[redacted]#
```

Grupo Energía Bogotá

ESTUDIO DE CASO

Vulnerabilidades de sistemas operativos



Grupo Energía Bogotá

ESTUDIO DE CASO

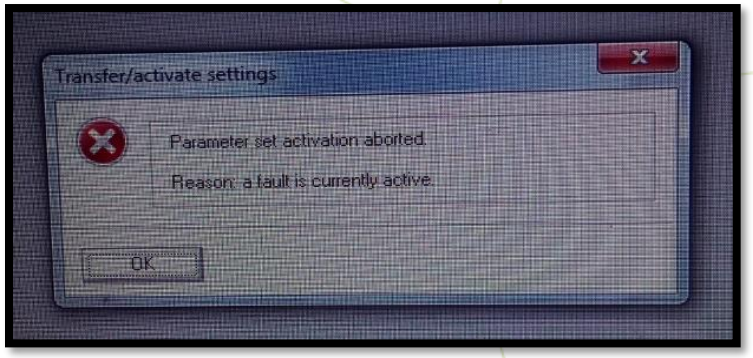
Vulnerabilidades de dispositivos OT instalados

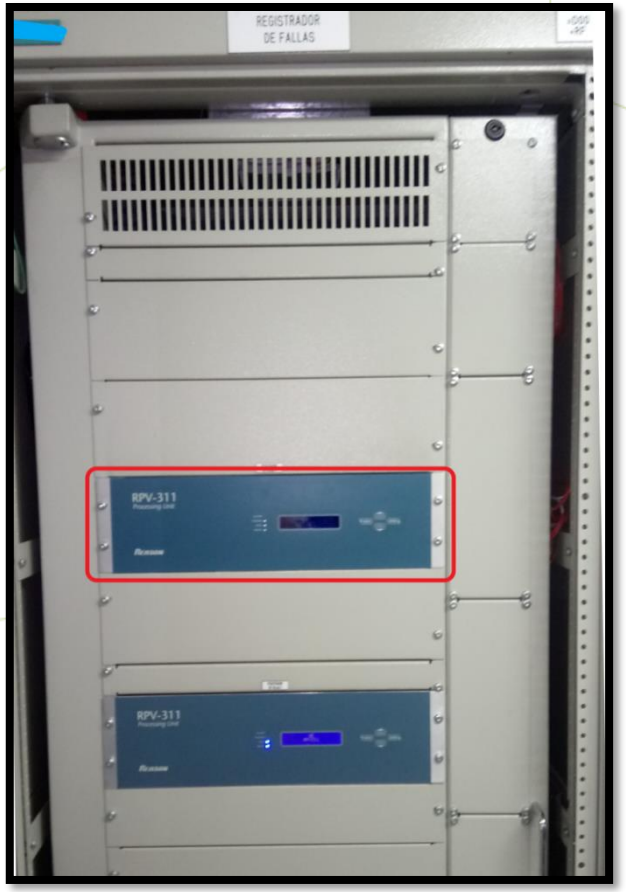
SSA-104088: Denial-of-Service Vulnerabilities in [redacted] Ethernet Communication Module and [redacted] relays

Publication Date: 2019-02-12
Last Update: 2019-02-12
Current Version: V1.0
CVSS v3.0 Base Score: 7.5

SUMMARY

The [redacted] Ethernet communication module and [redacted] relays are affected by a security vulnerability which could allow an attacker to conduct a Denial-of-Service attack over the network. [redacted] has released updates for some affected products, is working on updates for the remaining affected products, and recommends specific countermeasures until fixes are available.

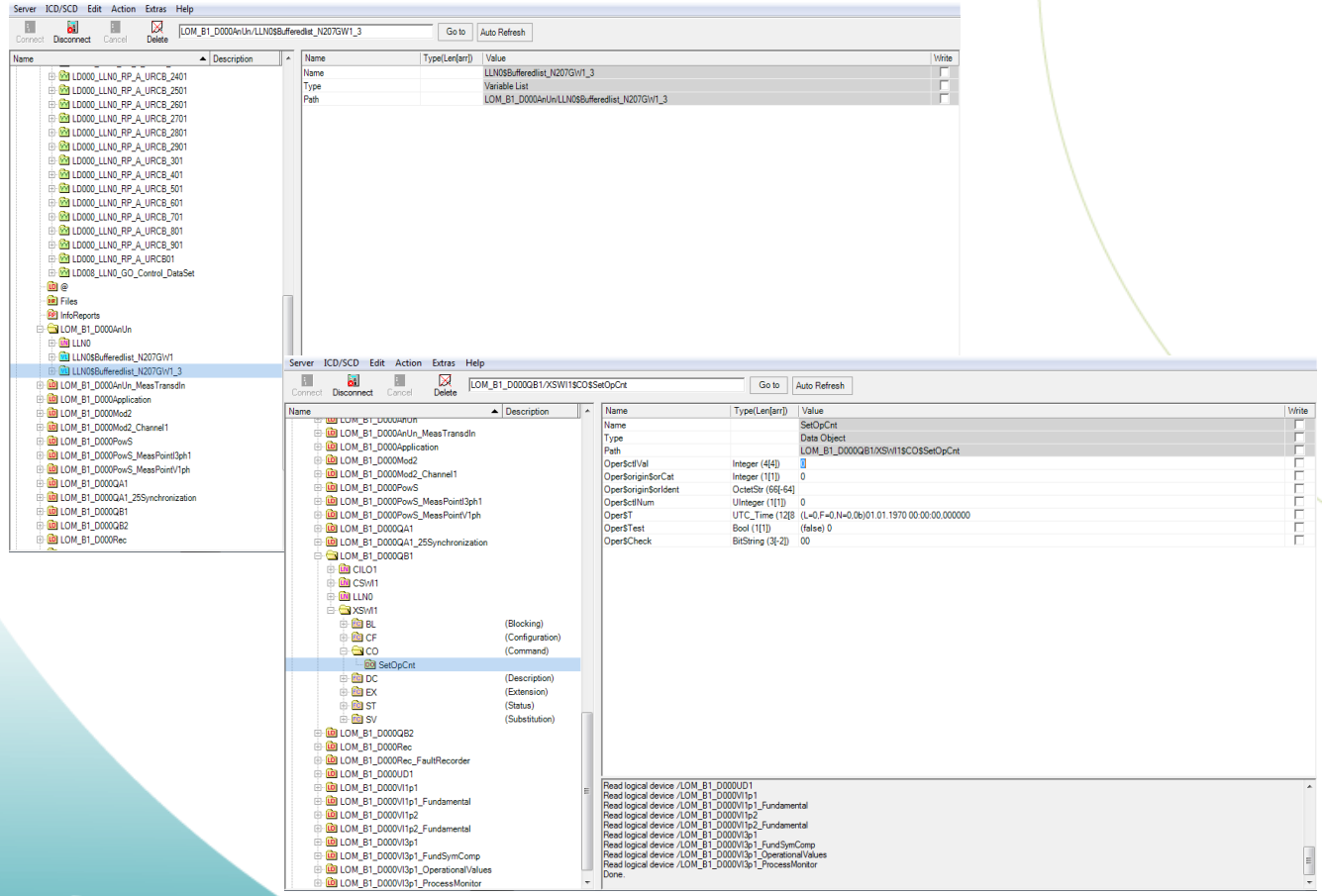




Grupo Energía Bogotá

ESTUDIO DE CASO

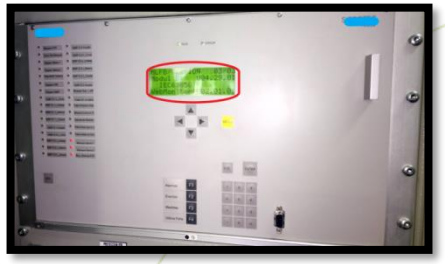
Vulnerabilidades de dispositivos OT instalados

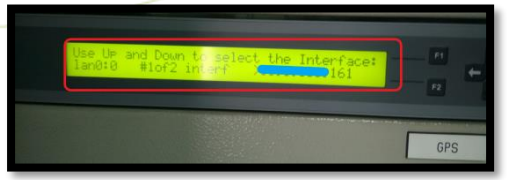


Grupo Energía Bogotá

ESTUDIO DE CASO

Vulnerabilidades de dispositivos OT instalados

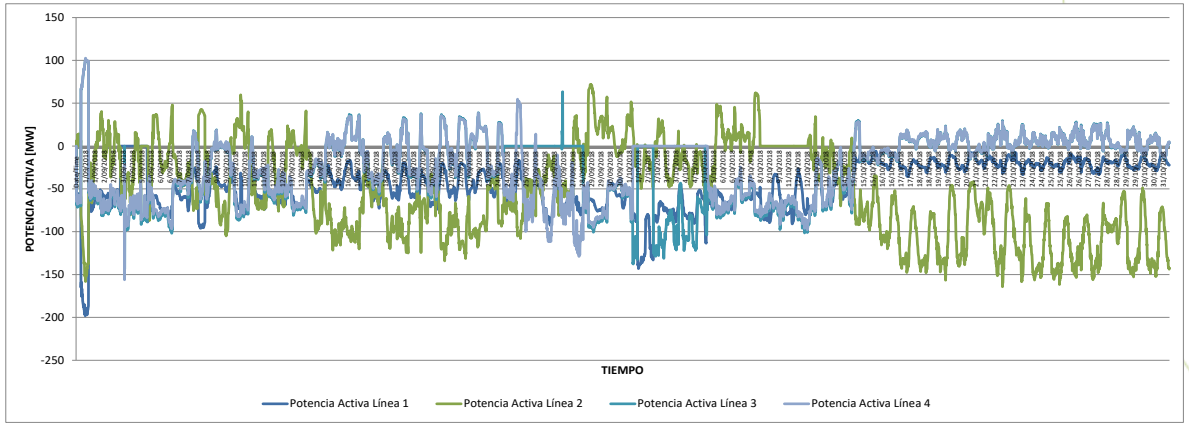


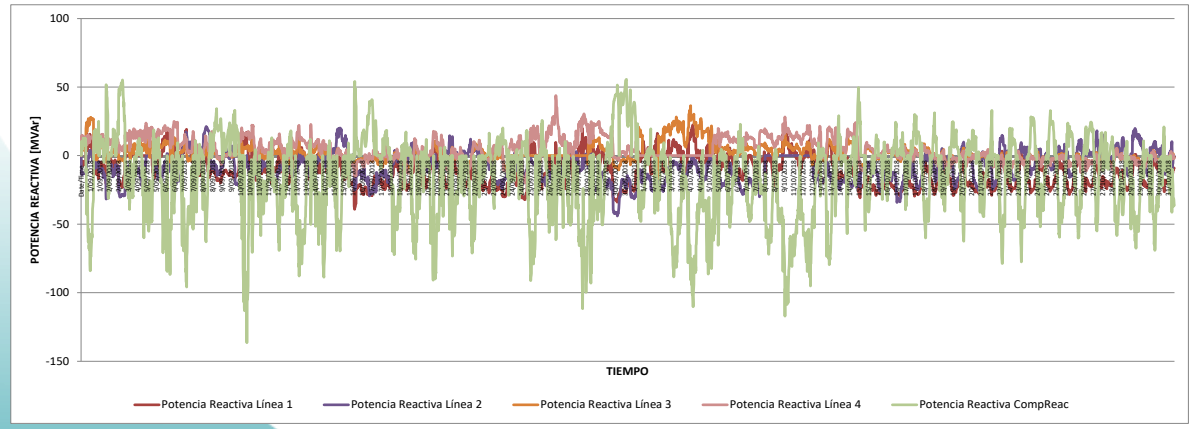


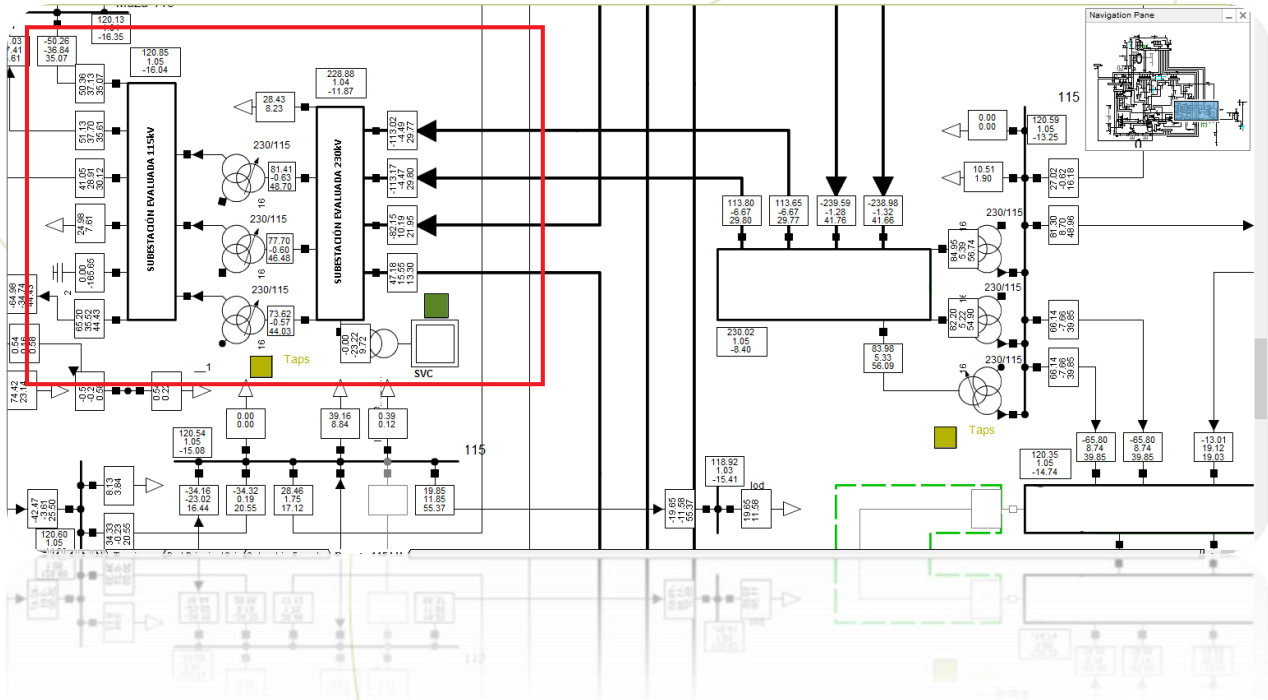
Grupo Energía Bogotá

ESTUDIO DE CASO

Cálculo del IVO



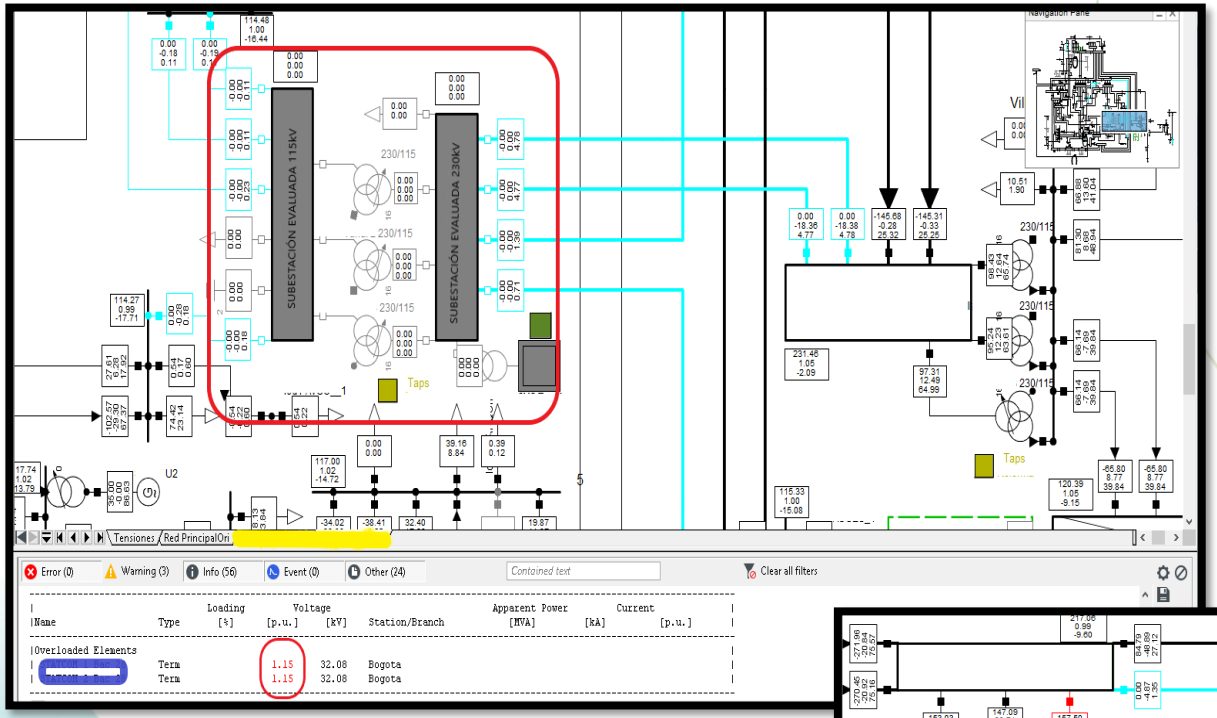


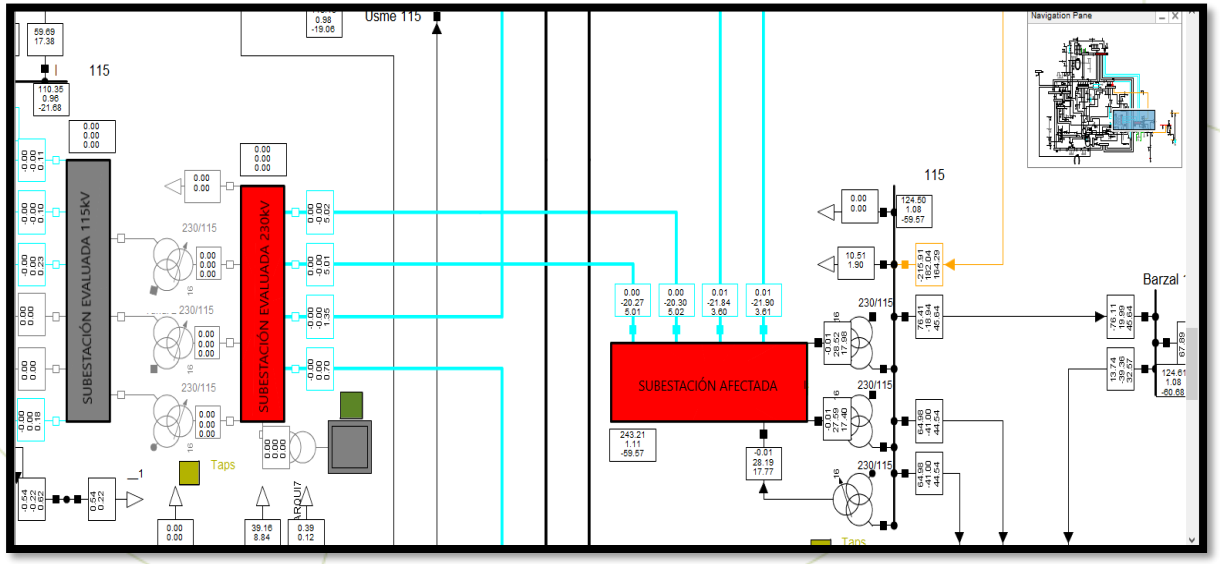


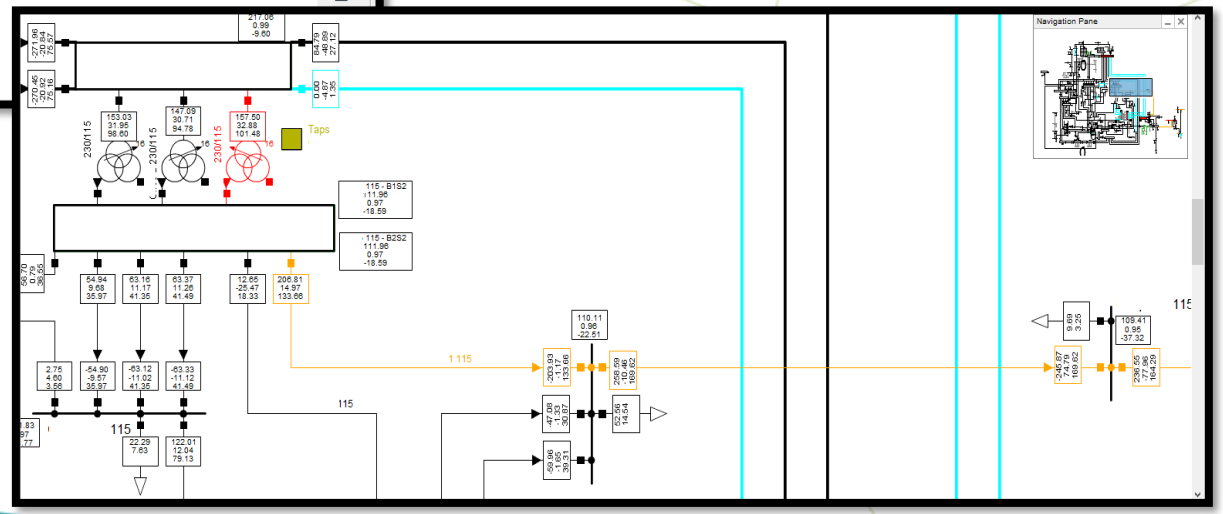
Grupo Energía Bogotá

ESTUDIO DE CASO

Cálculo del IVO







ESTUDIO DE CASO

Cálculo del IVO

$$DNA[MWh] = 259{,}93[MW] * 2$$

$$DNA[MWh] = 519{,}86[MWh]$$

$$DNA \leq 1000MWh = 0{,}1 + \left(0{,}6 * \frac{519{,}86[MWh]}{1000\ [MWh]}\right)$$

$$\boldsymbol{DNAn = 0{,}41}$$

$$PS = 4 * 300 + 5 * 700$$

$$PS = 4700$$

$$PSn = 0{,}7 + \left(0{,}3 * \frac{4700}{10000}\right)$$

$$\boldsymbol{PSn = 0{,}84}$$

$$\mathrm{PC} = 1 - 51/64$$

$$\mathbf{PC = 0{,}20}$$

$$IVO = 0{,}4 * 0{,}41 + 0{,}4 * 0{,}20 + 0{,}2 * 0{,}84$$

$$\boldsymbol{IVO = 0{,}42}$$

Grupo Energía Bogotá

ESTUDIO DE CASO

Cálculo del IVS

$$IAC = \frac{(1) * 2 + (3)}{16} = 0{,}312$$

$$DC = \frac{(0) * 2 + (2)}{8} = 0{,}250$$

$$TRE = \frac{(1) * 2 + (0)}{6} = 0{,}333$$

$$UC = \frac{(2) * 2 + (2)}{14} = 0{,}428$$

$$SI = \frac{(0) * 2 + (0)}{10} = 0$$

$$RDF = \frac{(4) * 2 + (2)}{12} = 0{,}833$$

$$RA = \frac{(3) * 2 + (1)}{18} = 0{,}388$$

$$\boldsymbol{IVS = 1 - \left[\left(\frac{1}{7}\right) * (0{,}312 + 0{,}333 + 0{,}428 + 0 + 0{,}250 + 0{,}833 + 0{,}388)\right]}$$

$$\boldsymbol{IVS = 0{,}637}$$

Grupo Energía Bogotá

ESTUDIO DE CASO

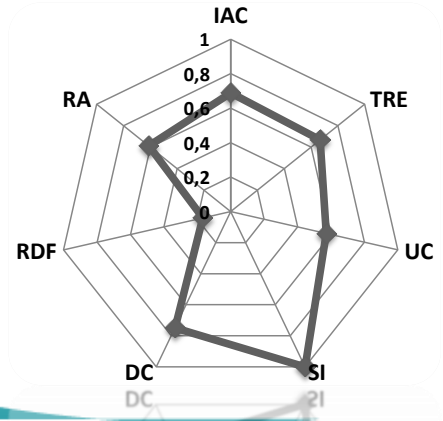
IVO
Si se tiene simultaneidad de afectación > N-2 con otra subestación del área de influencia, con una alta probabilidad podría generar un blackout.

$$IVO = 0,420 \Rightarrow 42,0\%$$

$$IVS = 0,637 \Rightarrow 63,7\%$$

Rango Medio 0,3> & <=0,7

IVS
Puntos críticos de vulnerabilidades



Grupo Energía Bogotá

Juan Carlos Carreño Pérez

¡MUCHAS GRACIAS!

jcarreno@geb.com.co
jccarrenop@correo.udistrital.edu.co
https://www.linkedin.com/in/juan-carlos-carreño-perez-891262132

Grupo Energía Bogotá

Mejoramos vidas con energía sostenible y competitiva

GrupoEnergíaBogotá