

# CARACTERIZACIÓN DE AMENAZAS CIBERNÉTICAS EN SISTEMAS DE TRANSMISIÓN 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

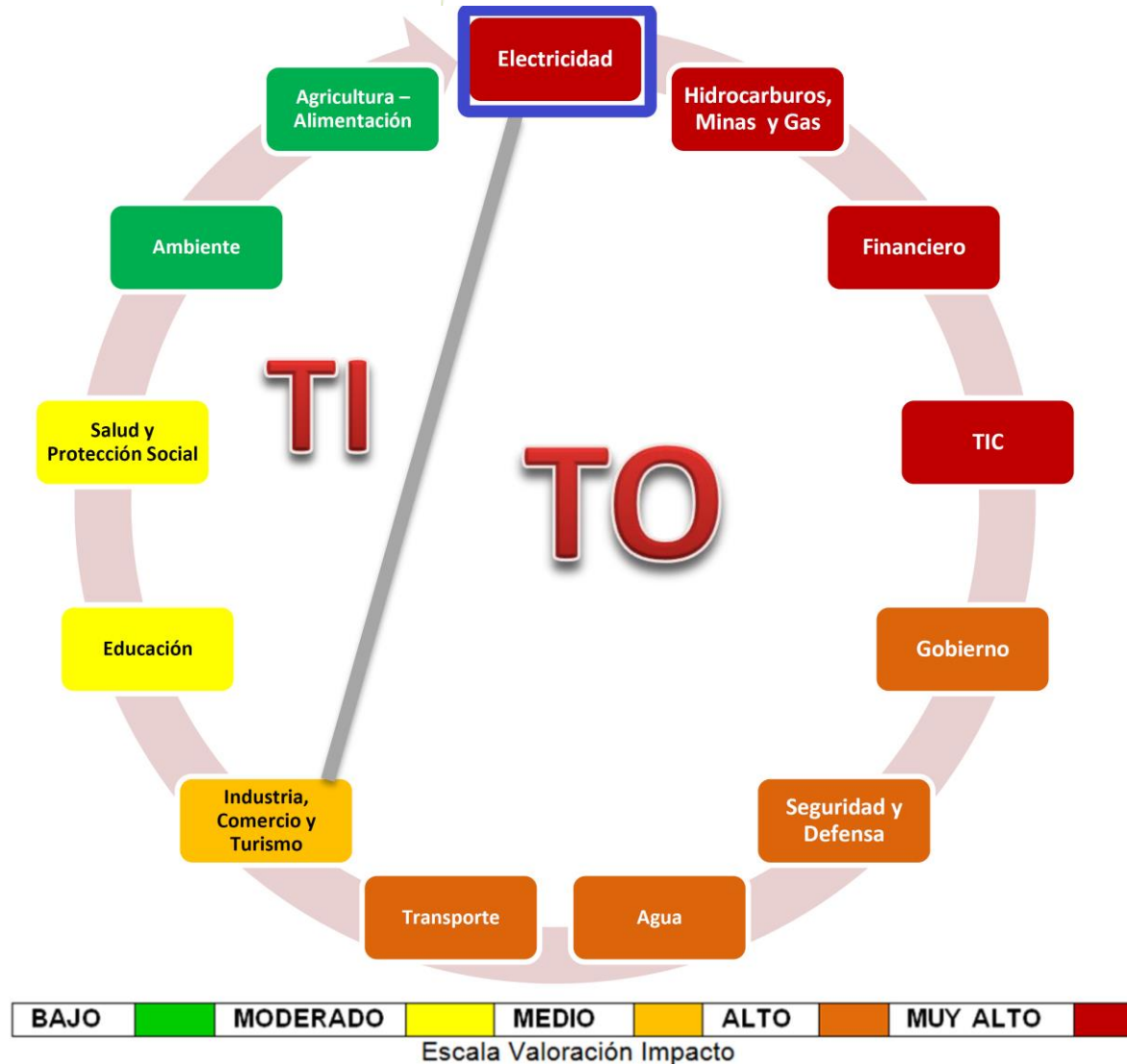
- INFRAESTRUCTURA CRÍTICA.
- CONCEPTOS GENERALES.
- METODOLOGÍA.
- ESTUDIO DE CASO.
- PREGUNTAS.





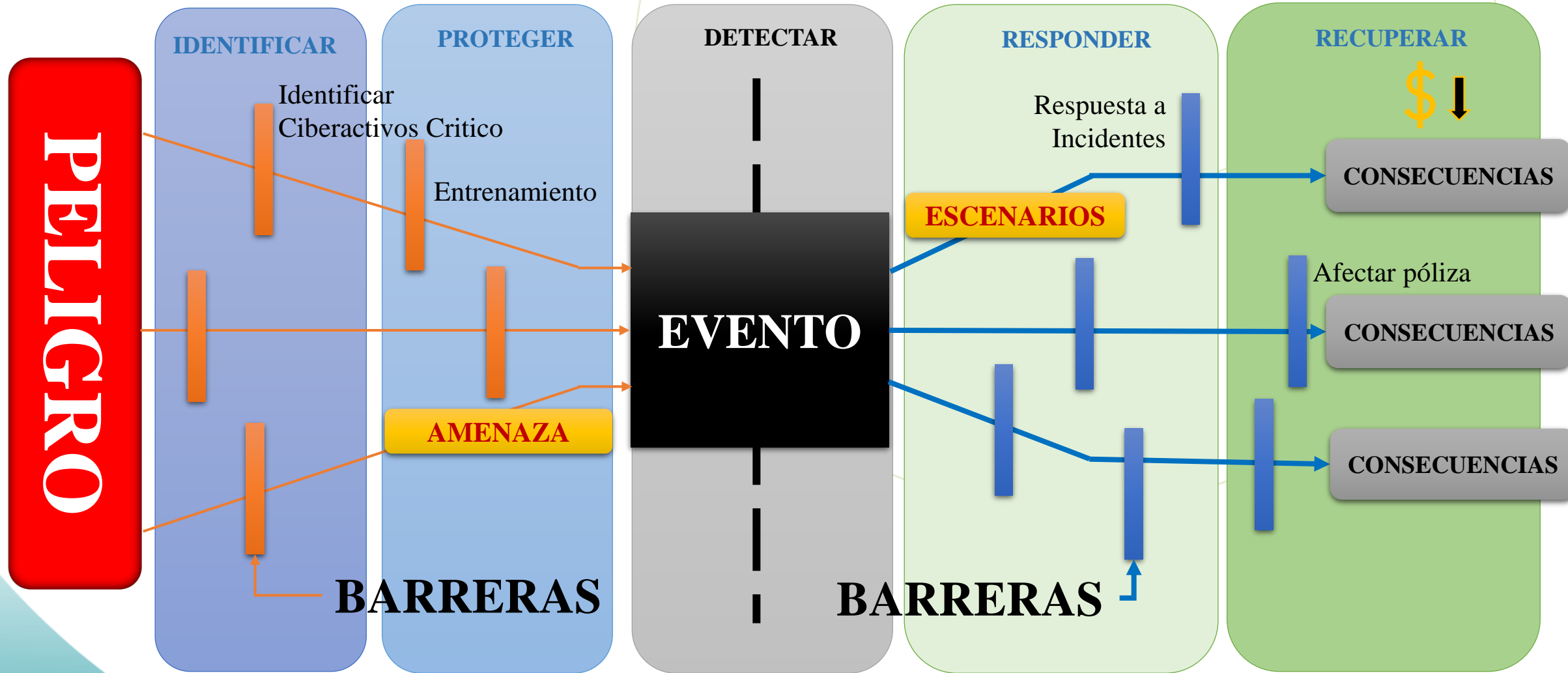
# AMENAZAS CIBERNÉTICAS

# INFRAESTRUCTURA CRÍTICA



Disminución de la probabilidad

Disminución del impacto



# MODELO DE FUNCIONAMIENTO

## SERVICIOS REMOTOS

8

### Inteligencia Operacional

- Analítica, Inteligencia Artificial, Algoritmos, Predicción, Estabilidad del Sistema, Proyección de Demanda, despacho de Generación.

7

### Sistemas

- Scada, ERP, MRP, Software de Gestión, Monitoreo, Sincrofasores, Ondas Viajeras, Estimación de estados, Simuladores eléctricos.

6

### Comunicaciones

- Protocolos de comunicación, Medios Físicos (FO, Onda Portadora, Radio, Microondas, Satélite, GPRS), Equipos Físicos (SDH, PDH, Routers, MPLS, DWDM, GPON).

5

### Procesamiento

- Lógicas de Automatismos, Algoritmos de Protección Eléctrica, Supervisión, Control, Registro de Eventos, Almacenamiento de Comtrade, Auto diagnósticos.

4

### Transporte de Información

- Protocolos de Comunicación, Medios Físicos (Fibra Óptica, SFTP, Seriales RS232-RS485)

3

### Dispositivos y Componentes Inteligentes

- Gateway, RTU (Remote Terminal Unit), IED, Controladores, Protecciones, Teleprotecciones, Registradores de Fallas, PMU, Routers, Switches, RedBox.

2

### Enlace de Datos Físicos

- Sensores, BI/BO/AI Controladores, BI/BO/AI Protecciones, BI/BO/AI RTU, Transductores, Maletas de Pruebas, Mediciones Indirectas.

1

### Elementos Físicos

- Equipos de Potencia (Interruptores, Seccionadores, Transformadores, CT's, PT's, Descargadores etc.), Líneas de Transmisión, Torres, Merging Unit.

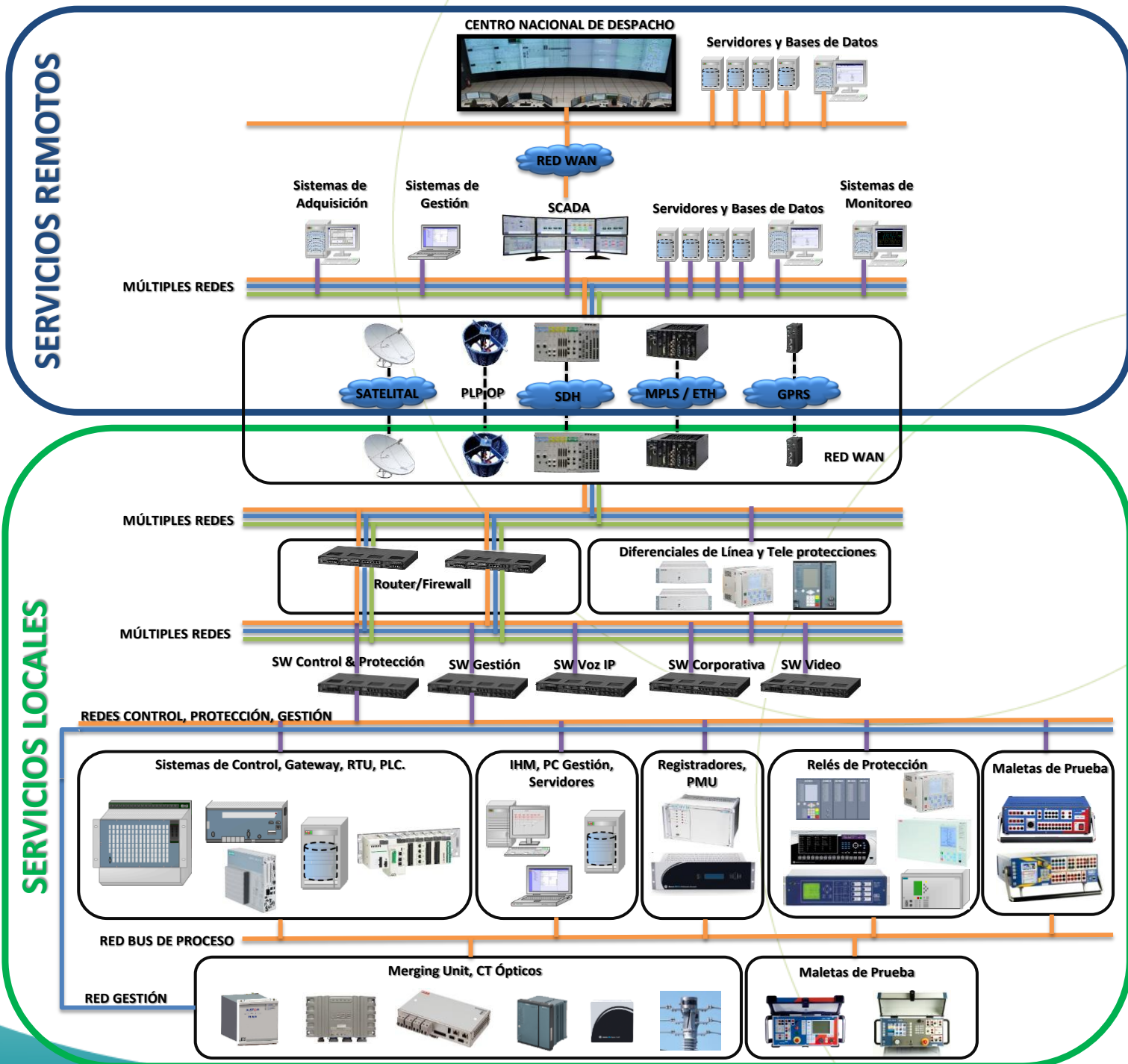
NIVEL 3

NIVEL 2

NIVEL 1

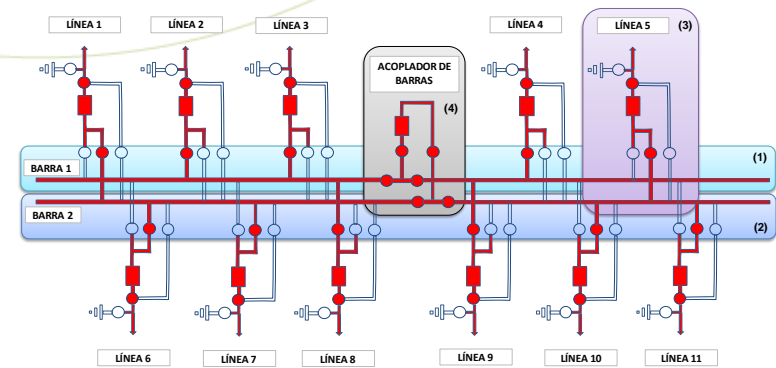
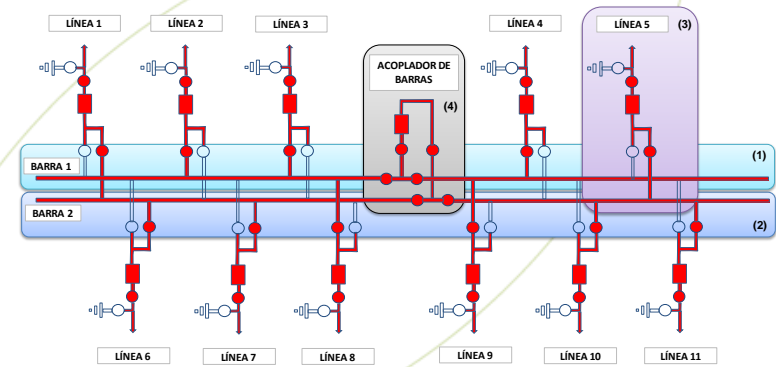
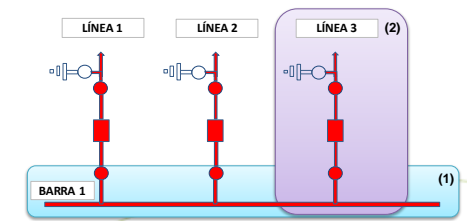
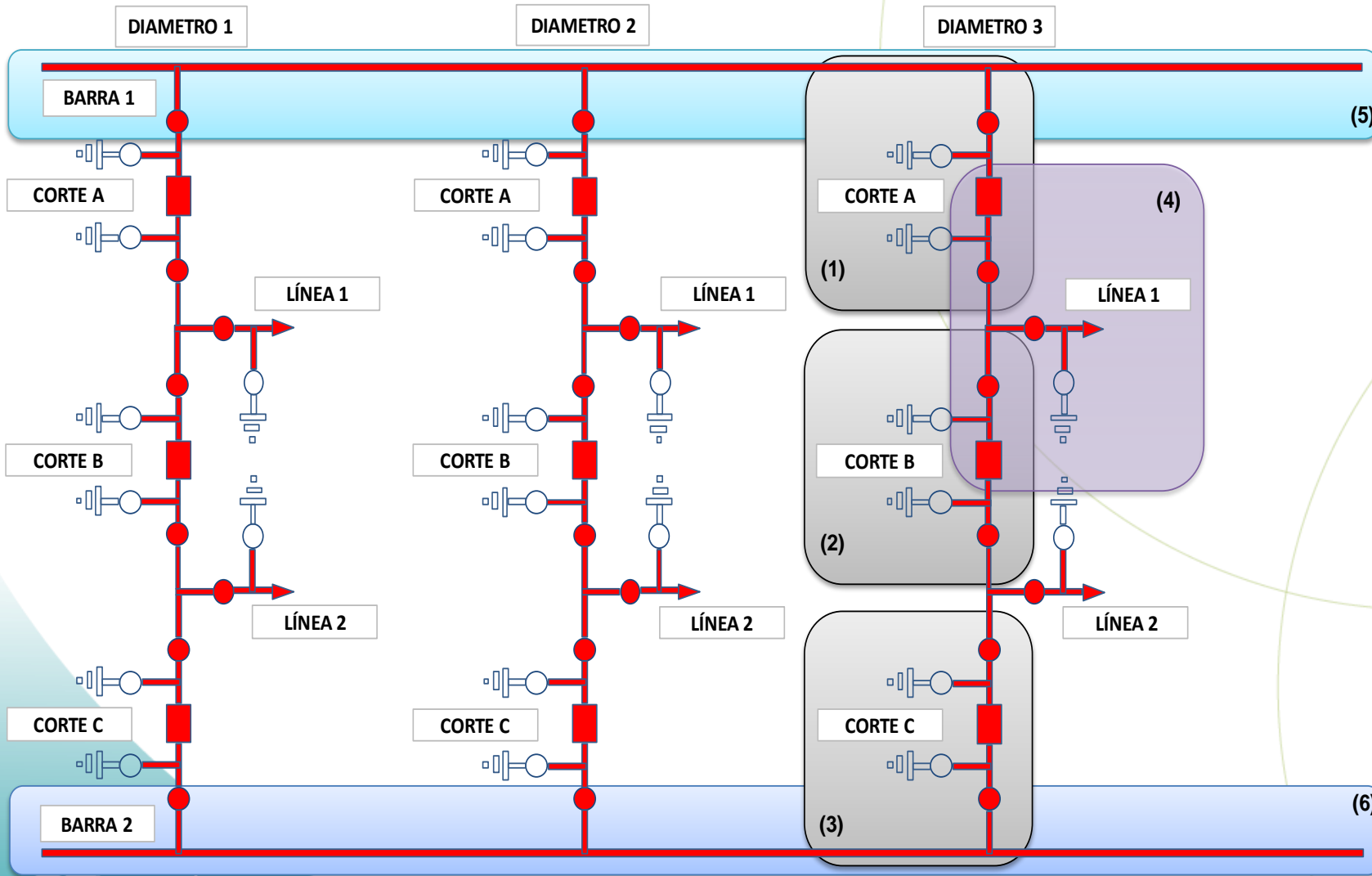
NIVEL 0

## SERVICIOS LOCALES



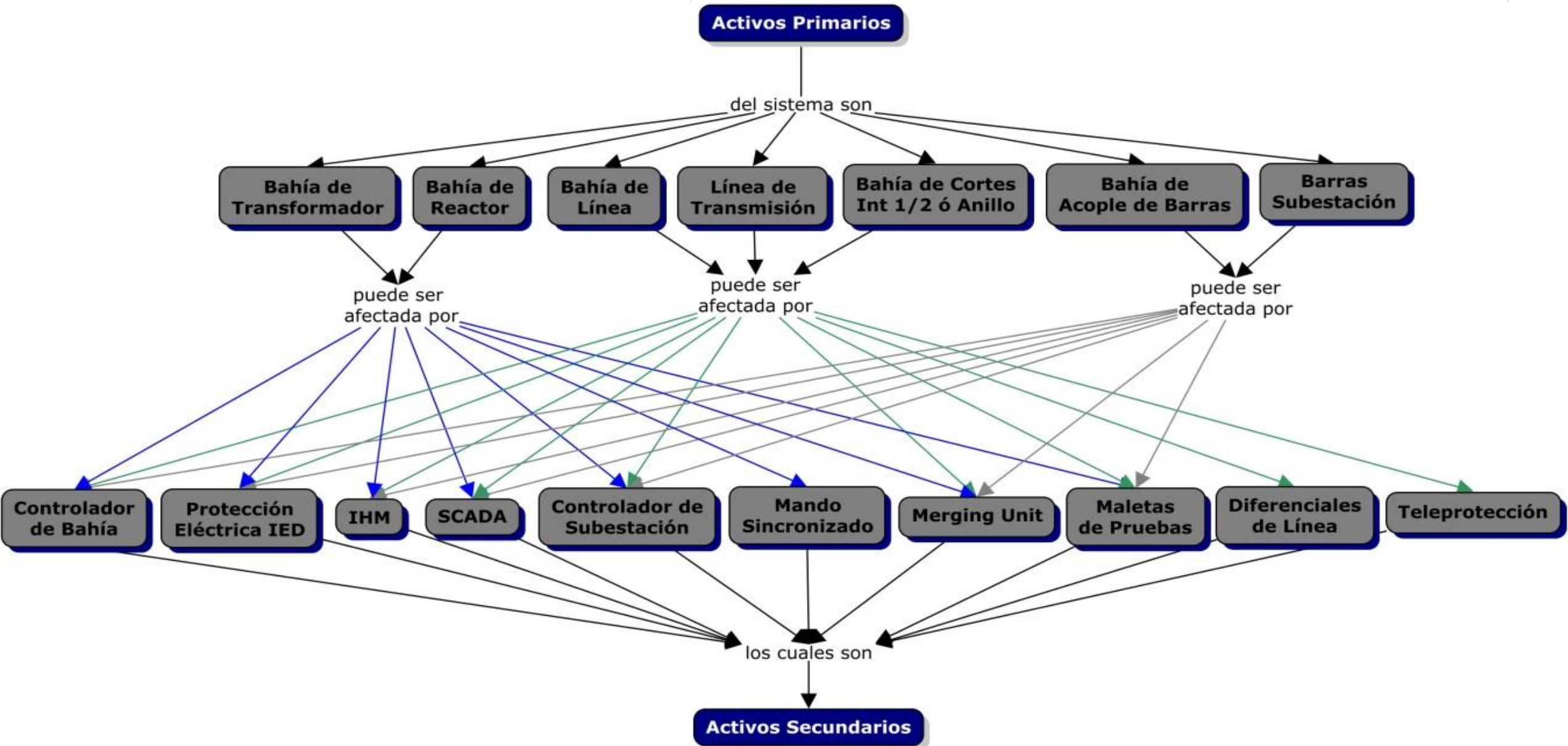


# ACTIVOS PRIMARIOS

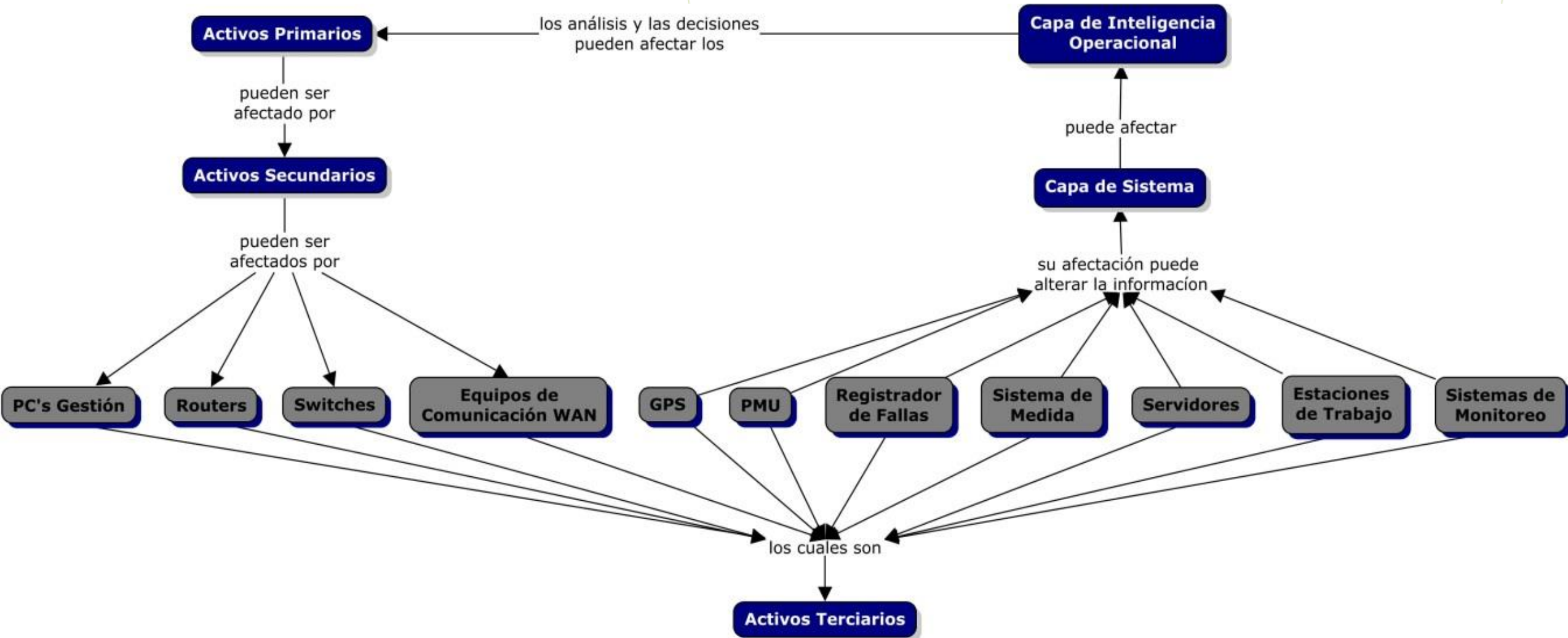




# ACTIVOS SECUNDARIOS

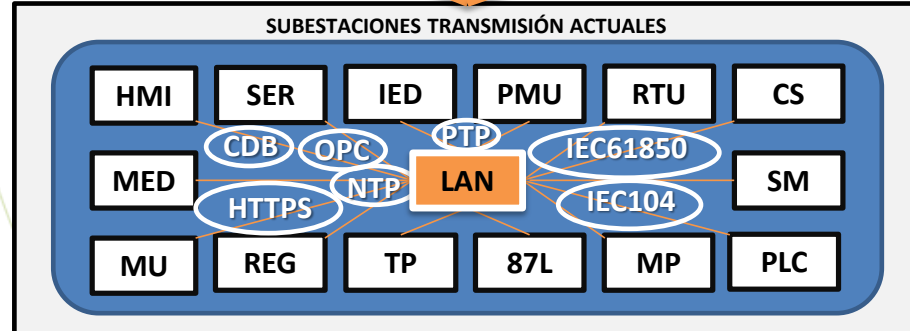
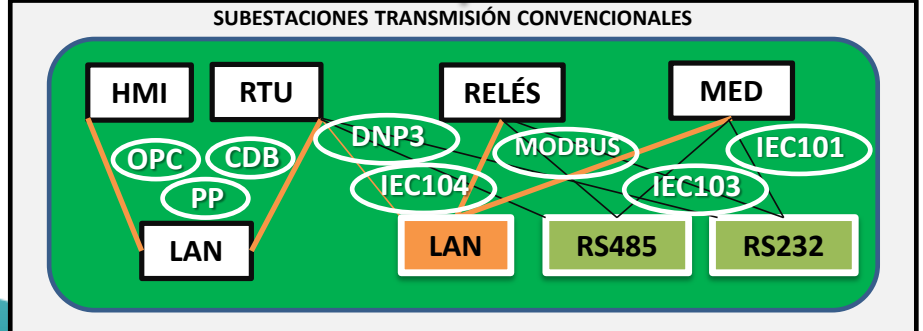
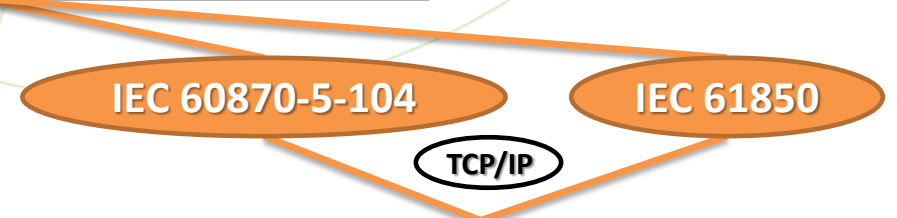
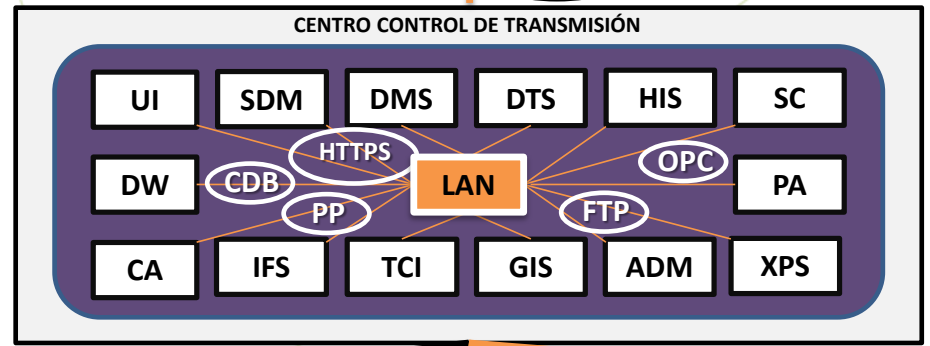
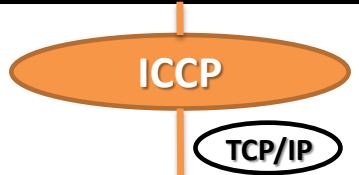
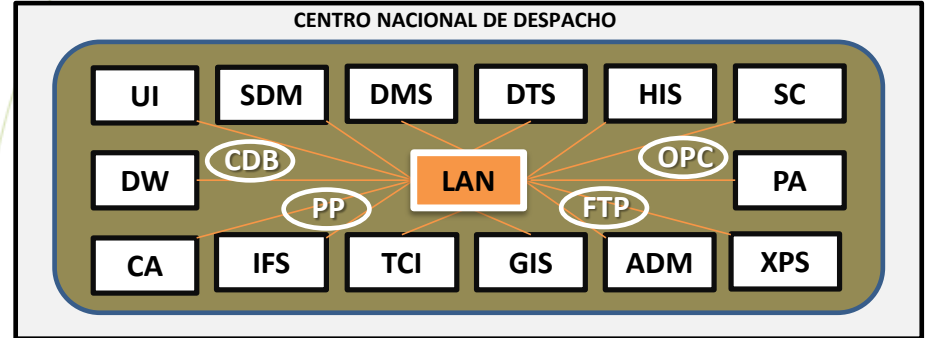


# ACTIVOS TERCIARIOS



| 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

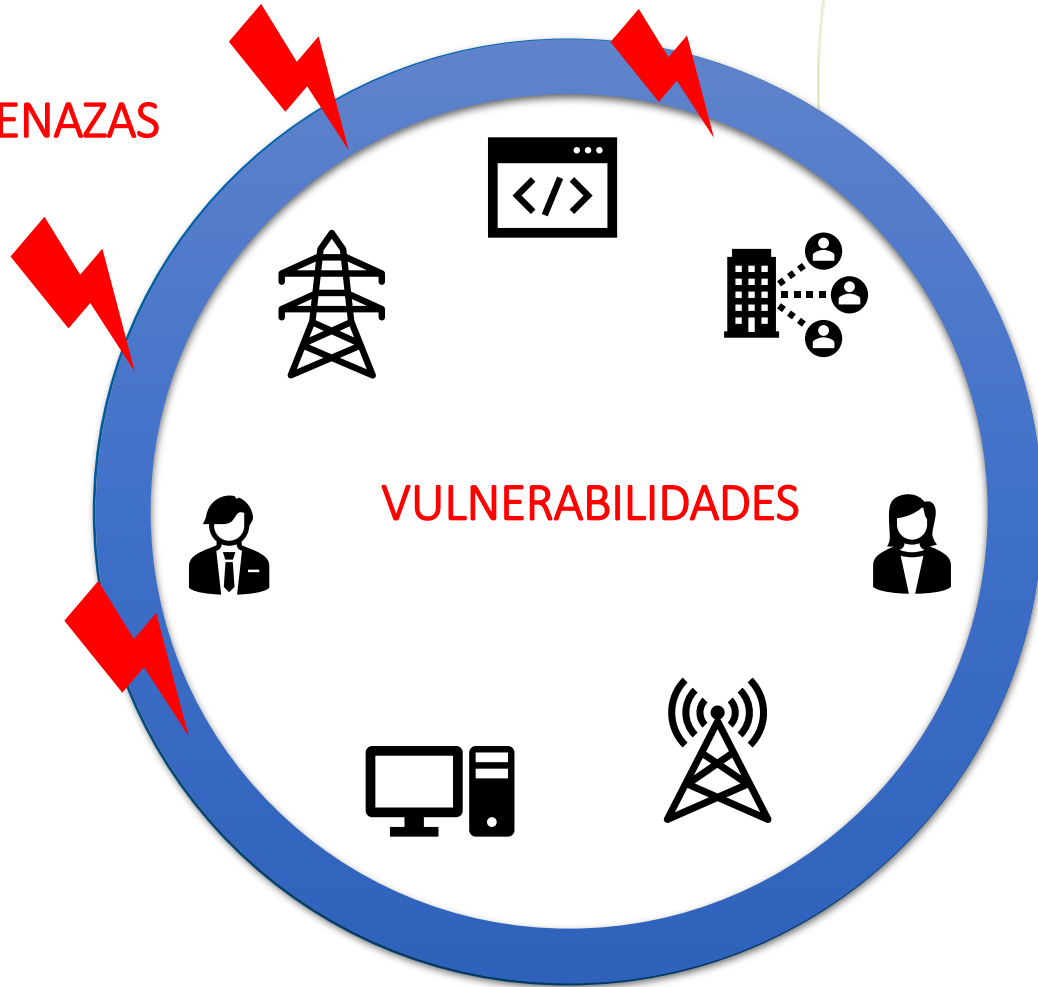








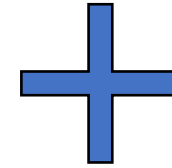
AMENAZAS



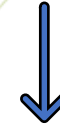
VULNERABILIDADES

SISTEMA DE TRANSMISION DE ENERGÍA

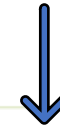
ANÁLISIS DE PROBABILIDAD



VALORACIÓN DE IMPACTO



NIVEL DE RIESGO



IMPLEMENTACIÓN DE  
CONTROLES

(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)

LISTA DE VULNERABILIDADES METODOLOGÍA Y SU RESPECTIVA CLASIFICACIÓN

| Amenaza                              | Propiedad Afectada | Vulnerabilidad                                  | Categoría 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   |
| Ciberterrorismo                      | 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     |
| Obsolescencia 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     |

# INDICADOR DE VULNERABILIDAD OPERATIVA

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

**Demanda No Atendida (DNA):**  $DNA \leq 1000MWh = 0,1 + \left(0,6 * \frac{DNA [MWh]}{1000 [MWh]}\right)$

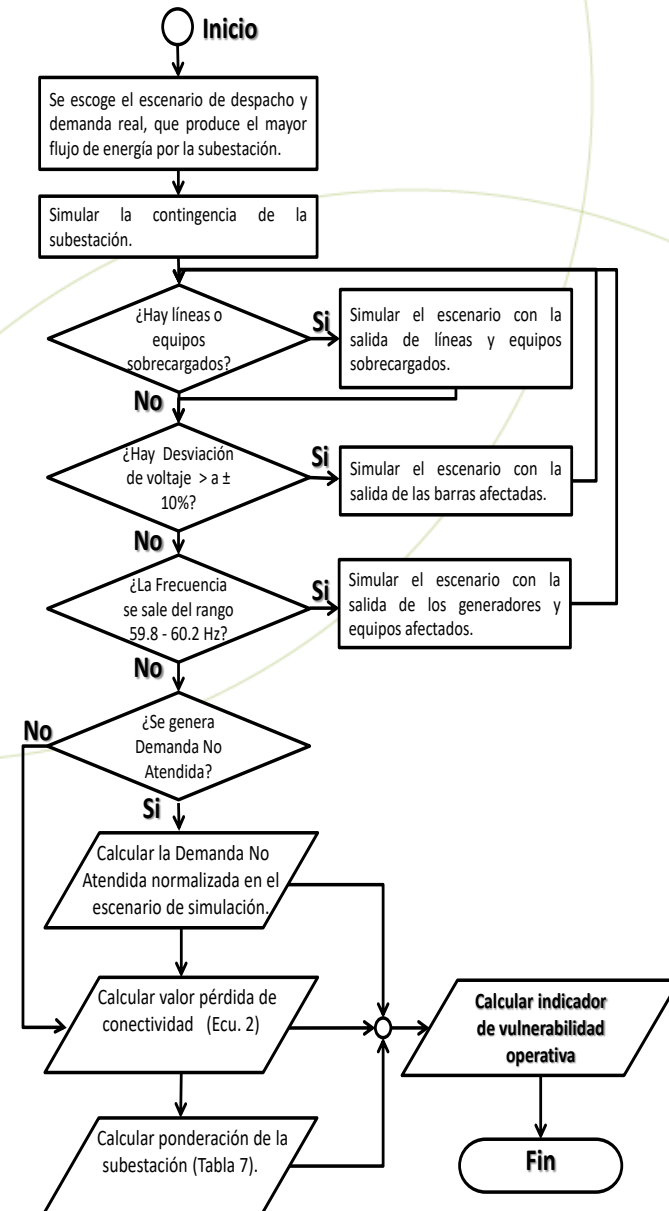
$DNA > 1000MWh = 0,7 + \left(0,3 * \frac{DNA [MWh]}{5000 [MWh]}\right)$

**Pérdida de Conectividad (PC):**  $PL = 1 - KL'/KL$  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:  $\geq 0,3$ ; Rango Medio  $0,3 > \& \leq 0,7$ ; Rango Alto  $> 0,7$



# INDICADOR DE VULNERABILIDAD DE SISTEMA

| 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.  |                 |            |             |

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

MÉTODO PARA EVALUAR LOS CONTROLES DE IDENTIFICACIÓN Y AUTENTICACIÓN

| 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. |                 |            |             |

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

MÉTODO PARA EVALUAR TIEMPOS DE RESPUESTA A EVENTOS

| 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.        |                 |            |             |

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

MÉTODO PARA EVALUAR LA INTEGRIDAD DEL SISTEMA

| 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. |                 |            |             |

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

MÉTODO PARA EVALUAR LOS CONTROLES DE USO

| 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.   |                 |            |             |

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

MÉTODO PARA EVALUAR LA CONFIDENCIALIDAD DE LOS DATOS

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

| 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 periódicamente.                    |                 |            |             |
| 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

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

| 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 críticas.   |                 |            |             |
| 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 demás. |                 |            |             |
| Se cuenta definidos los anchos de banda de acuerdo a los servicios que se utilizan.               |                 |            |             |

MÉTODO PARA EVALUAR EL FLUJO DE DATOS RESTRINGIDO

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

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

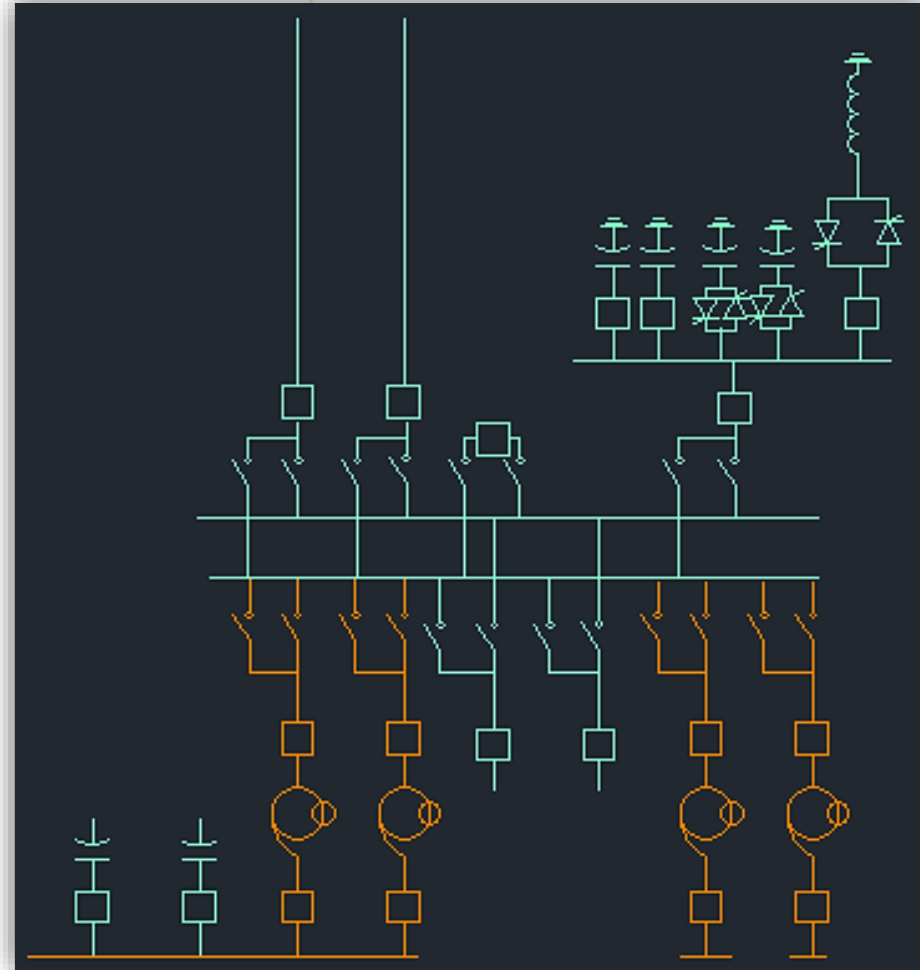


A photograph of a high-voltage electrical substation. The image shows several rows of insulators, which are tall, cylindrical structures with many horizontal ridges, mounted on metal frames. Power lines are visible, some with red and yellow-green markings. The background is a dense green forest. The text is overlaid in the center of the image.

**¿ PERO SI ES POSIBLE AFECTAR UN  
ACTIVO?**

# ESTUDIO DE CASO

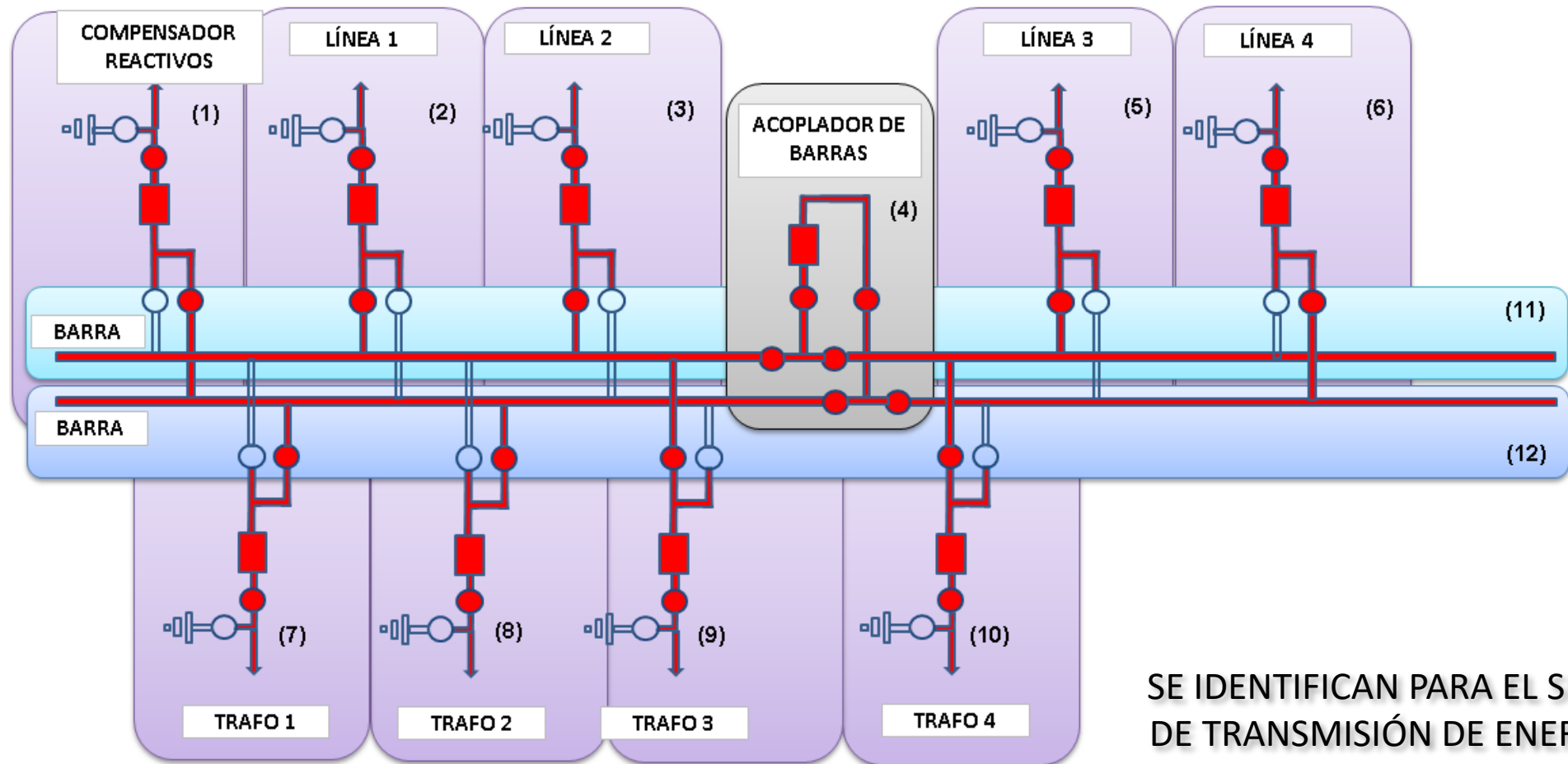
LA SUBESTACIÓN ESTA INTERCONECTADO A 230 kV





# ESTUDIO DE CASO

Identificación de activos primarios



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

# ESTUDIO DE CASO

## Escaneo de protocolos

The screenshots illustrate network traffic analysis using Wireshark. The first window shows a Transmission Control Protocol (TCP) segment with source port 102 and destination port 51830. The second window shows a Simple Network Management Protocol (SNMP) get-response packet with request-id 1565937. The third window shows a TCP segment with source port 61703 and destination port 10500.

| Protocolo de red            | Tipo   | Puerto      |
|-----------------------------|--------|-------------|
| IEC 60870-5-104             | TCP    | 2404 - 2405 |
| IEC 61850 Server            | TCP    | 102         |
| Registadores 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       |

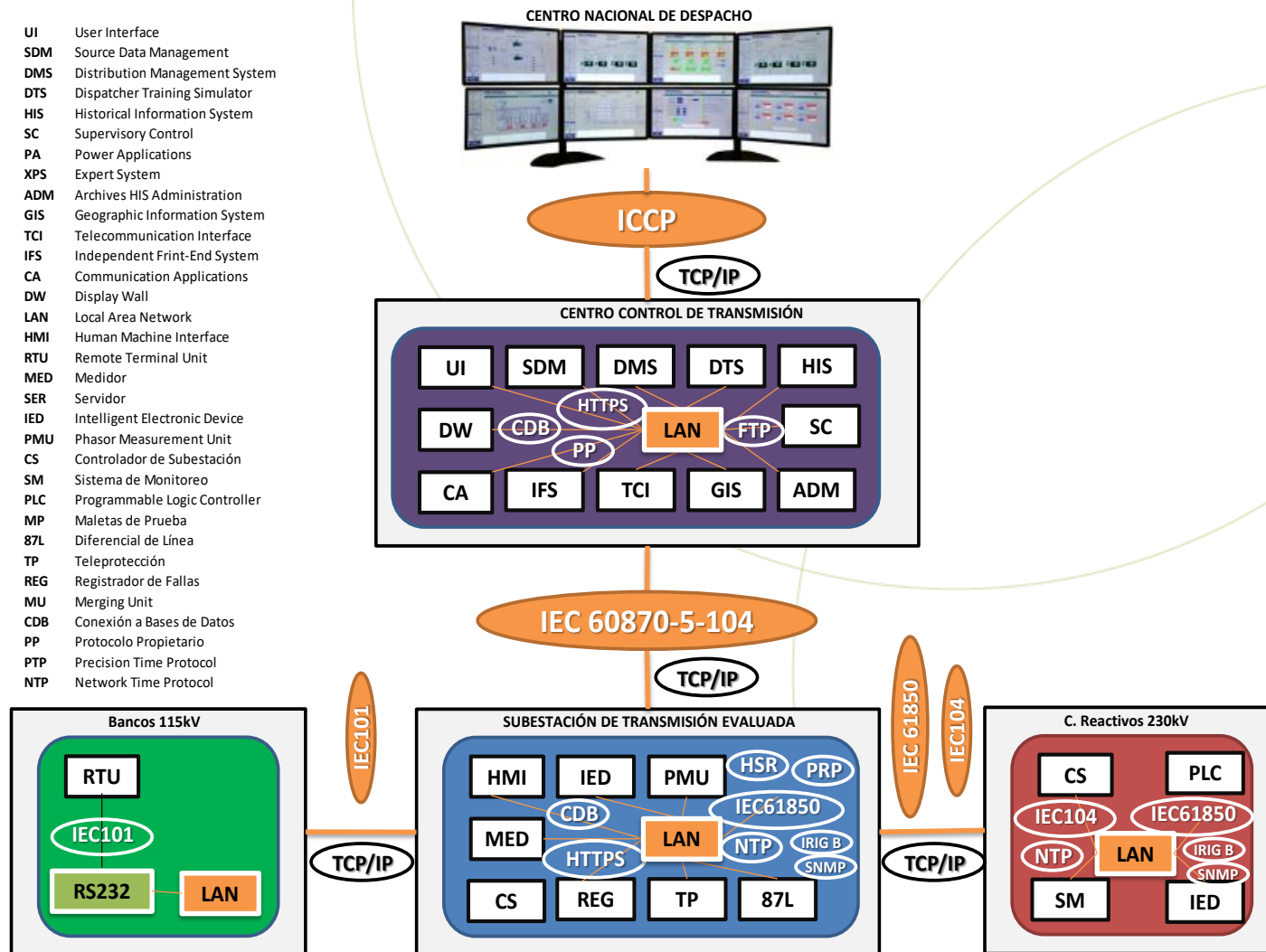


# ESTUDIO DE CASO

## 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 Front-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 Proprietario
- PTP Precision Time Protocol
- NTP Network Time Protocol



# ESTUDIO DE CASO

## Interpretación de tramas

Wireshark · Packet 55 · Mirror Puerto PAS.pcapng

- Version: 3
- Reserved: 0
- Length: 590
- ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
- ISO 8327-1 OSI Session Protocol
- ISO 8327-1 OSI Session Protocol
- ISO 8823 OSI Presentation Protocol
  - user-data: fully-encoded-data (1)
    - fully-encoded-data: 1 item
      - PDV-list
        - presentation-context-identifier: 3
        - presentation-data-values: single-ASN1-type (0)
          - Dissector is not available
            - [Expert Info (Warning/Undecoded): Dissector is not available]
            - [Dissector is not available]
            - [Severity level: Warning]
            - [Group: Undecoded]
- VSS-Monitoring ethernet trailer, Source Port: 31503
- Src Port: 31503

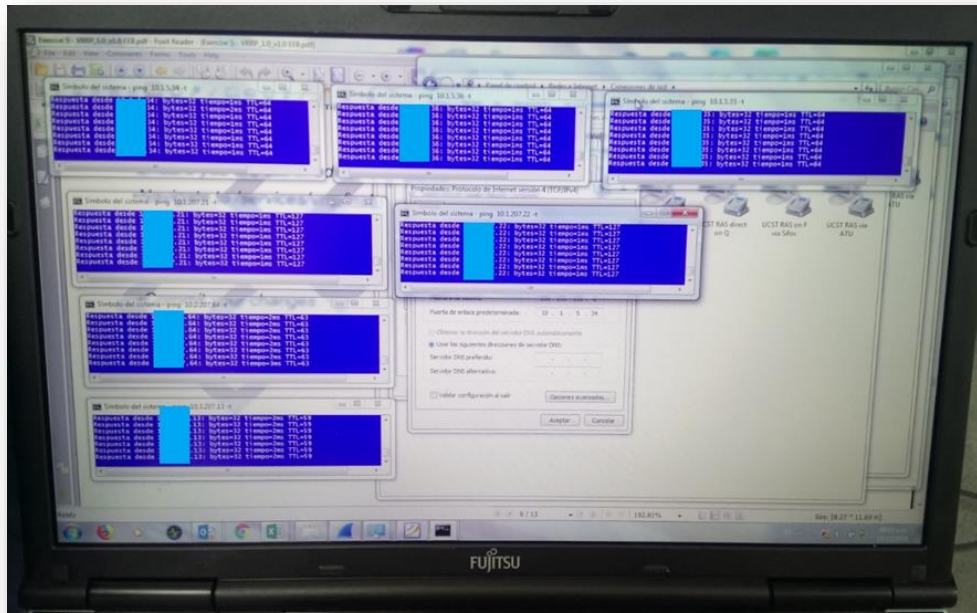
```
0110 77 53 5f 4d 65 61 73 50 6f 69 6e 74 49 33 70 68 ws_MeasP ointI3ph
0120 32 1a 20 4c 4f 4d 5f 4e 47 35 31 5f 44 30 30 31 2· LOM_N G51_D001
0130 50 6f 77 53 5f 4d 65 61 73 50 6f 69 6e 74 56 33 PowS_Mea sPointV3
0140 70 68 32 1a 10 4c 4f 4d 5f 4e 47 35 31 5f 44 30 ph2··LOM_NG51_D0
0150 30 31 52 65 63 1a 1e 4c 4f 4d 5f 4e 47 35 31 5f 01Rec··L OM_NG51
0160 44 30 30 31 52 65 63 5f 46 61 75 6c 74 52 65 63 D001Rec_ FaultRec
0170 6f 72 64 65 72 1a 10 4c 4f 4d 5f 4e 47 35 31 5f order··L OM_NG51
0180 44 30 30 31 55 44 31 1a 12 4c 4f 4d 5f 4e 47 35 D001UD1··LOM_NG5
0190 31 5f 44 30 30 31 56 49 33 70 31 1a 1e 4c 4f 4d 1_D001VI 3p1··LOM
01a0 5f 4e 47 35 31 5f 44 30 30 31 56 49 33 70 31 5f NG51_D0 01VI3p1
01b0 5f 4e 47 35 31 5f 44 30 30 31 56 49 33 70 31 5f FundSymc omp·$LOM
01c0 5f 4e 47 35 31 5f 44 30 30 31 56 49 33 70 31 5f NG51_D0 01VI3p1
01d0 4f 70 65 72 61 74 69 6f 6e 61 6c 56 61 6c 75 65 Operatio nalValue
01e0 73 1a 21 4c 4f 4d 5f 4e 47 35 31 5f 44 30 30 31 s·LOM_N G51_D001
01f0 56 49 33 70 31 5f 50 72 6f 63 65 73 73 4d 6f 6e VI3p1_Pr ocessMon
0200 69 74 6f 72 1a 12 4c 4f 4d 5f 4e 47 35 31 5f 44 itor··LO M_NG51_D
0210 30 30 31 56 49 33 70 32 1a 1e 4c 4f 4d 5f 4e 47 001VI3p2 ··LOM_NG
0220 35 31 5f 44 30 30 31 56 49 33 70 32 5f 46 75 6e 51_D001V I3p2_Fun
0230 64 53 79 6d 43 6f 6d 70 1a 24 4c 4f 4d 5f 4e 47 dSymComp ·$LOM_NG
0240 35 31 5f 44 30 30 31 56 49 33 70 32 5f 4f 70 65 51_D001V I3p2_Ope
0250 72 61 74 69 6f 6e 61 6c 56 61 6c 75 65 73 1a 21 rational Values·l
0260 4c 4f 4d 5f 4e 47 35 31 5f 44 30 30 31 56 49 33 LOM_NG51_D001VI3
```

| No. | Time                    | Direction | TI | Type    | Identifier           | Code | Cause | Of                  | Transmission                         | Originator | C-ADDR      | address | IO  | Information | Object | Addr |
|-----|-------------------------|-----------|----|---------|----------------------|------|-------|---------------------|--------------------------------------|------------|-------------|---------|-----|-------------|--------|------|
| 7   | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 1191 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 8   | 12/12/2018 17:36:53.979 |           |    | Red TCP | TI 30: Single-pointe |      |       |                     | information with time tag CPSSTime2a | 3:         | spontaneous | 0       | 107 | 11          |        |      |
| 9   | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 1862 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 10  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2004 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 11  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2059 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 12  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2064 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 13  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2127 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 14  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2132 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 15  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2481 | IV    | 17.11.18.05049 (ms) | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 16  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2522 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 17  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2710 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 18  | 12/12/2018 17:36:53.979 |           |    | COMING  | MFE                  | 2822 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 19  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2882 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 20  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2880 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 21  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2859 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 22  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2900 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 23  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2901 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 24  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2449 | OK    | 11:51.52084 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 25  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2080 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 26  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2012 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 27  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 1089 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 28  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 1019 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 29  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2026 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 30  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2024 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 31  | 12/12/2018 17:36:53.979 |           |    | Red TCP | TI 30: Single-pointe |      |       |                     | information with time tag CPSSTime2a | 3:         | spontaneous | 0       | 107 | 11          |        |      |
| 32  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2022 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 33  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2046 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 34  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2047 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 35  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2002 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 36  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2709 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 37  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2022 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 38  | 12/12/2018 17:36:53.979 |           |    | COMING  | MFE                  | 2011 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 39  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2010 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 40  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2017 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 41  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2065 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 42  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2164 | OK    | 07:29.29372 (ms)    | -                                    | 10.12.18   | (MOT) 0     | ???     |     |             |        |      |
| 43  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2164 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 44  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2117 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 45  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2113 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 46  | 12/12/2018 17:36:53.979 |           |    | Red TCP | TI 30: Single-pointe |      |       |                     | information with time tag CPSSTime2a | 3:         | spontaneous | 0       | 107 | 11          |        |      |
| 47  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2125 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 48  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2122 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |
| 49  | 12/12/2018 17:36:53.979 |           |    | GOING   | MFE                  | 2126 | OK    | 13:54.20223 (ms)    | -                                    | 11.11.18   | (MOT) 0     | ???     |     |             |        |      |



# 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
```



# ESTUDIO DE CASO

## Descubrimiento de red con ping

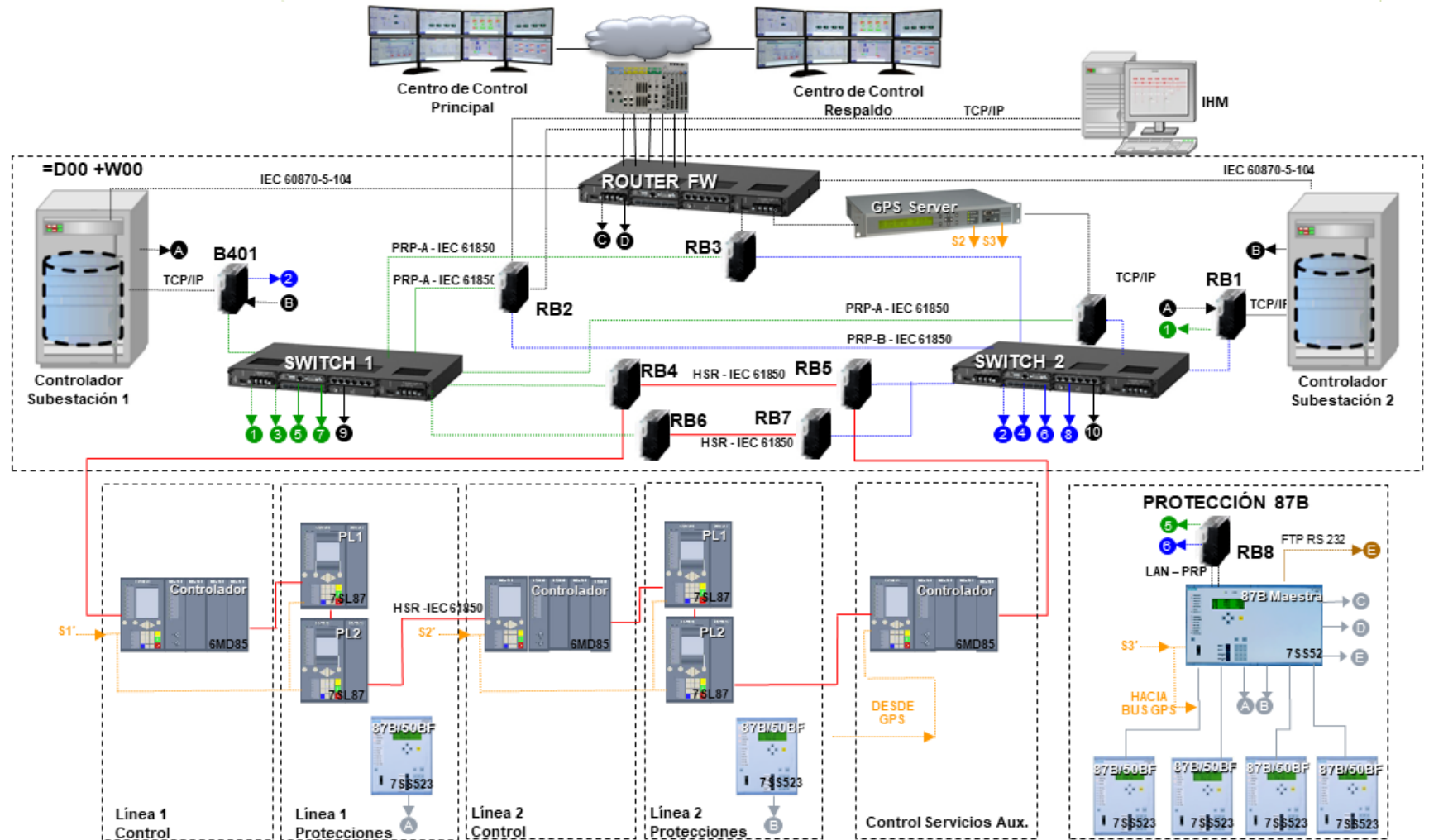
| IP IDENTIFICADA              | NOMBRE IED    | GATEWAY    | SUBRED        | TIEMPO PING | VERSION SNMP | DESCRIPCION                                      | TIPO EQUIPO                    | MAC               | LINK CANAL 1 | LINK CANAL 2 | PROTOCOLO | SERVIDOR SNTP | SERIAL       | REFERENCIA        |
|------------------------------|---------------|------------|---------------|-------------|--------------|--|--------------------------------|-------------------|--------------|--------------|-----------|---------------|--------------|-------------------|
| <a href="#">XX.X.XXX.61</a>  | 2D2_R02_F003  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.54.01.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025962 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.62</a>  | 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 |
| <a href="#">XX.X.XXX.63</a>  | 2D3_R03_F003  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025956 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.64</a>  | 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 8EFF CF 94  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.65</a>  | 2D4_R04_F003  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025963 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.66</a>  | 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 8EFF CE 2F  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.67</a>  | 2D5_R05_F003  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1512061443 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.68</a>  | 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 8EFF CE 32  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.69</a>  | 2D6_R06_F003  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025942 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.70</a>  | 2D7_R07_F003  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.54.01.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025950 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.71</a>  | 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 |
| <a href="#">XX.X.XXX.72</a>  | 2D9_R09_F003  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1510048742 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.73</a>  | 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 8EFF CF 98  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.74</a>  | 2D10_R10_F003 | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025964 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.75</a>  | 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 8EFF CE 30  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.76</a>  | 2D12_R12_F003 | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025965 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.77</a>  | 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 8EFF CE 2D  | Up           | Up           | HSR       | XX.X.XXX.161  | N/E          | N/E               |
| <a href="#">XX.X.XXX.121</a> | 2D2_w02_D001  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025966 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.122</a> | 2D3_w03_D001  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410061244 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.123</a> | 2D4_w04_D001  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410061221 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.124</a> | 2D5_w05_D001  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410061235 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.125</a> | 2D6_w06_D001  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410039613 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.126</a> | 2D7_w07_D001  | XX.X.XXX.1 | 255.255.255.0 | 2 ms        | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410061223 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.127</a> | 2D9_w09_D001  | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410061228 | C53207A 602B110 1 |
| <a href="#">XX.X.XXX.128</a> | 2D10_w10_D001 | XX.X.XXX.1 | 255.255.255.0 | 1ms         | V3           | SIPROTEC5 ETH-BB-2FO Firmware (FW) V07.31.03.995 | sip5com                        | 00 00 7A CC 00 14 | Up           | Up           | HSR       | XX.X.XXX.161  | BF1410025930 | C53207A 602B110 1 |



# 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



# 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
```

# 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
```

```
Administrador: C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Administrador>net user
Cuentas de usuario de \KPF04

Administrador      Ingeniero      Invitado
-----
scadmin
Se ha completado el comando correctamente.

C:\Users\Administrador>
```





# ESTUDIO DE CASO

## Descubrimiento de configuración de Router/Firewall

**SIEMENS RUGGEDCOM ROX II**

Configure Running | Tools | Logout from rxunal

View | Edit Private | Edit Exclusive

File Explorer: admin, chassis, global, interface, interfaces, switch, tunnel, ip, dummy0, fe-cm-1, switch.0, switch.0, switch.0, switch.0, switch.1, ipv4, ipv6, .3/24

Address: /ip[switch.1931]ipv4/address

Addresses

| IP Address | Peer      |
|------------|-----------|
| .3/24      | not found |

Main Policy Settings

| Policy Name | Policy | Log Level | Description |
|-------------|--------|-----------|-------------|
| Fw2Any      | accept | none      | not found   |
| Ingn2Any    | accept | none      | not found   |
| Scada2CCT   | accept | none      | not found   |
| CCT2Scada   | accept | none      | not found   |
| CYP2Gstn    | accept | none      | not found   |
| CYP2Fw      | accept | none      | not found   |
| Any2Any     | reject | none      | not found   |

File Explorer: tunnel, ip, qos, mpls, routing, security, services, apps, dynamic, static, status, multicast, ipv4routes, ipv6routes, multicast, memory, rip, ospf, bgp, pim-sm

Address: /routing/status/ipv4routes/active-routes

IPv4 Kernel Active Routing Table

| Subnet  | Gateway Address | Interface Name | Route Type | Route Weight | Metric |
|---------|-----------------|----------------|------------|--------------|--------|
| 0/24    |                 | switch.00      | kernel     |              |        |
| 1.0/24  | .20             | switch.00      | zebra      |              |        |
| 1.0/24  | .30             | switch.00      | zebra      |              |        |
| .0/24   |                 | switch.01      | kernel     |              |        |
| .0/24   |                 | switch.04      | kernel     |              |        |
| .0/24   |                 | switch.07      | kernel     |              |        |
| 1.0/24  |                 | switch.19      | kernel     |              |        |
| 10.0/24 | .88             | switch.19      | zebra      |              |        |

| 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              |

# 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]# █
```

# ESTUDIO DE CASO

## Vulnerabilidades de sistemas operativos

**Vulnerabilities** 39

Filter Search Vulnerabilities 39 Vulnerabilities

| Sev                               | Name  | Family  | Count |
|-----------------------------------|---|---------|-------|
| <input type="checkbox"/> CRITICAL | Microsoft Windows SMBv1 Multiple Vulnerabilities      | Windows | 1     |
| <input type="checkbox"/> CRITICAL | MS17-010: Security Update for Microsoft Windows SM... | Windows | 1     |
| <input type="checkbox"/> MEDIUM   | Microsoft Windows Remote Desktop Protocol Server ...  | Windows | 1     |

**Host Details**

IP: [REDACTED]  
MAC: [REDACTED]  
OS: Microsoft Windows 7 Professional  
Start: November 28 at 10:25 PM  
End: November 28 at 10:50 PM  
Elapsed: 26 minutes  
KB: [Download](#)



# ESTUDIO DE CASO

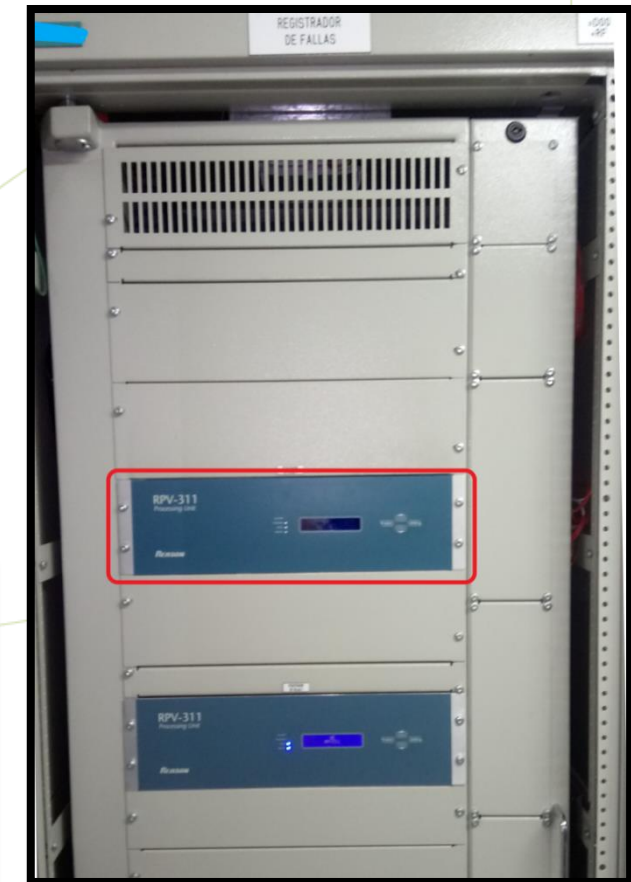
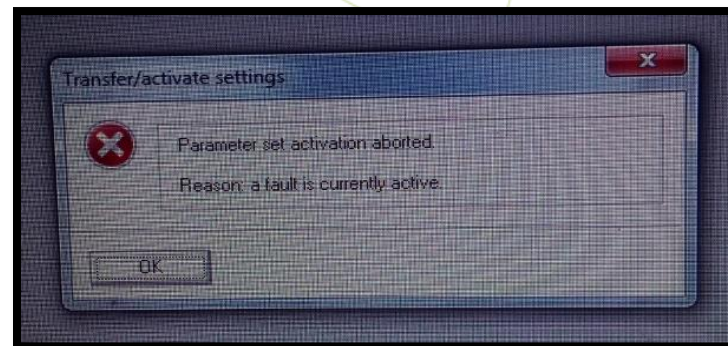
## Vulnerabilidades de dispositivos OT instalados

### 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.



# ESTUDIO DE CASO

## Vulnerabilidades de dispositivos OT instalados

The image displays two screenshots of a SCADA software interface. The top screenshot shows a tree view of devices on the left and a table of variables on the right. The bottom screenshot shows a similar view but with a detailed table of variables selected.

| Name | Type(Len[arr]) | Value                                    | Write                    |
|------|----------------|--|--------------------------|
| Name |                | LLN0SBufferList_N207GW1_3                | <input type="checkbox"/> |
| Type |                | Variable List                            | <input type="checkbox"/> |
| Path |                | LOM_B1_D000AIn/LLN0SBufferList_N207GW1_3 | <input type="checkbox"/> |

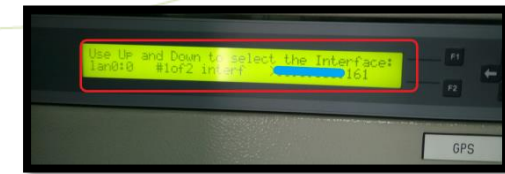
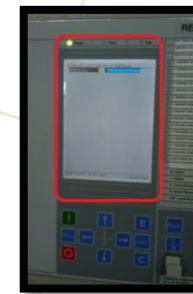
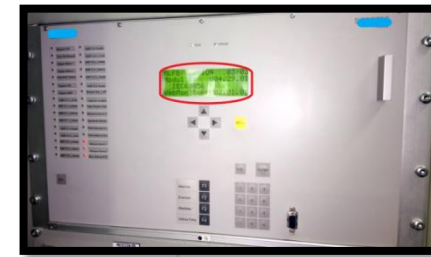
| Name                | Type(Len[arr])   | Value                                      | Write                    |
|---------------------|------------------|--|--------------------------|
| Name                |                  | SetOpCnt                                   | <input type="checkbox"/> |
| Type                |                  | Data Object                                | <input type="checkbox"/> |
| Path                |                  | LOM_B1_D000QB1/XSW119COISetOpCnt           | <input type="checkbox"/> |
| OperSetVal          | Integer (44)     | 0  | <input type="checkbox"/> |
| OperSorigInSorCat   | Integer (11)     | 0  | <input type="checkbox"/> |
| OperSorigInSorIdent | OctetStr (66-64) |  | <input type="checkbox"/> |
| OperSetNum          | UInteger (11)    | 0  | <input type="checkbox"/> |
| OperST              | UTC_Time (128)   | (L-0-F-0-N-0.0b)01.01.1970.00.00.00.000000 | <input type="checkbox"/> |
| OperSTest           | Bool (11)        | (false) 0                                  | <input type="checkbox"/> |
| Oper\$Check         | BitString (31-2) | 00   | <input type="checkbox"/> |





# ESTUDIO DE CASO

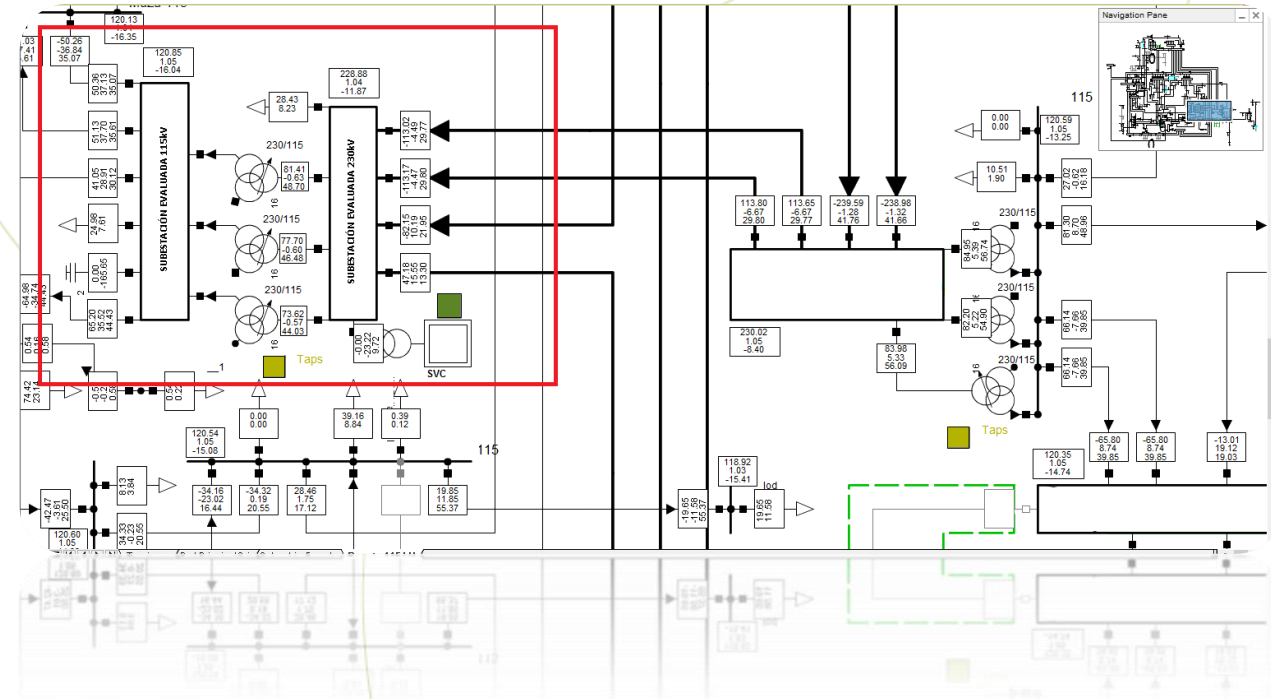
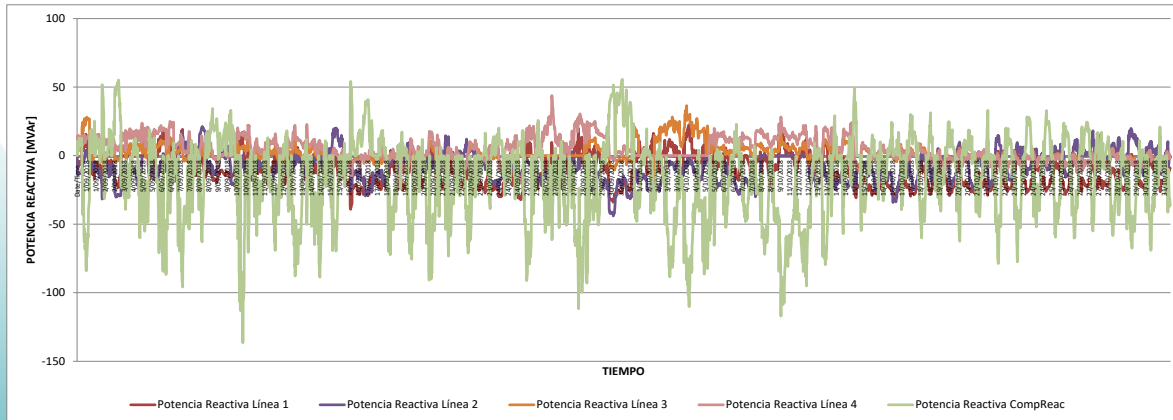
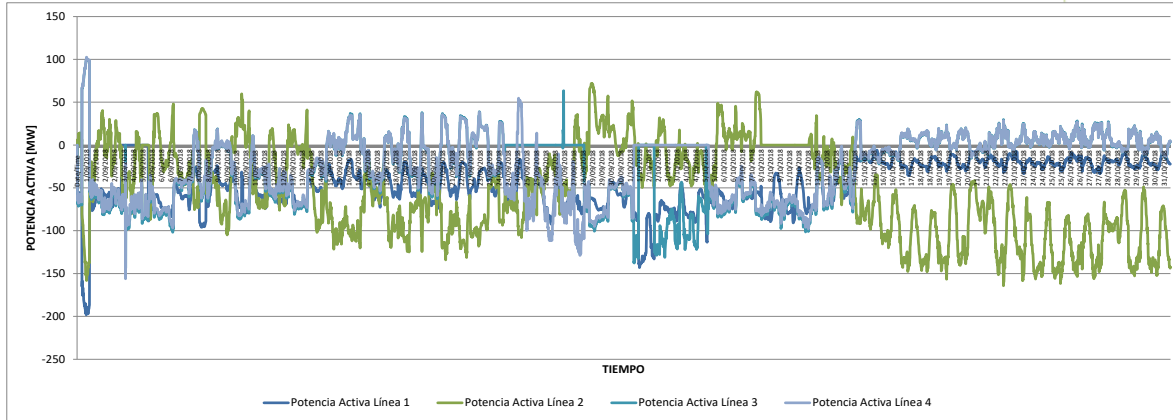
Vulnerabilidades de dispositivos OT instalados





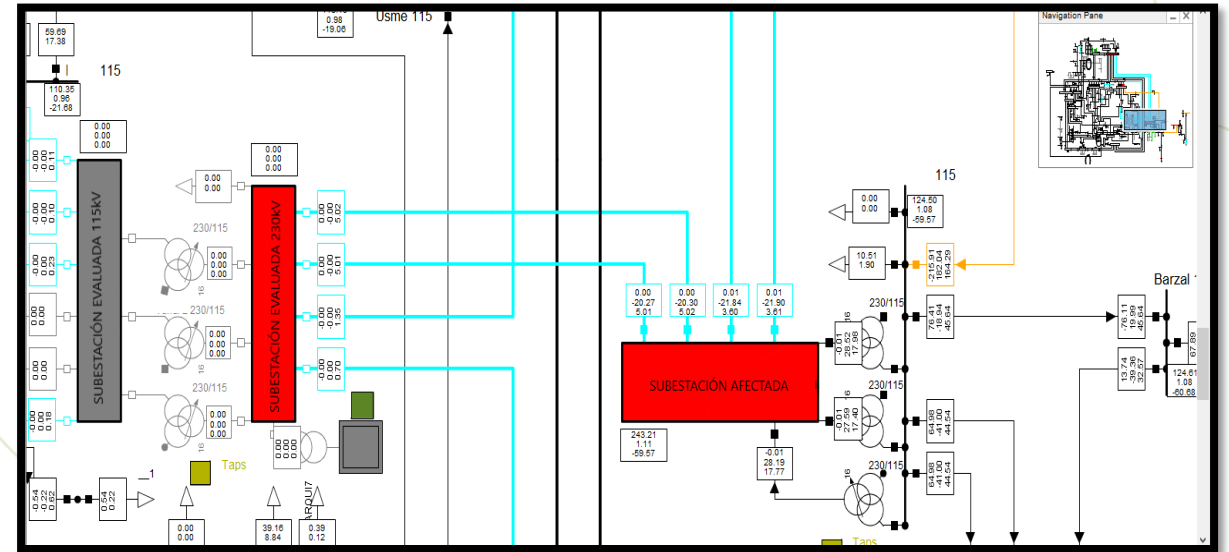
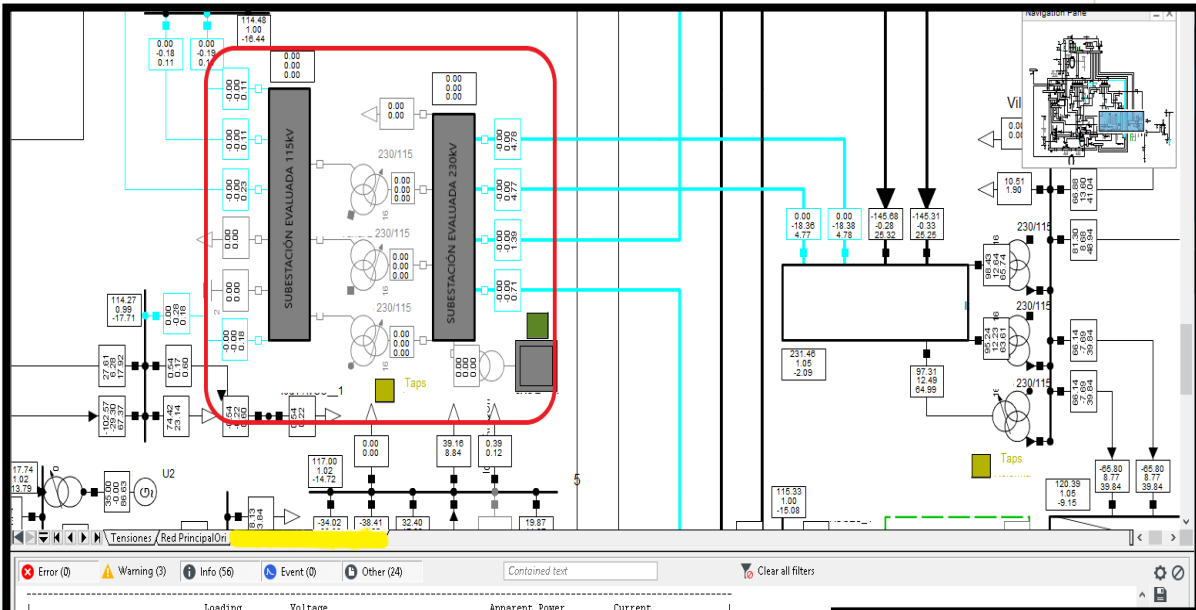
# ESTUDIO DE CASO

## Cálculo del IVO

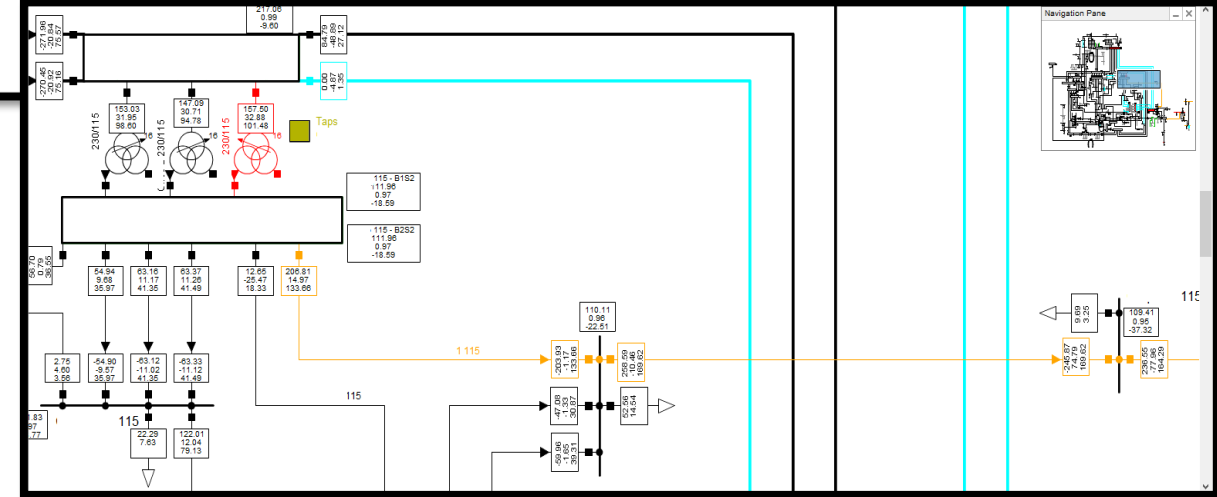


# ESTUDIO DE CASO

## Cálculo del IVO



| Name                       | Type  | Loading [%] | Voltage [p.u.] | Voltage [kV] | Station/Branch | Apparent Power [MVA] | Current [kA] |
|----------------------------|-------|-------------|----------------|--------------|----------------|----------------------|--------------|
| <b>Overloaded Elements</b> |       |             |                |              |                |                      |              |
|                            | Terza | 1.15        | 32.08          | 32.08        | Bogota         |                      |              |
|                            | Terza | 1.15        | 32.08          | 32.08        | Bogota         |                      |              |



# ESTUDIO DE CASO

## Cálculo del IVO

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

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

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

$$DNA_n = 0,41$$

$$PC = 1 - 51/64$$

$$PC = 0,20$$

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

$$PS = 4700$$

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

$$PS_n = 0,84$$

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

$$IVO = 0,42$$

# ESTUDIO DE CASO

## Cálculo del IVS

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

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

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

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

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

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

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

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

$$IVS = 0,637$$



# 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.

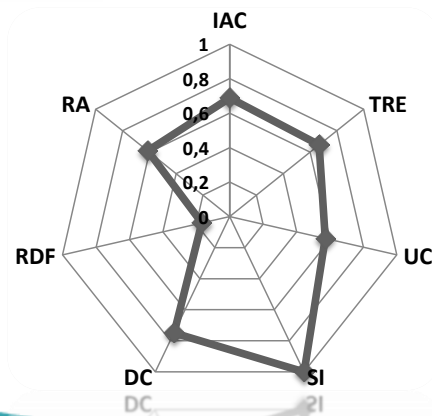
$IVO = 0,420 \Rightarrow 42,0\%$

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

Rango Medio  $0,3 > \& \leq 0,7$

IVS

Puntos críticos de vulnerabilidades



**¡MUCHAS  
GRACIAS!**



**Grupo  
Energía  
Bogotá**

*Mejoramos vidas  
con energía  
sostenible y  
competitiva*

[jcarreno@geb.com.co](mailto:jcarreno@geb.com.co)

[jccarrenop@correo.udistrital.edu.co](mailto:jccarrenop@correo.udistrital.edu.co)

<https://www.linkedin.com/in/juan-carlos-carreño-perez-891262132>



# Grupo Energía Bogotá



---

Para uso restringido GRUPO ENERGÍA BOGOTÁ S.A. ESP. y sus filiales  
Todos los derechos reservados. Ninguna parte de esta presentación  
puede ser reproducida o utilizada en ninguna forma o por ningún medio  
sin permiso explícito de GRUPO ENERGÍA BOGOTÁ S.A. ESP. o sus  
filiales como propietarias de la información.