Metodología para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano

Sigifredo Hernández Hernández

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2019

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DE CIBERSEGURIDAD PARA LOS CONCENTRADORES QUE SOPORTAN LA INFRAESTRUCTURA DE MEDICIÓN AVANZADA EN EL SECTOR ELÉCTRICO COLOMBIANO

ALUMNO:

SIGIFREDO HERNÁNDEZ HERNÁNDEZ

DIRECTOR:

RAFAEL V. PÁEZ MÉNDEZ PHD

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO

BOGOTA – COLOMBIA

2019

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

METODOLOGÍA PARA EL ANÁLISIS Y EVALUACIÓN DE CIBERSEGURIDAD PARA LOS CONCENTRADORES QUE SOPORTAN LA INFRAESTRUCTURA DE MEDICIÓN AVANZADA EN EL SECTOR ELÉCTRICO COLOMBIANO

ALUMNO: SIGIFREDO HERNÁNDEZ HERNÁNDEZ

DIRECTOR: RAFAEL V. PÁEZ MÉNDEZ PHD

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

2019

TABLA DE CONTENIDO

Resumen

Las redes inteligentes surgen como respuesta a la obsolescencia de los sistemas e infraestructuras de la red eléctrica, el aumento de las energías renovables, la integración del vehículo eléctrico en la red y la necesidad de mejorar la seguridad del suministro eléctrico y la eficiencia del sistema.

La Infraestructura de Medición Avanzada (AMI) (por sus iniciales en inglés) en el servicio público de energía eléctrica, AMI se define como la infraestructura que permite la comunicación bidireccional con los usuarios del servicio de energía eléctrica. Esta infraestructura integra hardware (medidores avanzados, centros de gestión de medida, enrutadores, concentradores, antenas, entre otros), software y arquitecturas y redes de comunicaciones, que permiten la operación de la infraestructura y la gestión de los datos del sistema de distribución de energía eléctrica y de los sistemas de medida. (MINMINAS, 2018, pág. 4)

En un mundo globalizado e interconectado del cual forman parte las redes eléctricas inteligentes un ataque podría originarse desde cualquier lugar, en cualquier momento, pasando desapercibido por días o meses, teniendo un alto grado de dificultad detectarlo y responder al ataque de forma oportuna y efectiva.

Comprometer el canal de precios o lectura de medidas de contadores, en tiempo real, puede resultar en el robo de energía o el control remoto malicioso de electrodomésticos. Por lo tanto, se requiere una seguridad rigurosa del hardware / software para garantizar la validez de las diferentes partes de la comunicación tales como concentradores de cabecera y los contadores inteligentes. Si un atacante se apodera del concentrador de cabecera, entonces podría ser capaz de enviar un

comando de interrupción de suministro a los contadores inteligentes con respuesta a la demanda. La interrupción puede hacerse permanente si se ordena a todos los contadores que cambien sus claves criptográficas a algún nuevo valor que solo conoce al atacante. El impacto podría ser enorme, millones de hogares se quedarían sin energía hasta que los contadores fuesen sustituidos o se repusiesen las claves auténticas. Como consecuencia de ello, la seguridad podría verse en peligro a nivel local, y las empresas podrían perder millones. La ciberseguridad en las redes inteligentes necesita prevenir este tipo de ataques y tener un mecanismo de recuperación / capacidad de supervivencia en caso de ataques (con éxito). (UPME Parte 4, 2016, pág. 3)

Por lo anterior, el trabajo de grado propuesto pretende establecer una metodología para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano, mediante el análisis documental de distintas fuentes y documentos entre ellos el marco de trabajo de seguridad de NIST, normas y estándares como NERC CIP, ISO 27019, IEC 62351, IEC 62443 y NTC 6079.

La metodología propuesta pretende resolver el "COMO", debido a que Las normas o estándares internacionales de ciberseguridad ayudan a las empresas del sector eléctrico con buenas prácticas sobre implementación de programas y políticas de protección de infraestructura crítica, pero no plantean o definen una metodología para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano.

Palabras clave: AMI, Concentrador, Ciberseguridad, Marco de trabajo, Metodología.

Abstract

Smart Grids arise in response to the obsolescence of the systems and infrastructures of the electric network, the increase of renewable energies, the integration of electric vehicles in the network and the need to improve the security of electricity supply and the efficiency of the system.

The Advanced Metering Infrastructure (AMI) in the public electric power service, AMI is defined as the infrastructure that allows two-way communication with users of the electric power service. This infrastructure integrates hardware (advanced meters, measurement management centers, routers, concentrators, antennas, among others), software and architectures and communication networks, which allow the operation of the infrastructure and the data management of the distribution system. electrical energy and measuring systems. (MINMINAS, 2018, pág. 4)

In a globalized and interconnected world of which intelligent electrical networks are part, an attack could originate from anywhere, at any moment, going unnoticed for days or months, having a high degree of difficulty detecting it and responding to the attack in a timely and effective manner.

Committing the price channel or reading meter measurements, in real time, can result in power theft or malicious remote control of appliances. Therefore, a rigorous hardware / software security is required to guarantee the validity of the different parts of the communication such as headend concentrators and smart meters. If an attacker seizes the headend concentrator, then it might be able to send a supply interrupt command to the smart meters responding to demand. The

interruption can be made permanent if all the Smart Meters are ordered to change their cryptographic keys to a new value that only the attacker knows. The impact could be enormous, millions of homes would run out of energy until the meters were replaced or the authentic keys were replaced. As a consequence, security could be endangered locally, and companies could lose millions. Cybersecurity in smart grids needs to prevent this kind of attacks and have a recovery mechanism / survivability in case of attacks (with success). (UPME Parte 4, 2016, pág. 3)

Due to the above, the proposed degree work aims to establish a methodology for the analysis and evaluation of cybersecurity for the concentrators that support the Advanced Measurement infrastructure in the Colombian Electricity Sector, through the documentary analysis of different sources and documents, including the framework of NIST safety work, standards and standards such as NERC CIP, ISO 27019, IEC 62351, IEC 62443 and NTC 6079.

The proposed methodology aims to resolve the "HOW", because international cybersecurity standards or standards help companies in the electricity sector with good practices on implementing critical infrastructure protection programs and policies, but do not propose or define a methodology for the analysis and evaluation of cybersecurity for the concentrators that support the Advanced Measurement infrastructure in the Colombian Electric Sector.

Keywords: AMI, Concentrator, Cybersecurity, Framework, Methodology.

Lista de acrónimos

AMI	Infraestructura de Medición Avanzada (***A**dvance **M**etering Infrastucture*)
CIP	Protección de infraestructura Crítica (***C**ritical Infrastructure protection*)
CNO	Consejo Nacional de Operación del sector eléctrico Colombiano
ISA	Sociedad Internacional de Automatización (*International Society of Automation*)
ISO	Organización Internacional para Estandarizaciones (*International Organization for Standardization*)
NERC	Corporación Norteamericana de Confiabilidad Eléctrica (*North American Electric Reliability Corporation*)
NIST	Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*)
MDC	Sistema de Recolección de la Medición (*Meter Data Collector*)
MDM	Sistema de Gestión de la Medición (*Meter data management*)
WAN	Red de Área Amplia (*Wide Area Network*)

Glosario de términos

Activo Crítico: Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecta la confiabilidad y operatividad del sistema eléctrico.

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema. Esto incluye tanto daños a equipamiento a nivel físico como a su funcionalidad e información.

AMI (*Advanced Metering Infrastructure*): Son sistemas que miden, recopilan y analizan el uso de energía y se comunican con dispositivos de medición tales como contadores de electricidad, ya sea a solicitud o en un horario. Estos sistemas incluyen hardware, software, comunicaciones, pantallas de consumo de la energía, sistemas de los clientes asociados y sistemas de gestión de datos de medición (MDM) de software.

Ciberactivos: Dispositivos electrónicos programables y elementos de las redes de comunicaciones incluyendo hardware, software y datos. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso del mismo de forma local o remota.

Ciberactivo Crítico: Ciberactivo esencial para la operación confiable de activos críticos.

Ciberseguridad: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

Malware: Programas maliciosos con el propósito de denegación de servicios, espionaje, inclusión de una puerta trasera y sabotaje de personas o compañías.

Medidor inteligente: Un medidor inteligente es un dispositivo digital que consta de un componente de medición de estado sólido para la recolección de datos en tiempo real, un microprocesador, una memoria local para almacenar las mediciones y al menos una interfaz de red para comunicarse con el MDC.

MDC (Meter Data Collector): Elemento de un sistema AMI el cual recolecta la información de los medidores. La comunicación con los medidores es de forma bidireccional.

MDM (Meter data Management): Es uno de los componentes claves de una infraestructura de red inteligente o Smart Grid que realiza el almacenamiento a largo plazo de datos y la gestión de grandes cantidades de datos entregados por los equipos de medición inteligente (Smart Meter).

NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection): Requisitos para la protección de infraestructuras críticas hechas por la NERC, donde las empresas de servicios públicos en América del Norte deben cumplir, aplica a generación, centrales eléctricas, subestaciones de transmisión (típicamente de 100 kV o más).

PLC (Programmable Logic Controller): Son dispositivos diseñados específicamente para el control industrial. El ámbito de aplicación del PLC suele ser en el control de un único proceso o máquina, no interrelacionados directamente con otro proceso o máquina vecinos.

SCADA (Supervisory Control and Data Acquisition): Conjunto de redes, equipos y programas que monitorizan en tiempo real procedimientos industriales y tareas complejas, a partir de la información obtenida a través de sensores, comunicándose con los dispositivos

actuadores para transmitirles las órdenes adecuadas y pudiendo controlar el proceso de forma automática mediante un software especializado.

Smart Grid: Una red inteligente es aquella que incorpora información y las comunicaciones en todos los aspectos de la generación, suministro y consumo de electricidad, con el fin de minimizar el impacto ambiental, ampliar los mercados, incrementar la confiabilidad, reducir los costos y mejorar la eficiencia.

Telecontrol: Para la operación de la red eléctrica, las empresas de energía cuentan con activos eléctricos (generalmente IED) capaces de enviar indicaciones a distancia mediante un enlace de transmisión de datos bidireccional (en este caso llamado enlace de Telecontrol) y envía órdenes para controlar su sistema eléctrico. El telecontrol se lleva a cabo en tiempo real.

Telemedida: Como parte del proceso de energía se encuentra la lectura automática de medida, cuya tecnología permite obtener la información de consumo de cualquier medidor y transferir esta información al centro de gestión de la medida de manera remota y automática, para el control de sus procesos.

Teleprotección: Los sistemas eléctricos de potencia poseen equipos encargados de evitar daños en los diversos elementos del sistema y preservar su estabilidad. Las teleprotecciones consiguen desconectar ante una falla eléctrica la parte afectada mediante la transmisión de señales en el menor tiempo posible, a través de un enlace de teleprotección.

Vulnerabilidad: Se refiere a una debilidad en un sistema que puede ser utilizado por un atacante para dañar un sistema, obtener acceso no autorizado o ejecutar código arbitrario.

Índice de figuras

Motivación y antecedentes

En esta sección se describe el contexto, los antecedentes y justificación del proyecto de grado.

Contexto

La décimo tercera edición del reporte global de riesgos ubica el riesgo de ciberseguridad en segundo lugar después de los riesgos por causas naturales (GRP, 2018, pág. 3)

La Organización de los Estados Americanos (OEA) en conjunto con Microsoft, destaca en el reporte de protección de infraestructura crítica en América y el Caribe lo siguiente: (Microsoft-OEA, 2018, págs. 25-26).

- Con base en los resultados del estudio, el 53% de las organizaciones que respondieron Indicaron que tenían la capacidad de detectar y registrar incidentes cibernéticos. Además, el 73% indicó que había detectado un ciberataque en los últimos 12 meses.
- El 48% de los encuestados indicaron que tenían capacitación en concienciación sobre seguridad cibernética para empleados, el 46% indicó que tenía un plan de recuperación ante desastres, El 42% indicó que tenía un plan de respuesta a incidentes cibernéticos, el 41% indicó que tenía una estrategia de ciberseguridad documentada.

- En términos de medidas de ciberseguridad empleadas por su organización, el 82% respondió "Firewall" y "Internet Gateways", el 68% indicó "control de acceso", el 61% declaró "protección de malware", 55% "auditorías" y 50% declaró "respaldo automatizado". En lo que respecta a la gestión de riesgos, 55% de Los que respondieron a esa pregunta indicaron que su organización implementó prácticas de gestión de riesgos de ciberseguridad y el 49% de los encuestados indicaron que tenían previsto realizar una evaluación de riesgos. Además, el 62% de los encuestados indicó que hay un rol dedicado dentro de sus organizaciones un responsable de la ciberseguridad.
- 57% de los que respondieron indicaron que no tenían un presupuesto específico para medidas de ciberseguridad.
- El 69% de los encuestados indicaron haber notado un aumento en el número de ataques a sus sistemas informáticos y / o redes en los últimos 12 meses. Además, en términos de los activos que han sido objeto de los ciberataques en los últimos 12 meses, el 61% de los encuestados identificaron "datos", 58% "perímetro de la red de la empresa", 18% "sistemas de personal" y el 13% indicó "propiedad intelectual". En relación con los métodos de ataque específicos, el 76% de ellos quienes respondieron indicaron "phishing", seguido por un 71% que identifica "malware" (por ejemplo, virus, gusanos, troyanos). Otras actividades identificadas incluyeron el rastreo de puertos (sin intrusión real) y la ingeniería social. Curiosamente, algunos ataques de ransomware y de denegación de servicio (distribuidos) identificados, que cuando se trata de infraestructura crítica son

amenazas críticas a tener en cuenta en la gestión de riesgos y respuesta a incidentes.

El Centro de Ciberseguridad Industrial destaca en el Estudio sobre la Ciberseguridad Industrial en Colombia, lo siguiente: (CCI, 2018, págs. 11-14-16-19-20)

- En lo que a unidades organizacionales responsables se refiere, gran parte de las entidades encuestadas (55,2%) asigna dicha tarea al área de seguridad de la información y/o seguridad lógica, enfocando estas acciones desde un punto de vista más cibernético que físico o asociado a procesos.
- En segundo lugar, aunque muy de cerca, en torno a un 48% de las respuestas obtenidas asignan dicha responsabilidad, a las áreas de Tecnologías de la Información corporativa (TI) y un significativo 31%, al CISO-Oficial de Seguridad Informática.
- Los empleados en las áreas de OT poseen un nivel bajo (28%) o normal (41%) de capacitación, y solo un 17% de los gestores considera que su equipo de automatización esté adecuadamente formado. Incluso un 7% considera que hay una falta total de capacitación en dicho equipo.
- Entre el conjunto de las evaluaciones realizadas, destaca con un 55% lo referente a la capacidad organizativa, que incluye, entre otras variables, las políticas y procedimientos establecidos. Un casi 45% de los encuestados declara haber llevado a cabo otros dos tipos de evaluaciones: técnicas sobre las redes, como análisis de vulnerabilidad, de segmentación y test de intrusión; y normativas, al

amparo de distintas normas y estándares como NERC-CIP, IEC62443, el SGCI de CCI (https://www.cci-es.org/sgci), entre otras.

- El 18% de las empresas estudiadas afirma tener un proceso de Gestión de Incidencias de Ciberseguridad Industrial desarrollado y en aplicación. En el 6,9% de las empresas este proceso no existe, y el 17,2% actúa de forma reactiva cuando ocurren incidencias de Seguridad. Por otro lado, el 28% de las empresas estudiadas afirma estar definiendo este proceso, el cual es necesario como se evidenció en los eventos de alto impacto global ocurridos en el 2017, como Wanacry y Petya, y en los sectores industriales afectados por los eventos como los apagones en Ucrania.
- Más de la cuarta parte (31%) de las empresas industriales estudiadas afirman que existe una separación total entre sus redes, la corporativa y la industrial. La mayoría de las empresas estudiadas (35%) afirma tener dispositivos que están conectados a Internet de forma permanente. Desciende al 25% aquellos cuya conexión a internet es solo activada bajo demanda, y el mismo número 25%, el de los que manifiestan no tener ningún tipo de dispositivo en red abierta.
- El porcentaje más significativo de las empresas que reconocen tener establecida conexión entre la red corporativa y la de automatización están segmentadas por un firewall (55%) o bien cuentan con distintos niveles de segmentación con varios dispositivos de filtrado (31%). Sin embargo, existe un muy preocupante 10% de empresas que mantiene sus redes directamente conectadas, lo que representa un enorme riesgo de incidencias de seguridad.

- La gran mayoría de las empresas industriales estudiadas afirma que dispone de accesos remotos (75,8%). De todas ellas, el 24,1% tiene el acceso remoto permanentemente disponible para la conexión, mientras que en el 51,7% de estas empresas, los dispositivos de comunicación se conectan a demanda.
- La familia ISO 27001 lidera de lejos las preferencias de los entrevistados (71%). Son muy pocas las organizaciones industriales colombianas que no utilizan ninguna norma para implementar la Ciberseguridad Industrial (4,1%). Es muy destacable también que el 20% de las organizaciones encuestadas utilizan el estándar internacional IEC 62443 de seguridad en la automatización y control industrial.
- También encuentran fuerte cabida en el gráfico la aplicación de la Ley de Protección de Datos Personales (67%), y la futura y próxima Ley de Protección de Infraestructuras Críticas (33%).
- Casi todas las empresas estudiadas afirman tener implantado algún tipo de medida de Ciberseguridad Industrial. De las medidas técnicas, las más habituales (por orden de mayor a menor influencia) son las soluciones automatizadas de respaldo: backups o copias de seguridad, los antivirus, los firewalls convencionales y el cifrado de las comunicaciones.
- También ocupan un lugar importante los IDS/IPS, la definición de políticas y procedimientos, la gestión de respuesta a incidentes, y la realización periódica de auditorías de seguridad internas.

Antecedentes

Las aplicaciones de redes inteligentes necesitan información sobre el estado de la red, los consumidores y los generadores. La infraestructura de la medida, junto con una red de comunicaciones adecuada, proporciona a la red inteligente la información necesaria para la toma de decisiones y los medios adecuados para el envío y recepción de órdenes y consignas.

Esta tecnología incluye tanto a los elementos de la medida que informan el estado de la red, (en subestación centro de transformación y reparto, transformadores, entre otros), como a los contadores inteligentes instalados a nivel de usuario. Este último elemento, el contador inteligente, aporta nuevas funcionalidades que favorecen la comunicación desde el operador de red hasta el usuario, pasando por los agentes intermedios necesarios (comercializadoras, empresas de servicios energéticos, gestores de recarga del vehículo eléctrico y permitiendo participación activa del usuario en el mercado eléctrico. Las funcionalidades consideradas para esta tecnología son Lectura y operación remota, limitación de potencia de forma remota, detección de manipulación de los contadores y aviso a compañía, información al usuario, tarificación horaria, Medida de generación distribuida, Gestión activa de cargas. (UPME Parte I, 2016, pág. 11)

La arquitectura de AMI consiste en medidores inteligentes, redes de comunicaciones y un servidor AMI o MDM/MDC (Meter Data Management/Meter Data Collector) y son usados por empresas prestadoras de servicio de agua, energía y gas donde tienen como principal característica ser altamente distribuidos y permiten ser masivamente escalable a millones de nodos (Miyashita & Takada, 2013, págs. 324-329). En general, los sistemas AMI son operados

desde el centro de operación de una empresa de energía, una red WAN (Wide Area Network) que provee la comunicación desde el MDM/MDC a la zona de medición, a través equipos que permiten la comunicación por esta red WAN y una red NAN (Neighborhood Area Network), FAN (Field Area Network) o MAN (Metropolitan Area Network) que provee medidores inteligentes o concentradores de medidores que están conectados a las viviendas de los usuarios. (K. C. Budka, 2014, pág. 151)

Como se menciona en el párrafo anterior las TIC son el medio que permite a la infraestructura AMI proporcionar los beneficios de las redes inteligentes, por lo tanto, es necesario tener en cuenta sus riesgos, es por ello que la ciberseguridad se define como uno de los aspectos claves a proteger en la resolución 40072 de 29 de enero de 2018, donde se establecen los mecanismos para implementar la Infraestructura AMI en el servicio público de energía eléctrica. (MINMINAS M. D., 2018, pág. 1)

En un ejercicio de pruebas de penetración realizado a la infraestructura AMI de una empresa del sector eléctrico, conectado directamente al poste mediante un cable ethernet al puerto RJ45, debido a que las contraseñas se encontraban configuradas por defecto se accedió a la configuración del concentrador y mediante la conexión vía celular debido a una configuración inadecuada de las listas de acceso fue posible acceder a la red operativa de control, supervisión y adquisición (SCADA). Igualmente se accedió a la red corporativa y a las bases de datos.

Utilizando la herramienta SHODAN, disponible en internet, fue posible tener acceso a los concentradores de la infraestructura AMI de un fabricante de la alianza PRIME, debido a que se encontraban expuesto a Internet. Por geolocalización se accedió a un concentrador que se

encontraba en Colombia específicamente en Bogotá cuyo usuario y contraseña se encontraban por defecto, permitiendo acceder a la configuración del concentrador y a los medidores conectados a él.

Justificación

Las soluciones de ciberseguridad para la infraestructura de energía crítica son imperativas para la entrega de una energía confiable. En la actualidad en un mundo altamente conectado, con una ciberamenaza cada vez más sofisticada, no es realista suponer que los sistemas de entrega de energía sean aislados o inmunes a ser comprometidos. (Hawk C. & Kaushiva A, 2014, págs. 84-95).

La modernización tecnológica de la infraestructura del sector eléctrico en Colombia, la automatización de los procesos y de sus centros de gestión de energía local y remota, bajo un mundo influenciado por la transformación digital como habilitador para que las empresas sean competitivas y el establecimiento de normas y regulaciones que buscan proteger la infraestructura crítica, se convierten en motivadores de cambios drásticos en las empresas para enfrentar los riesgos que conllevan la adopción de las tecnologías emergentes y el cumplimiento regulatorio y normativo tales como:

- Acuerdos realizados en el Concejo Nacional de Operación que se vuelven de obligatorio cumplimiento para las empresas del sector eléctrico.
- En un corto plazo se aprobará el proyecto de Ley para la protección de infraestructura crítica del país (ICCN, 2017, pág. 4)

- Adicional al tema regulatorio aumentan las amenazas emergentes como el secuestro de información que son aplicables a la tecnología de la operación.

Las empresas del sector eléctrico que intenten sobrevivir no solo tienen que cambiar su forma de ofrecer los servicios y retener al cliente, si no que se hace necesario adoptar nuevas formas de implementar la seguridad, pasando del concepto de seguridad por oscuridad, donde solo el fabricante conocía las vulnerabilidades a una red eléctrica interconectada e inteligente, que requiere un enfoque donde converge la seguridad física, ciberseguridad y seguridad operativa para reducir los riesgos de un ciberataque sobre los ciber activos críticos.

Descripción del problema

Las redes eléctricas han sido identificadas como infraestructuras críticas. (Alan T. Murray, 2007, pág. 2) Estas son cada vez más dependientes de las Tecnologías de la Información y la Comunicación (TIC) para el funcionamiento y control de las instalaciones físicas. A medida que aumenta la conectividad de las TIC, también aumenta el potencial de intrusiones cibernéticas. (Stefanov, 2014, pág. 11238)

Las empresas con infraestructura crítica del sector eléctrico del país se están enfrentado a cambios en su manera de atender la demanda de sus servicios, con la necesidad de ser competitivos adoptan nuevas formas de hacer las cosas a través de la transformación digital. Este proceso de adopción trae consigo amenazas emergentes además de los cambios regulatorios que intentan proteger la infraestructura critica del país y la privacidad de las personas. Frente a este panorama, las aplicaciones de los modelos de seguridad de la información tradicionales de tecnología informática podrían poner en riesgo la confiabilidad del servicio por ej. Una actualización de un sistema operativo de la consola de operación que aún no ha sido homologada por el fabricante, pero su vulnerabilidad se encuentra reportada como crítica y dicho sistema operativo ya no es soportado por que cumplió su ciclo de vida.

Las amenazas emergentes como los ataques de día cero, que aún no han sido identificados por los fabricantes de seguridad para incluirlos en sus bases de datos de firmas de antivirus, podrían comprometer la infraestructura crítica mediante técnicas de ataque como el secuestro de la información y de dispositivos electrónicos inteligentes.

El análisis de Miller y Rowe (2012) indica que el número de ciberataques en redes de infraestructura crítica aumenta con el tiempo. El número de incidentes relacionados con SCADA (Supervisory Control And Data Acquisition) también crece de manera constante. En 2010, el repositorio de Incidentes de Seguridad Industrial (RISI) tuvo 161 incidentes enumerados con aproximadamente 10 nuevos incidentes que se agregan cada trimestre (Tudor y Fabro, 2010). En 2013, la base de datos RISI contenía ya 240 incidentes registrados entre 2001 y 2012 (RISI, 2013). Además, un extenso estudio del estado actual de seguridad cibernética de los sistemas SCADA basado en un conjunto de entrevistas con un gran número de expertos confirmó que las amenazas cibernéticas en los sistemas SCADA están aumentando, son "reales y están en expansión" (Morgan, 2013). (Cherdantseva, y otros, 2016, pág. 2)

La probabilidad que un ataque ocurra es cada vez mayor, debido al aumento de las amenazas emergentes tales como el secuestro de la información, como se evidenció en mayo de 2017, a través del ataque a nivel mundial, wannacry y sus distintas variantes, que explotaron la falta de actualización de la infraestructura TIC que soporta las tecnologías de la operación.

Comprometer el canal o lectura de medidas de contadores, en tiempo real, puede resultar en el robo de energía o el control remoto malicioso de electrodomésticos. Por lo tanto, se requiere una seguridad rigurosa del hardware / software para garantizar la validez de las diferentes partes de la comunicación tales como concentradores de cabecera y los contadores inteligentes. Si un atacante se apodera del concentrador de cabecera, entonces podría ser capaz de enviar un comando de interrupción de suministro a los contadores inteligentes con respuesta a la demanda. La interrupción puede hacerse permanente si se ordena a todos los contadores que cambien sus claves criptográficas a algún nuevo valor que solo conoce al atacante. El impacto podría ser enorme,

millones de hogares se quedarían sin energía hasta que los contadores fuesen sustituidos o se repusiesen las claves auténticas. Como consecuencia de ello, la seguridad podría verse en peligro a nivel local, y las empresas podrían perder sumas importantes de dinero. La ciberseguridad en las redes inteligentes necesita prevenir este tipo de ataques y tener un mecanismo de recuperación y capacidad de supervivencia en caso de ataques. (UPME Parte 4, 2016, pág. 3)

Teniendo en cuenta lo expuesto en los antecedentes y la justificación del trabajo de grado propuesto se realizó el análisis documental de distintas fuentes y documentos entre ellos el marco de trabajo de seguridad de NIST, normas y estándares como NERC CIP, ISO 27019, IEC 62351, IEC 62443 y NTC 6079, para establecer una metodología para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano encontrando que en dichas fuentes se expresa el "QUE" pero no el "COMO" asegurarlos.

Pregunta de investigación:

¿Cuál es la metodología para el análisis y evaluación de ciberseguridad para proteger y asegurar los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano ante posibles ataques cibernéticos?

Objetivos

Objetivo general

Establecer una metodología para el análisis y evaluación de ciberseguridad para proteger y asegurar los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano ante posibles ataques cibernéticos.

Objetivos específicos

1. Identificar y analizar las vulnerabilidades de los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia.

2. Establecer los requisitos de ciberseguridad para los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia.

3. Construir una metodología de ciberseguridad la cual permita analizar el riesgo y el impacto en el servicio de medición avanzada en una empresa de energía en Colombia.

4. Evaluar la metodología diseñada en una empresa de energía de Colombia, tomando como muestra las vulnerabilidades encontradas, aplicando técnicas de ethical hacking, revisión documental y pruebas de vulnerabilidades a un concentrador seleccionado.

Marco teórico

A continuación, se define que es una red inteligente, la infraestructura de medición avanzada y los protocolos que la soportan.

Gracias la unión y estandarización establecida entre distribuidores de energía, fabricantes y desarrolladores, la existencia de protocolos relacionados con las redes inteligentes no es tan profusa como en otros entornos de la industria. De entre los protocolos salidos de esta unión y estandarización se analizan aquellos cuyo uso es más común en el territorio español y aquellos que son usados ampliamente a lo largo del territorio europeo: (CERTSI, Protocolos y puntos de análisis, 2017, págs. 7-23)

- PRIME
- Meters and More
- DLMS/COSEM
- G3-PLC
- OSGP

Prime

PRIME se utiliza principalmente en Europa, siendo España uno de los países con mayor implantación gracias a las compañías Iberdrola (principal fundador e impulsor de la alianza) y Gas Natural Fenosa, aunque su uso también se ha expandido a otras partes del mundo, el despliegue de dispositivos con tecnología PRIME supera los 10 millones de equipos alrededor del mundo. (PRIME, 2018)

A nivel de seguridad, PRIME define 3 perfiles diferentes, a nivel de capa MAC o capa de nivel 2:

- Perfil de seguridad 0: no aporta cifrado y la protección queda relegada al nivel de seguridad que aporten las capas superiores.
- Perfil de seguridad 1 y 2: Aportan cifrado. El perfil 2 aparece con en la especificación 1.4 del protocolo y se diferencia del perfil 1 en que cifra más tipos de paquetes, basándose para ello en primitivas criptográficas y utilizando AES128.

Las ventajas que aporta el cifrado son:

- Confidencialidad, autenticidad e integridad de paquetes garantizada por el uso de un algoritmo de cifrado a nivel de capa de enlace.
- Autenticación garantizada porque cada nodo posee su propia clave única, conocida solo por el propio nodo y el nodo base, y que se establece en la fabricación del dispositivo.
- Prevención de ataques por repetición mediante el uso de un campo de 4 bytes para el contador de paquetes.

Los mecanismos de seguridad propuestos en los perfiles de seguridad no protegen frente a ataques al medio (ataques temporizados, ataques eléctricos o electromagnéticos, ruido en el canal, etc.). (CERTSI, Protocolos y puntos de análisis, 2017, pág. 10)

Meters and More

Meters and More es la evolución del protocolo propietario de telegestión de la compañía energética italiana ENEL, que se ha desplegado en España gracias a su compra de la compañía ENDESA. Actualmente se ha creado una alianza para promocionar el uso del protocolo de forma abierta con otros competidores y fabricantes. (Meters and More, 2018)

A nivel de seguridad, el protocolo Meters and More presenta las siguientes características dentro de la capa de acceso al medio o capa dos (2) del modelo OSI:

- Cifrado mediante claves AES de 128 bits.
- Autenticación en base a claves simétricas.
- Protección frente a ataques de retransmisión.
- Comprobación de integridad de mensaje.
- Claves individuales para cada contador, con control de acceso (lectura/escritura).
- Protección extremo-extremo.

Los mensajes se cifran y autentican mediante la misma clave. (CERTSI, Protocolos y puntos de análisis, 2017, pág. 12)

G3-plc

El protocolo está impulsado por el gestor de redes de distribución francés (ERDF).

G3-PLC11 es un protocolo estándar internacional abierto desarrollado específicamente para las redes inteligentes por Sagem12, ERDF13 y Maxim14; que trabaja a baja frecuencia, por

debajo de los 500 kHz, promoviendo la interoperabilidad entre los 10 kHz y los 490 kHz en su comunicación. Soporta diferentes modulaciones de OFDM y se trata de un protocolo con comunicación bidireccional, de gran fiabilidad. La especificación G3-PLC incluye las capas física y de enlace (MAC), donde se apoya en OFDM, y una capa de adaptación 6LoWPAN para transmitir paquetes IPv6 por la red. Estas características hacen que este protocolo esté pensado para infraestructuras que poseen multitud de nodos a gran escala. (G3-PLC, 2018)

El método G3-PLC adoptado para la implementación de la seguridad a nivel físico por G3-PLC consiste en un cifrado AES-128 a nivel de capa de control de acceso al medio (MAC), correspondiente con la capa 2 del modelo OSI, que posee las siguientes características:

- Simplicidad: Se basa en una sola credencial (una clave de 128 bits pre-compartida) y un único algoritmo de cifrado (AES-128).
- Seguridad: Tiene un diseño bien conocido y mejorado de esquemas criptográficos.
- Extensibilidad: En el caso de OFDM sobre PLC, se puede ampliar fácilmente para apoyar la distribución de la clave de grupo.

La confidencialidad e integridad están asegurados a nivel de MAC. Como se define en IEEE 802.15.4, un tipo de cifrado CCM se entrega a cada trama transmitida entre los nodos de la red. El modo de cifrado CCM es utilizado en la capa MAC, y previene de accesos indebidos de dispositivos a la red que realizan acciones maliciosas en la misma y en otros procesos de capas inferiores. Las tramas MAC se cifran y descifran en cada salto. Las únicas excepciones son algunas tramas en las primeras etapas del proceso de arranque. Para apoyar este servicio, todos los nodos de la red reciben la misma clave de sesión de grupo (GMK). Esta GMK se distribuye de forma individual y de forma segura a cada nodo mediante el canal seguro EAP-PSK.

Por otra parte, G3-PLC presenta dos arquitecturas de autenticación diferentes:

- La función de servidor de autenticación esta soportada directamente por un LBS (LoWPAN BootStrapping Server). En este caso todo el material de autenticación (credenciales, listas de acceso, etc.) se debe cargar en los LBS. El LBS contiene toda la información base de cada uno de los dispositivos activos.
- El servidor de autenticación está soportado por un servidor AAA (autenticación, autorización y contabilización) remoto. En este caso, el LBS sólo es responsable de la transmisión de los mensajes EAP al servidor AAA través de un protocolo AAA estándar como es RADIUS.

Dlms/Cosem

DLMS/COSEM es un protocolo de nivel de aplicación que define desde la capa cuatro (4) hasta la capa siete (7) del modelo OSI. El significado de las siglas que dan nombre al protocolo es el siguiente: (DLMS/COSEM, 2018)

- DLMS: "Device Language Message Specification", un concepto generalizado para un modelo abstracto de entidades de comunicación.
- COSEM: "COmpanion Specification for Energy Metering", fija las reglas, basadas en estándares, para el intercambio de información con los contadores de energía.

La seguridad en el protocolo DLMS/COSEM se clasifica en tres niveles de seguridad diferentes:

- Lowest level security: Este nivel no aporta ningún tipo de seguridad a la comunicación DLMS/COSEM.
- Low Level security: La seguridad de la comunicación DLMS/COSEM está basada en el uso de credenciales. El cliente ha de disponer de una contraseña para poder realizar la comunicación.
- High Level security: Es el máximo nivel de seguridad permitido. El cliente y el servidor han de realizar un método de autenticación mutua utilizando un proceso de cuatro pasos.

El contexto de seguridad define atributos de seguridad relevantes para transformaciones criptográficas e incluye los siguientes elementos:

- Suite de seguridad: Determina el algoritmo de seguridad utilizado y el uso de cifrado (AES 128).
- Política de seguridad: Determina el tipo de protección que es aplicado a los paquetes del protocolo.
- Material de seguridad: Es información relevante para el algoritmo de seguridad, incluye claves de seguridad, vectores de inicialización, certificados de clave pública, etc. El material de seguridad es específico para cada algoritmo. (CERTSI, Protocolos y puntos de análisis, 2017, pág. 21)

Osgp

El protocolo abierto de Smart Grid (OSGP) se aplica actualmente en varios países en proyectos de Smart Metering a gran escala. Fue desarrollado por OSGP Alliance y publicado como un estándar por el Instituto Europeo de Estándares y Telecomunicaciones (ETSI). Es uno de los protocolos más utilizados y probados en el campo de los contadores y redes inteligentes y en la actualidad existen más de 100 millones de dispositivos que lo soportan desplegados por todo el mundo. (OSGP, 2018)

OSGP sigue un enfoque moderno basado en el modelo OSI y la frecuencia a la que trabajan los dispositivos que lo utilizan se encuentra en un rango entre 9 kHz y 95 kHz.

OSGP especifica una capa de control independiente del medio para la comunicación segura entre medidores y nodos de control.

Las medidas de seguridad se incluyen para proteger la privacidad de los consumidores al restringir el acceso a los datos, utilizándose el cifrado de estos datos para evitar el acceso no autorizado. Las medidas de seguridad también se incluyen para detectar intentos de eludir otras funciones, como por ejemplo no realizar de forma correcta la medición y evitar que se envíen los datos de las lecturas al concentrador.

A continuación, se detallan las cuatro (4) características de seguridad del protocolo:

- Algoritmo RC4: Sistema de cifrado de flujo entre puntos que convierte el texto plano en texto cifrado bit a bit. La implementación del algoritmo RC4 en OSGP es similar a la utilizada en WEP y con similares debilidades.

- Función de respuesta: OSGP implementa una función de respuesta para usar con el mensaje de autenticación.
- Secure Broadcast: Es un mecanismo que se utiliza para enviar actualizaciones de firmware.
- Claves: El protocolo usa claves de sesión para cifrar los mensajes y una clave maestra para la autenticación. (CERTSI, Protocolos y puntos de análisis, 2017, pág. 18)

Imsys

IMSYS es una empresa colombiana que diseña, desarrolla, construye e implementa soluciones de sistemas de medición, soluciones que van desde los Sistemas de Gestión de la Información (SGI), hasta los sistemas de medición (Contadores), pasando por el cerebro de la solución, que es el Concentrador IMSYS. (IMSYS, 2018)

La solución ofrecida, corresponde a un concentrador de datos, que permite leer múltiples marcas de medidores, por medio de diferentes protocolos de comunicación y con diferentes medios de comunicación, solucionando así el problema de la interoperabilidad:

- Actualmente están desarrollados e integrados los protocolos de los medidores TECUN, INELCA y AMS, todos con lectura por puerto RS-485.
- Los medidores TECUN se leen con protocolo DLMS/COSEM, mientras que los medidores INELCA y AMS se leen con protocolo DLT-645.

- Los medidores de CAM, aún no están integrados, pues va a salir una nueva versión con PLC, por lo cual se está a la espera de tenerla a disposición, para iniciar el proceso de integración.

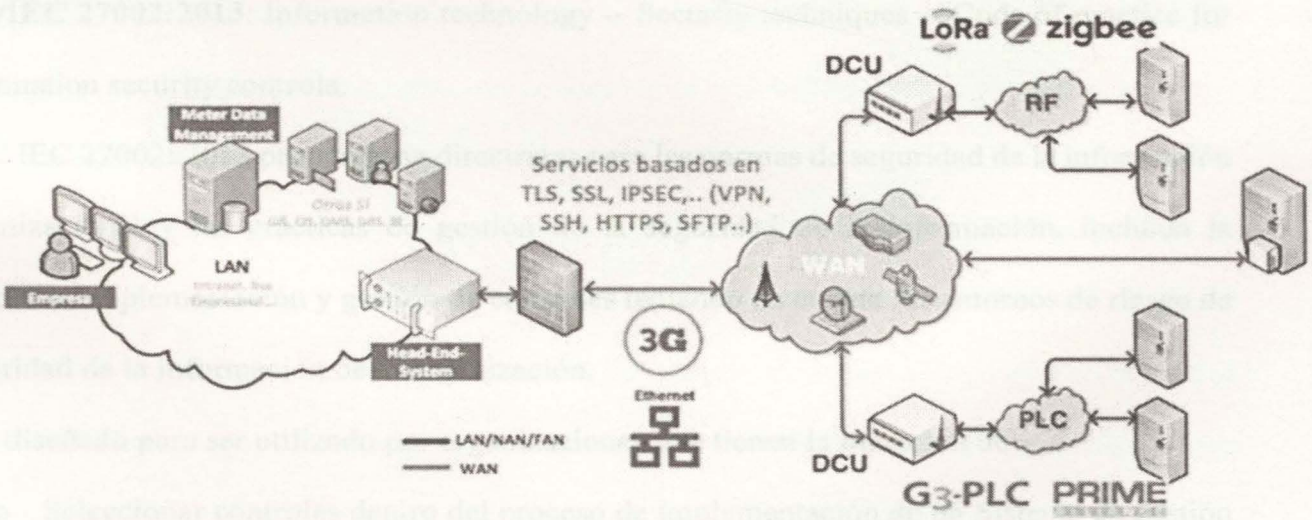
Cumple con la norma NTC 6079 "requisitos para sistemas de infraestructura de medición avanzada (AMI) en redes de distribución de energía electrica, 6.5 requisitos de seguridad", (NTC6079, 2014, pág. 24), para dar cubrimiento a los requisitos de seguridad para los equipos de la infraestructura de medición centralizada:

Los requisitos de seguridad se enfocan en mantener la confidencialidad, integridad y disponibilidad de la información.

Arquitectura de la Infraestructura de Medición Avanzada

La arquitectura de AMI consiste en medidores inteligentes, redes de comunicaciones y un servidor AMI o MDM/MDC (Meter Data Management/Meter Data Collector) y son usados por empresas prestadoras de servicio de agua, energía y gas donde tienen como principal característica ser altamente distribuidos y permiten ser masivamente escalables a millones de nodos (Miyashita & Takada, 2013, págs. 324-329). En general, los sistemas AMI son operados desde el centro de operación de una empresa de energía, una red WAN (Wide Area Network) que provee la comunicación desde el MDM/MDC a la zona de medición, a través equipos que permiten la comunicación por esta red WAN y una red NAN (Neighborhood Area Network), FAN (Field Area Network) o MAN (Metropolitan Area Network) que provee medidores inteligentes o concentradores de medidores que están conectados a las viviendas de los usuarios. (K. C. Budka, 2014, pág. 151)

Figura 1. Arquitectura de una Infraestructura de Medición Avanzada



Fuente: Universidad del Valle, Universidad Nacional. Taller de interoperabilidad y ciberseguridad para infraestructura de Medición Avanzada.

Principales iniciativas de seguridad a nivel mundial para Infraestructura de Medición Avanzada

A continuación, se nombran las normas internacionales aplicables a la infraestructura AMI:

- **ISO/IEC 27001:2013**: Information technology -- Security techniques -- Information security management systems – Requirements.

  ISO / IEC 27001: 2013 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO / IEC 27001: 2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (ISO 27001, 2013, pág. 1)

- **ISO/IEC 27002:2013**: Information technology -- Security techniques -- Code of practice for information security controls.

  ISO / IEC 27002: 2013 proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.

  Está diseñado para ser utilizado por organizaciones que tienen la intención de:

  - Seleccionar controles dentro del proceso de implementación de un Sistema de gestión de la seguridad de la información basado en ISO / IEC 27001;

- Implementar controles de seguridad de la información comúnmente aceptados;
- Desarrollar sus propias pautas de gestión de seguridad de la información. (ISO/IEC 27002, 2015, pág. 1).

- **ISO/IEC 27019:2017:** Information technology -- Security techniques -- Information security controls for the energy utility industry.

ISO / IEC 27019: 2017 proporciona una guía basada en ISO / IEC 27002: 2013 aplicada a los sistemas de control de procesos utilizados por la industria de energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor y para el control de los procesos de soporte asociados. Esto incluye en particular lo siguiente: (ISO / IEC 27019, 2017, pág. 1)

- La tecnología central y distribuida de control, supervisión y automatización de procesos, así como los sistemas de información utilizados para su funcionamiento, como los dispositivos de programación y parametrización;
- Controladores digitales y componentes de automatización tales como dispositivos de control y de campo o controladores lógicos programables (PLC), incluidos sensores digitales y elementos de actuador;
- Controladores digitales y componentes de automatización tales como dispositivos de control y de campo
- Todos los demás sistemas de información de soporte utilizados en el dominio de control del proceso, por ejemplo: para tareas de visualización de datos complementarios y para controlar, archivar datos, registrar historiadores, informar y documentar;

- Tecnología de comunicación utilizada en el dominio de control del proceso, por ejemplo: redes, telemetría, aplicaciones de telecontrol y tecnología de control remoto;
- Componentes avanzados de Infraestructura de medición (AMI), por ejemplo: contadores inteligentes;
- Dispositivos de medición, por ejemplo: para valores de emisión;
- Sistemas de seguridad y protección digital, por ejemplo: relés de protección, PLC de seguridad, mecanismos de gobernador de emergencia;
- Sistemas de gestión de energía, por ejemplo: de Recursos de Energía Distribuida (DER), infraestructuras de carga eléctrica, en hogares privados, edificios residenciales o instalaciones industriales de clientes;
- Componentes distribuidos de entornos de redes inteligentes, por ejemplo: en redes de energía, en hogares privados, edificios residenciales o instalaciones industriales de clientes;
- Todo el software, firmware y aplicaciones instaladas en los sistemas mencionados anteriormente, por ejemplo: Aplicaciones DMS (Sistema de gestión de distribución) o OMS (sistema de gestión de interrupción);
- Cualquier local que albergue los equipos y sistemas mencionados anteriormente;
- Sistemas de mantenimiento remoto para los sistemas mencionados anteriormente.
- ISO / IEC 27019: 2017 no se aplica al dominio de control de procesos de las instalaciones nucleares. Este dominio está cubierto por IEC 62645.

- ISO / IEC 27019: 2017 también incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en ISO / IEC 27001: 2013 a la orientación específica del sector de servicios de energía que se proporciona en este documento.

- **NERC:** (North American Electric Reliability Corporation) y compuesta por los estándares CIP (Critical Infrastructure Protection), CIP-002 a CIP-009. (NERC, 2012)

  Las normas NERC CIP-002 a la CIP-009, tratan:

  - CIP-002: Definición de ciber activos críticos
  - CIP-003: Controles en la gestión de seguridad e información
  - CIP-004: Personal y entrenamiento
  - CIP-005: Perímetros de seguridad electrónica
  - CIP-006: Seguridad física
  - CIP-007: Gestión del sistema de seguridad
  - CIP-008: Reporte de incidentes y planes de respuestas
  - CIP-009: Planes de recuperación para ciber activos críticos.

- **IEC 62351**: IEC 62351 es un estándar de la industria destinado a mejorar la seguridad en los sistemas de automatización en el dominio del sistema de potencia. Contiene disposiciones para garantizar la integridad, la autenticidad y la confidencialidad de los diferentes protocolos utilizados en los sistemas de potencia. (Obermeier, 2015, pág. 1)

- **IEC 62443**: Uno de los principales objetivos de seguridad de la IEC 62443 es la defensa en profundidad, profundizando en los conceptos planteados por ISA99 y extendiendo la seguridad a otros ámbitos desde los fabricantes hasta los operadores.

IEC 62443 recoge todos los aspectos planteados por la ISA99, de hecho, los primeros documentos publicados bajo esta nueva numeración fueron los ya publicados por la ISA, eso sí, con las respectivas modificaciones y actualizaciones de acuerdo con un entorno de sistemas de control cambiante. (INCIBE, 2015, pág. 2)

- **NTC 6079** (NTC6079, 2014, pág. 24), que establece los requisitos para los sistemas de infraestructura de medición avanzada (AMI) en redes de distribución eléctrica.

  La norma en mención define un sistema AMI con una solución integral que tiene la capacidad de gestionar el intercambio de información y datos entre el sistema de gestión y las unidades de medida, permite la gestión remota de diferentes funcionalidades como la toma de lecturas, procesos de conexión y desconexión para los medidores que poseen dicha capacidad, eventos y alarmas, el control de acceso a las interfaces entre otras funcionalidades. El sistema AMI incluye una amplia gama de aplicaciones que permite gestionar la demanda, optimizar la red de distribución, garantizar la integridad del sistema y proveer servicios de valor agregado.

  La norma también indica los requisitos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información. (UPME Parte3, 2016, pág. 67)

Estado del arte

Ciberseguridad y ciberdefensa

> Los Estados se han venido preparando para afrontar este contexto en materia de Seguridad cibernética, siendo Colombia un caso representativo en la región, manteniendo un suministro constante y fiable de información sobre amenazas y vulnerabilidades en el ciberespacio y determinando las acciones que le permiten responder ante estos incidentes y recuperarse de los mismos, en coherencia con las recomendaciones y acciones de organizaciones supranacionales como la ONU, OEA, OCDE y la Comunidad Andina de Naciones. (ESDEGUE, 2019, pág. 111)

Según el documento CONPES 3701, el cual busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país, la ciberseguridad se define como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética. Así mismo, dentro de esta temática se incluye el concepto de ciberdefensa, el cual se define como la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. (CONPES 3701, 2011, pág. 39)

Este documento estableció formalmente la creación del CERT nacional conocido como ColCERT que había sido concebido desde el 2005 en trabajos coordinados de múltiples organismos, el cual se encargaría de la coordinación a nivel nacional de los diferentes actores en aspectos de seguridad informática, este mismo documento estableció la creación del Comando

Conjunto Cibernético (CCOC) encargado de la defensa del país en el ciberespacio y la integración del Centro Cibernético Policial (CCP) como el equipo encargado de la seguridad de los ciudadanos en este entorno. (CCI C. d., 2016, pág. 9)

La primera línea de defensa frente a un ataque cibernético dirigido, son las empresas del sector eléctrico, por lo tanto, deben estar preparadas adoptando nuevas formas de implementar la seguridad, pasando del concepto de seguridad por oscuridad donde solo el fabricante conocía sus vulnerabilidades a una red eléctrica interconectada e inteligente que requiere un enfoque donde converge la seguridad física, ciberseguridad y seguridad operativa.

Según el informe de gestión del riesgo cibernético nacional preparado por la OEA ningún país está preparado cibernéticamente y la preparación debe comenzar con un enfoque de gestión de riesgos disciplinado. Por ejemplo, Colombia inició un enfoque de gestión de riesgos para evaluar su preparación cibernética y promover la confianza de la sociedad en el uso del entorno digital. Las gestiones fueron la respuesta a la tarea impuesta por la Política Nacional de Seguridad Digital (estrategia nacional de seguridad digital), que fue aprobada en abril de 2016 por el Consejo Nacional de Política Económica y Social (CONPES), mediante la emisión del Documento CONPES 3854 de 2016. Colombia adoptó la guía de gestión de riesgos de la OCDE y utilizó ese marco junto con las recomendaciones de la OEA, la UIT y la Organización del Tratado del Atlántico Norte (OTAN) para evaluar las amenazas digitales al país y comprender qué activos críticos estaban en riesgo. El estudio llevó a que el país evaluara los riesgos cibernéticos más apremiantes, identificara cómo afectan los incidentes cibernéticos a las organizaciones colombianas tanto en el sector privado como en el público y convirtiera la seguridad cibernética en una prioridad y un componente importante de su desarrollo

socioeconómico. También ayudó a crear conciencia entre los diferentes interesados en el país sobre los tipos comunes y singulares de incidentes, amenazas y ataques cibernéticos que afectan las entidades y empresas del sector público y se comenzaron a cuantificar los costos para la economía del país. (Hathaway, 2018, págs. 15-16)

Ciberseguridad en el mundo

La décimo tercera edición del reporte global de riesgos ubica el riesgo de ciberseguridad en segundo lugar después de los riesgos por causas naturales (GRP, 2018, pág. 3).

Según el estudio Smart Grids Colombia Visión 2030 - Mapa de ruta para la implementación de redes inteligentes en Colombia, a continuación, se presentan los puntos más importantes de la comparación internacional la cual incluye: (UPME Parte3, 2016, pág. 12)

- **Unión Europea**. El concejo de la Unión Europea ordenó a los estados miembros a identificar posibles infraestructuras críticas europeas. Informar a los otros estados miembros acerca de la existencia de infraestructuras críticas y desarrollar planes de seguridad para los operadores. (CE13, 2008, pág. 2)

  Los países de la Comunidad Europea no han adoptado medidas de ciberseguridad específicas para redes inteligentes, pero varios de ellos si han establecido estrategias nacionales de ciberseguridad. (UPME Parte3, 2016, pág. 28)
- **Reino Unido**. El Centro de Protección de la Infraestructura Crítica Nacional del Reino Unido, da soporte a las compañías eléctricas en comparar sus prácticas de

ciberseguridad contra las mejores prácticas, especialmente en sistemas SCADA. (UKCyber, 2011)

- **Organización de Estados Americanos**. El 37% de las organizaciones encuestadas por la Organización de Estados Americanos (OEA) han adoptado estándares de seguridad industrial como NERC CIP (North American Electric Reliability Corporation, Critical Infrastructure Protection) e ISO 27000. (TrendMicro & OEA, 2015, pág. 32)
- **Estados Unidos**. Las normas NERC han sido referenciadas en Colombia por el Concejo Nacional de Operación (CNO) en su guía sobre ciberseguridad (CNO788, 2015, pág. 8)
- **Brasil**. El tema de ciberseguridad es un elemento transversal a la arquitectura de la Red Inteligente pero el tema se encuentra en desarrollo, con avances realizados por la Agencia Brasilera de Desarrollo Industrial. (UPME Parte3, 2016, pág. 18)

  El Operador Nacional del Sistema eléctrico de Brasil elaboró una estructura de gestión y gobernanza para ciberseguridad tomando como marco de referencia ISO 27002 y el information security fórum. (CIER_ONS, 2018, pág. 14)
- **Chile**. No se identifican recomendaciones específicas en relación con las redes inteligentes.
- **Argentina**. EDENOR es la mayor distribuidora de electricidad de la Argentina en términos de números de clientes y de electricidad vendida, elaboró su marco normativo de ciberseguridad basado en NERC y el modelo de madurez adoptando COBIT 4.1 de ISACA. (CIER_Edenor, 2018, págs. 7-8)

Ciberseguridad en Colombia

Frente a las tendencias de los ciberataques a nivel mundial, Colombia ha tenido su propio campo de preparación como consecuencia de su lucha contra los grupos insurgentes y delincuencia común, viéndose obligada a proteger su infraestructura física y lógica, es por ello que ha realizado esfuerzos de coordinación entre el sector público y privado para que, a través de su participación en el comité de infraestructura crítica nacional sea posible trabajar en un marco de referencia con el objetivo de proteger las infraestructuras críticas del país.

El comité de infraestructura crítica ha permitido la elaboración de una guía, un catálogo, un plan nacional de protección y defensa de la infraestructura crítica para reducir las vulnerabilidades frente a los riesgos y ataques cibernéticos, actualmente se encuentra en la elaboración de los planes sectoriales. (ICCN, 2017, pág. 4)

Marco Jurídico

A continuación se resume el marco jurídico en Colombia:

1982 La ley 23 de 1982, norma de derechos de autor, reconoce la protección de la información en las creaciones intelectuales.

1991 Constitución Nacional:

- Principios y derechos fundamentales: Garantías respecto de la persona.
- Soberanía del Estado: Poder eminente del Estado sobre sus administrados y autonomía.
- Estructura Orgánica y funciones.
- Define instituciones e instrumentos jurídicos.

1993 La Ley 44 de 1993, introduce modificaciones en derechos de autor, complementa la protección de las creaciones intelectuales al soporte lógico.

Decisión 351 de 1993, Protección a los derechos de autor, identifica su alcance y aporta elementos de uso de la información en sistemas de información.

1999 Ley 527 de 1999, trata conceptos para darle valor a la información en el medio electrónico bajo criterios de integridad y accesibilidad.

2000 Ley 599 de 2000, código Penal, establece las sanciones contra los derechos de autor y daño por divulgación de información confidencial.

Ley 594 de 2000 (Ley General de Archivo). Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.

2004 Resolución AG/RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americanos.

- Estrategia para combatir amenazas a la seguridad cibernética.
- Vías de acción:
    - Creación de una red de respuesta a incidentes CSIRT.
    - Identificación y adopción de normas técnicas para arquitectura segura de internet.
    - Adecuación de instrumentos para proteger a los usuarios y las redes de información.

Decisión Andina 587 de 2004, prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.

2005 Ley 962 de 2005, Ley anti trámites, prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de trámites.

Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005.

2007 Ley 1150 de 2007, permite la expedición de actos administrativos por medios electrónicos, se desarrolla el SECOP.

Circular 052 de 2007 (Superintendencia Financiera de Colombia), fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

2009 Ley 1341 de 2009, crea el concepto de la sociedad de la información y la organización de las Tic´s.

Ley 1273 del 2009, sanciona las conductas penales contra la información.

2011 Resoluciones CRC 3066 y 3067 de 2011 (Régimen integral de protección de los derechos de los usuarios e indicadores de calidad para los servicios de telecomunicaciones)

CONPES 3701 Entre sus objetivos se encuentra promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRT (Computer Security Incidente Response) sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura critica nacional, el sector privado y la sociedad civil.

Ley 1453 de 2011. Medidas para garantizar la seguridad ciudadana.

- Vigilancia electrónica.
- Interceptación legal de comunicaciones.

2012 Decreto 1704 de 2012 (reglamenta el artículo interceptación legal de comunicaciones).

Decreto Ley 019 de 2012 (entidades de certificación digital y uso de medios electrónicos).

Ley 1581 de 2012. Ley de Protección de datos personales.

Resolución de la Superintendencia de Industria y Comercio de Colombia (SIC) No. 76434 de 2012 (protección de datos personales).

2013 Decreto 1377 del 2013. Reglamenta la ley de datos personales.

Ley 1621 de2013, actividades de inteligencia y contrainteligencia.

Resolución 68/167 de 18 de diciembre del 2013 de la Asamblea General de la ONU. El derecho a la privacidad en la era digital.

Acuerdo entre Colombia y la OTAN, sobre Cooperación y Seguridad de la Información del 25 de junio del 2013.

2014 Decreto 2573 de 2014 (Gobierno en línea).

2016 CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

2017 Convenio sobre Ciberdelincuencia del Consejo de Europa – CCC (conocido como en convenio sobre cibercriminalidad de Budapest)

- Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004.
- Prevención de las conductas delictivas y contribuya con herramientas eficientes.
- Se encuentra en trámite la ley de ratificación por el Congreso de Colombia (Agosto 2017).

2018 Resolución 40072 de 29 de enero de 2018 Por la cual se establecen los mecanismos para implementar la Infraestructura de Medición Avanzada (AMI) (por sus iniciales en inglés) en el servicio público de energía eléctrica.

Una revisión del marco jurídico permite identificar que existen algunos aspectos que ameritan ser revisados:

- Art. 269E de la ley 1273 es aplicable solo al territorio nacional, (LEY1273, 2009, pág. 2)
- No existe una ley para la protección de infraestructuras críticas
- No hay una regulación respecto a las medidas técnicas de gestión de incidentes de ciberseguridad,
- El espionaje contra personas naturales o jurídicas no se encuentra tipificado como un delito.

En la resolución 40072 de 29 de enero de 2018 se establecen los mecanismos para implementar la Infraestructura AMI en el servicio público de energía eléctrica, donde se define la ciberseguridad como uno de los aspectos claves a proteger. (MINMINAS M. D., 2018, pág. 1)

Acuerdos

A continuación, se describen los acuerdos realizados por parte del Concejo Nacional de Operación para el sector eléctrico:

- **Acuerdo No. 788 septiembre 3 De 2015**. Para la elaboración de este documento se utilizó como referente la normativa publicada por la NERC y compuesta por los estándares CIP-002 a CIP-009, de los cuales se extractaron aspectos aplicables al caso colombiano. (CNO788, 2015, pág. 8), el anexo del acuerdo contiene la guía de implementación de ciberseguridad.

- **Acuerdo CNO 701 – 1004 – 1043.** "Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas y entre este último y el ASIC". (CNO701, 2014, pág. 2), (CNO1004, 2017, pág. 2), (CNO1043, pág. 2). El mayor punto de discusión que motivo el cambio en los acuerdos se centró en las medidas de protección a establecerse para la integridad de los datos.

Metodología

Esquema de trabajo

La metodología que se propone para el "análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano se desarrollará en las siguientes etapas:

1. **Fase uno: Planeación.**
    - Aplicando el concepto de ciberseguridad por diseño se elaboró una propuesta de 34 requisitos para los concentradores, que abordaba los controles de autenticidad (9), autorización (1), disponibilidad (3), Integridad (11), confidencialidad (10).
    - Los requisitos de ciberseguridad incluidos en el RFP, fueron elaborados considerando el estándar NERC, el acuerdo 788 del Concejo Nacional de Operación (CNO) y la norma técnica ICONTEC NTC 6079.

      Entregables:

      1.1 Requerimientos de ciberseguridad para concentradores que soportan la infraestructura AMI.
2. **Fase dos: Análisis.**
    - Los requerimientos fueron diligenciados por cinco (5) fabricantes.
    - El cumplimiento de los requisitos proporcionados por los fabricantes se verificó mediante revisión documental.

- Como resultado se obtuvo que de cinco (5) fabricantes, solo tres (3) cumplieron con 19 requisitos básicos.

  Entregables:

  2.1 Análisis de los requerimientos de ciberseguridad.

3. **Fase tres: Diseño.**

- Los proveedores debían incorporar los requerimientos en el diseño de los concentradores.
- El cumplimiento de los requisitos fue evaluado mediante una actividad de ethical hacking con los tres (3) proveedores seleccionados.

  Entregables:

  3.1 Resultados de las pruebas de ethical hacking realizadas.

4. **Fase cuatro: Evaluación.**

- Los resultados fueron presentados al proyecto como parte de los criterios de selección del proveedor.
- Los fabricantes presentaron los planes de acción para cumplir con los requisitos solicitados.
- Finalmente se realizó un re-test para verificar si los fabricantes implementaron los requisitos faltantes.

  Entregables:

  4.1 Resultados del re-test.

A continuación, se desarrollará cada una de las fases del proyecto:

Contribuciones y resultados del proyecto

Identificar y analizar las vulnerabilidades de los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia.

Amenazas

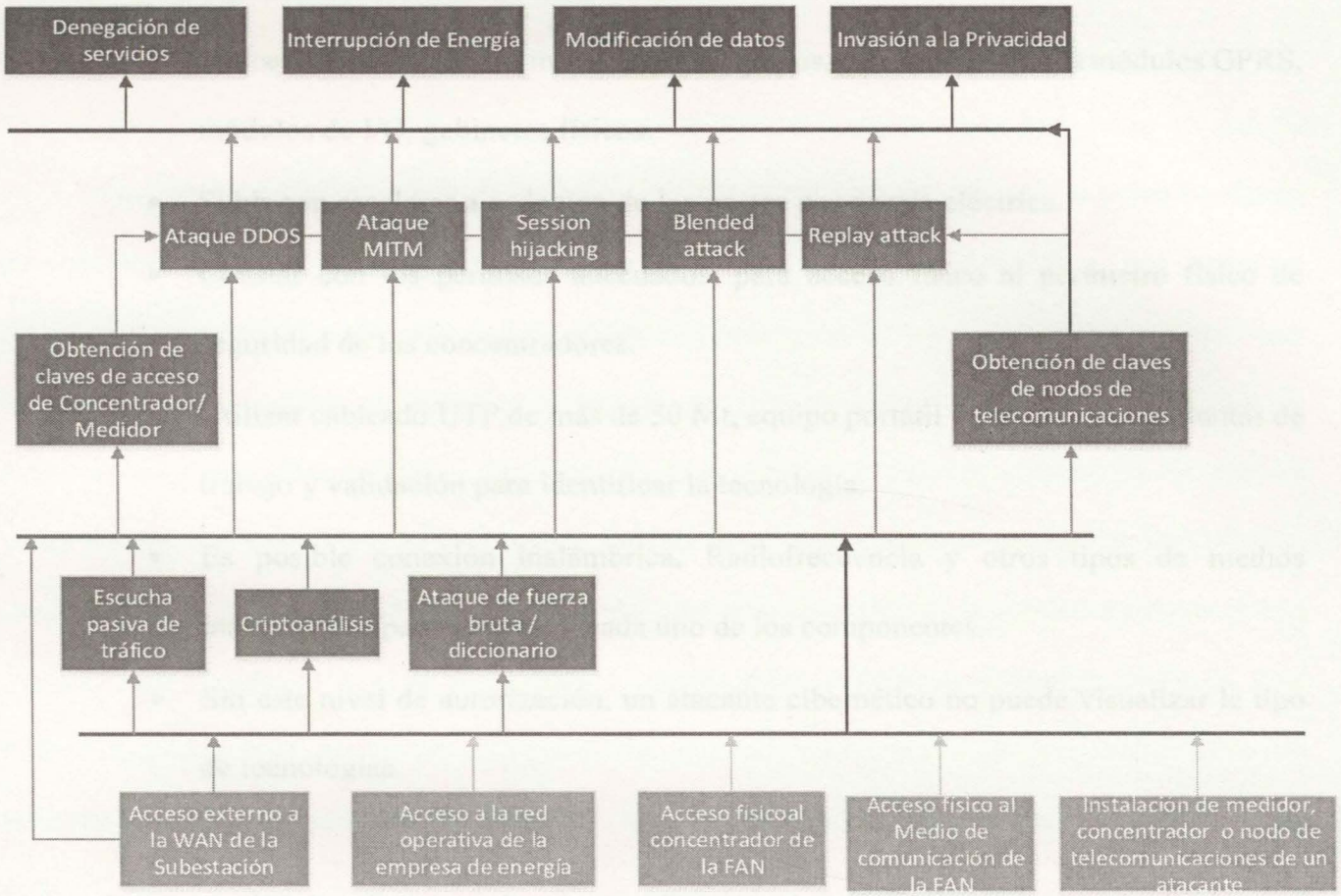
Para identificar las amenazas y vulnerabilidades se propone la técnica de "árbol de ataques" que proporciona un medio estructurado y flexible del diseño de análisis de seguridad de protocolos, aplicaciones y redes de telecomunicaciones. (Schneier, 1999)

En los sistemas AMI de una red inteligente existen múltiples amenazas de seguridad cuyos objetivos están:

- Denegación de servicios de medición (S. Khaithan, 2015.), corte y reconexión remota.
- Interrupción del servicio de energía. (Foreman & Gurugubelli)
- Modificación de datos de la medida desde y hacia el MDC/MDM. (Sahu, Tippanaboyana, Hefton, & Goulart, 2017)
- Invasión a la privacidad. (Neetesh Saxena1, 2017)

Estas amenazas pueden ocurrir desde ataques externos a la WAN y FAN de las redes de telecomunicaciones de AMI, como ataques internos en la FAN o desde las redes operativas de la empresa de energía.

Figura 2 Árbol de Ataques



Fuente: Propia

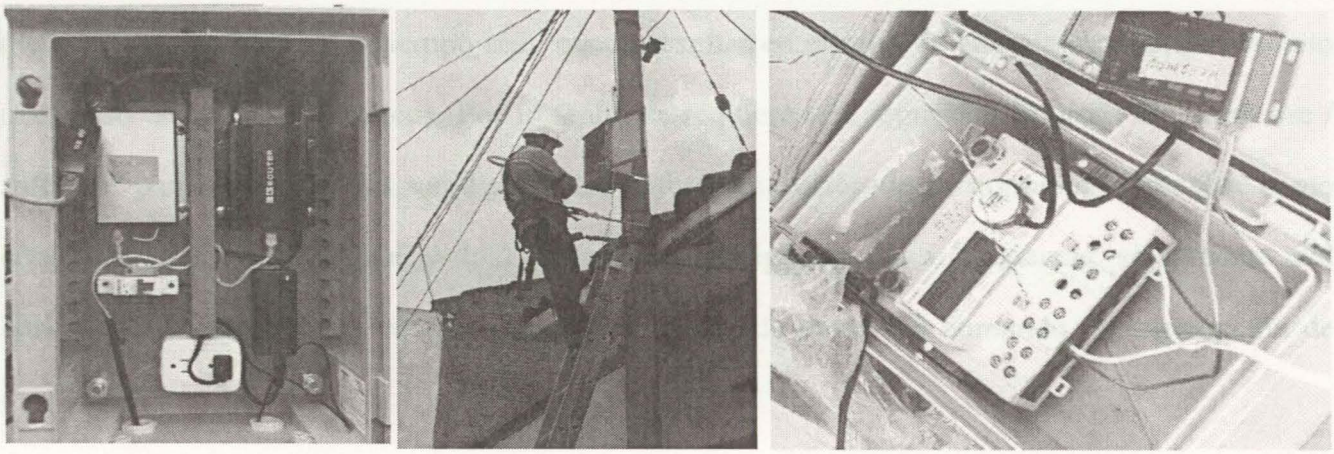
El árbol de ataques permite identificar las amenazas y vulnerabilidades, esta técnica fue diseñada en diseñada en 1999 por Bruce Schneier (Schneier B. , 1999), es necesario pensar como el atacante para entender las diferentes formas por las que un sistema podría ser atacado.

Para el desarrollo de las pruebas a los concentradores, fue necesario tener los siguientes privilegios de acceso físico y lógico a los dispositivos:

- Acceso Físico a la arquitectura de red AMI / Medida Centralizada.
- Ubicación física de los concentradores
- Destapar físicamente los módulos y los equipos, para identificar los módulos GPRS, módulos de I/O, gabinetes físicos.
- Subir con escaleras a cada uno de los postes de energía eléctrica.
- Constar con los permisos adecuados, para acceso físico al perímetro físico de seguridad de los concentradores.
- Utilizar cableado UTP de más de 50 Mt, equipo portátil industrial, herramientas de trabajo y validación para identificar la tecnología.
- Es posible conexión inalámbrica, Radiofrecuencia y otros tipos de medios inalámbricos para detectar a cada uno de los componentes.
- Sin este nivel de autorización, un atacante cibernético no puede visualizar le tipo de tecnologías.

Para la realización de las pruebas se coordinó con el equipo operativo para tener acceso al concentrador desde el poste, conectando un cable al puerto ethernet del concentrador.

Figura 3 Acceso externo a la WAN a través del concentrador ubicado en el poste



Fuente: Propia

Vulnerabilidades

Las amenazas informáticas de las redes inteligentes tienen el potencial de poner en riesgo la seguridad nacional, la estabilidad económica e incluso la seguridad física. Las centrales eléctricas y los sistemas de control, supervisión y adquisición de datos (SCADA), siempre han sido blanco de los piratas informáticos. El paso de sistemas de control cerrados a redes IP abre un nuevo abanico de vulnerabilidades. Por ejemplo, la integridad de datos y la autenticación pueden verse comprometidos a través de ataques de red tales como: spoofing, Man in the Middle, suplantación, o denegación de servicios (DoS). Del mismo modo, la seguridad de datos puede verse comprometida por ataques de sabotaje o internos tales como virus y caballos de Troya. Este último se convierte en una amenaza significativa teniendo en cuenta la apertura potencial de los sistemas y sus interconexiones con diferentes de redes, tales como NAN e Internet. (UPME Parte 4, 2016, pág. 3)

Una vez que se encuentra un punto de entrada, se hace más fácil para el atacante activar un ataque en cadena a la red inteligente. Por ejemplo, comprometer el canal de precios o lectura de medidas de contadores, en tiempo real, puede resultar en el robo de energía o el control remoto malicioso de electrodomésticos. Por lo tanto, se requiere una seguridad rigurosa del hardware / software para garantizar la validez de las diferentes partes de la comunicación tales como concentradores de cabecera y los contadores inteligentes. Si un atacante se apodera del concentrador de cabecera, entonces podría ser capaz de enviar un comando de interrupción de

suministro a los contadores inteligentes con respuesta a la demanda. La interrupción puede hacerse permanente si se ordena a todos los contadores que cambien sus claves criptográficas a algún nuevo valor que solo se conoce al atacante. El impacto podría ser enorme, millones de hogares se quedarían sin energía hasta que los contadores fuesen sustituidos o se repusiesen las claves auténticas. Como consecuencia de ello, la seguridad podría verse en peligro a nivel local, y las empresas podrían perder cantidades importantes de dinero. La ciberseguridad en las redes inteligentes necesita prevenir este tipo de ataques y tener un mecanismo de recuperación (resiliencia) y capacidad de supervivencia en caso de ataques (con éxito). (UPME Parte 4, 2016, pág. 3)

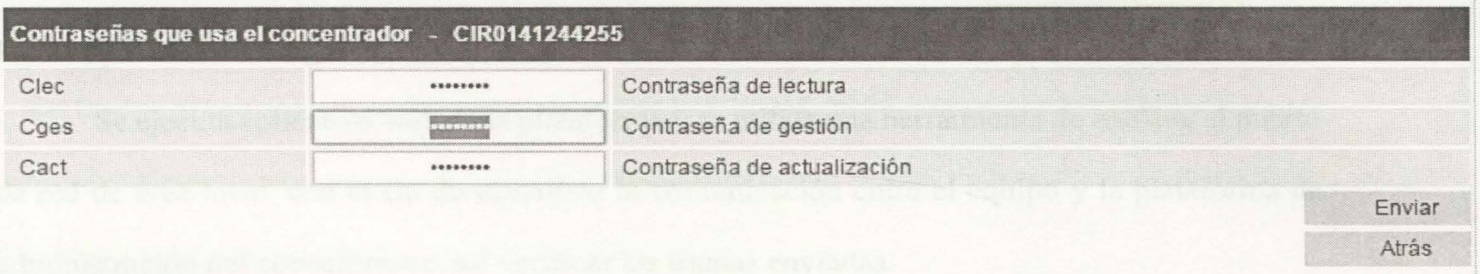
El cumplimiento de los requisitos se verificó mediante revisión documental proporcionada por los fabricantes, las siguientes pruebas de vulnerabilidades y su explotación se realizaron en un ambiente controlado:

- **Denegación de servicios**. Mediante una explotación a la vulnerabilidad en la confidencialidad y autenticidad fue posible una afectación a la disponibilidad del concentrador.
- **Interrupción de energía**. Mediante una explotación a una vulnerabilidad en la confidencialidad fue posible afectar la disponibilidad del servicio de energía.
- **Modificación de datos**. Mediante una explotación a una vulnerabilidad en la confidencialidad fue posible afectar a la Integridad de los datos.
- **Invasión a la privacidad.** Mediante una explotación a una vulnerabilidad en la confidencialidad fue posible obtener acceso a información del cliente.

Denegación de servicios

Se evidencia que las contraseñas que se van a enviar tanto como las que se solicitan al concentrador son completamente visibles ante una herramienta básica del navegador, esta es realizando una inspección del elemento.

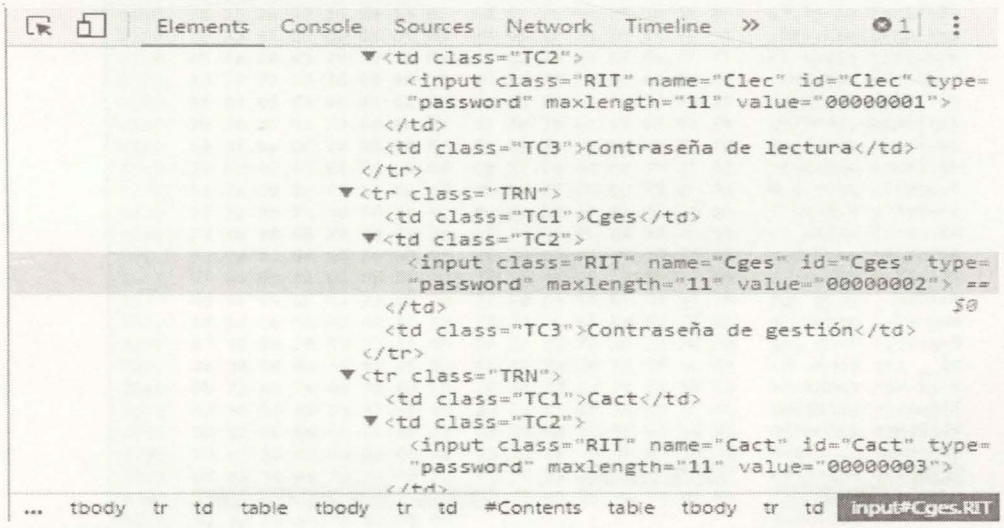
Figura 3. Acceso al concentrador desde la herramienta de Gestión



Fuente: Propia

Estos son los datos recibidos del concentrador al leer el medidor CIR0141244255, este trae las contraseñas, y al realizar una inspección de este elemento en el navegador podemos identificar lo claramente las contraseñas como se muestra en la siguiente imagen:

Figura 4. Acceso a contraseñas en texto plano



Fuente: Propia

Contraseñas de lectura, gestión y actualización.

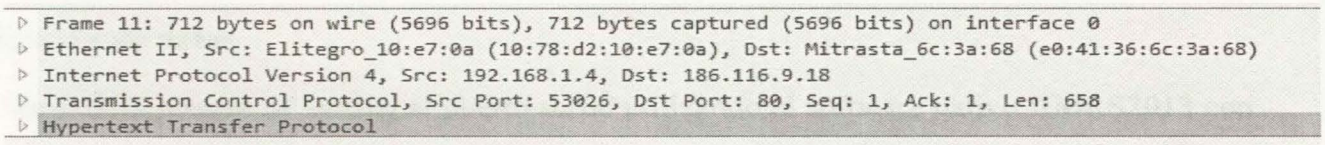
Clec:	**00000001**
Cges:	**00000002**
Cact:	**00000003**

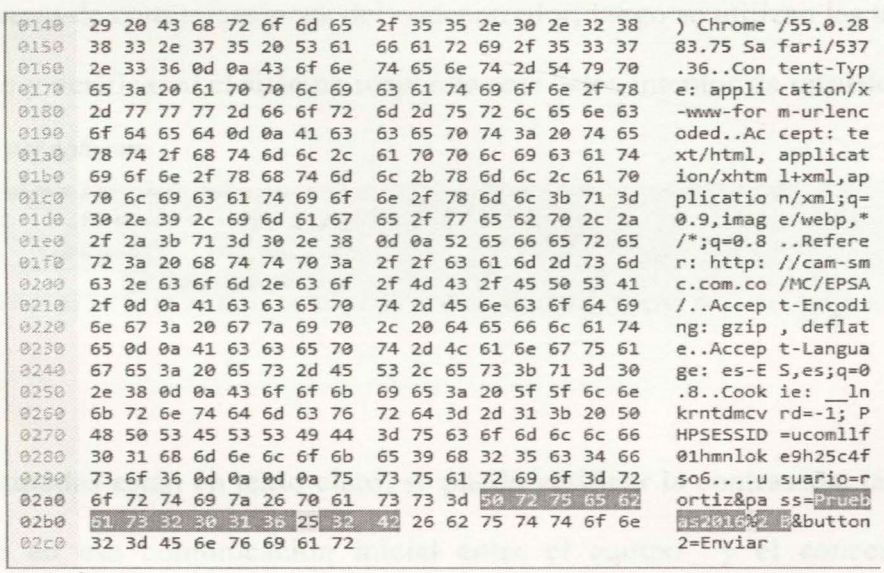
Explotando la debilidad del hallazgo anterior es posible cambiar la contraseña de gestión para que no se administrado, causando una denegación de servicio.

Interrupción de Energía

Se ejecuta aplicativo web de la plataforma y se utiliza una herramienta de sniffing al puerto de red de área local, con el fin de visualizar la comunicación entre el equipo y la plataforma de administración del concentrador, así verificar las tramas enviadas.

Figura 5. Captura de inicio de sección web en plataforma





Fuente: Propia

Se observan las credenciales expuestas en la trasmisión de inicio de sección, no está totalmente clara, pero estando de esta manera es más fácil descifrarla, siguiendo algunos pasos adicionales.

Usuario Real: rortiz Contraseña Real: Pruebas2016+

Se visualiza: rortiz Se visualiza: Pruebas2016%

La contraseña visualizada difiere solo en un carácter de la real.

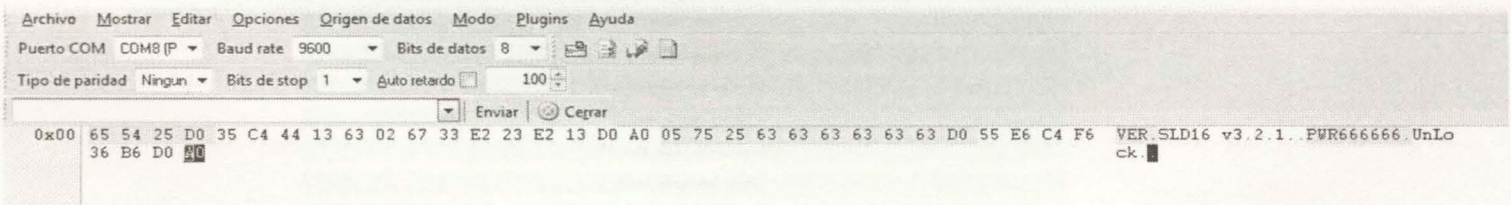
Explotando la vulnerabilidad anterior, es posible ingresar al concentrador con la contraseña del administrador para y realizar una interrupción manual del suministro eléctrico.

Mediante la explotación de la vulnerabilidad anterior es posible ingresar a la configuración del medidor para establecer el corte de energía manual.

Modificación de datos

Se realiza prueba de snifing al puerto serial utilizando el software nativo AMRS2013 con una sonda RS232 al puerto de comunicaciones del concentrador, luego se utilizan las tramas para ser inyectadas de nuevo y verificar si el sistema responde ante estos intentos de intrusión.

Figura 6. Trama inyectada por software.



Fuente: Propia

Las tramas capturadas están en texto claro, se puede verificar la contraseña, la petición y la versión del equipo en esa comunicación inicial entre el equipo y el concentrador. El Concentrador no diferencia entre la inyección de datos interceptada y los datos reales que debe

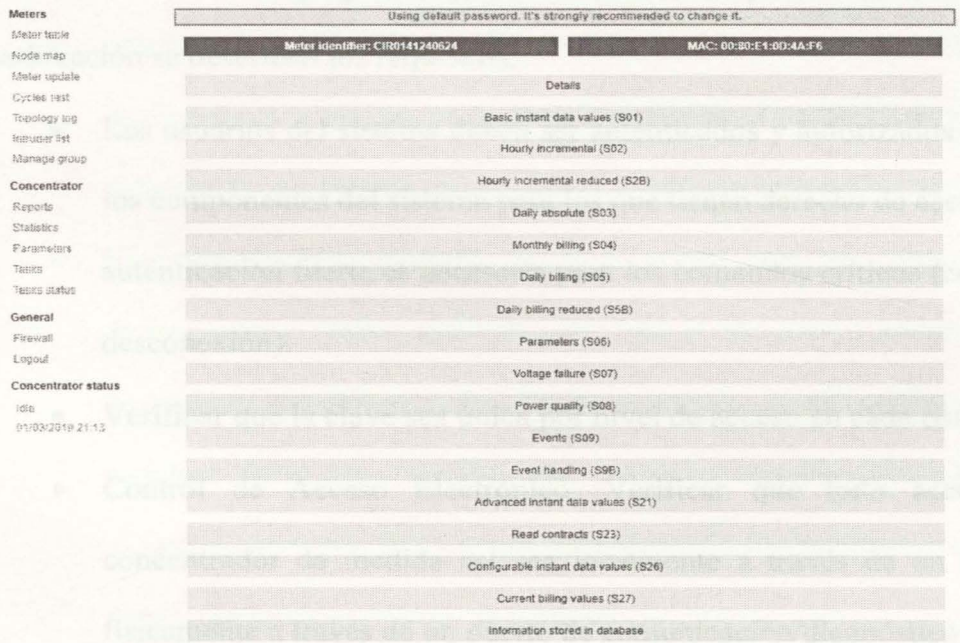
enviar el software nativo, por tanto, no hay seguridad en la información que viaja a través del puerto RS232 y el modem de comunicaciones.

Invasión a la privacidad

Debido a que las contraseñas para lectura del concentrador se encontraban configuradas de fábrica fue posible ingresar a las estadísticas y reportes de los medidores asociados.

A través de los reportes es posible monitorizar el consumo eléctrico e indirectamente también se monitorizan los hábitos y comportamientos de los clientes: cuándo la casa está ocupada, cuándo se enciende la lavadora, la plancha, etc.

Figura 7. Reportes y estadísticas del medidor



Fuente: Propia

Establecer los requisitos de ciberseguridad para los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia.

Aplicando el concepto de ciberseguridad por diseño se elaboró una propuesta de 34 requisitos para los concentradores, que abordaba los controles de autenticidad (9), autorización (1), disponibilidad (3), Integridad (11), confidencialidad (10), el detalle se encuentra en el anexo 1. requisitos de ciberseguridad para los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia.

Autenticidad

La autenticidad es la propiedad que una entidad es lo que dice ser (ISO27000, 2012, pág. 2), a continuación se describen los requisitos:

- Los usuarios del sistema deben ser autenticados y autorizados para acceder solo a los componentes del sistema para los que tienen derecho de acceso. Por ejemplo, la autenticación fuerte es necesaria para los comandos críticos (como el comando de desconexión).
- Verificar que la clave sea única por nivel de acceso en cada concentrador.
- Control de Acceso Electrónico. Verificar que todo acceso electrónico al concentrador de medida así sea localmente a través de un panel de control o físicamente a través de un puerto de comunicación/diagnóstico con un conjunto de pruebas o un computador personal o remotamente a través de medios de comunicación, sean protegidos por una identificación de usuario único (ID) y combinaciones de contraseñas. Una vez que el usuario ha configurado una

combinación apropiado, no será posible tener acceso al dispositivo sin la combinación del ID/contraseña generado por el usuario.

- Construcción de Contraseña. Verificar que las contraseñas creadas sigan un conjunto de reglas a las cuales deberán adherirse en la creación de cada contraseña. Validar que use como mínimo ocho caracteres y la contraseña sea sensible a mayúsculas y minúsculas. Al momento de codificar en texto común, las contraseñas deben contener los siguientes caracteres.
    - Por lo menos una letra mayúscula y una minúscula
    - Por lo menos un número
    - Por lo menos un carácter no alfanumérico (ej. @, %, &, *)
- Construcción de Contraseña. Verificar que cualquier intento de crear una contraseña que infrinja las normas descritas en el requisito anterior, será capturado al momento del intento de creación y el usuario será notificado.
- Visualización de Contraseña. Verificar que sólo se podrá visualizar la identificación de los usuarios en las pantallas, logs, área de memoria o archivos, y otros archivos de registro y configuración. No será posible visualizar las contraseñas de los concentradores de medida por cualquier medio, incluyendo pantallas de visualización local, software de configuración (local o remota, en línea y fuera de línea), navegador y acceso al terminal.
- Autenticación. Verificar que se tenga un medio para verificar que el software de configuración siendo usado para tener acceso o cambiar la configuración, es una

aplicación que ha sido autorizada por el proveedor/fabricante. Se debe evitar que se usen copias no autorizados para acceder a cualquiera de sus características.

- Control de Identificación/Contraseña. Verificar que el software de configuración es controlado por una identificación/contraseña para que no se pueda acceder al software sin la propia combinación de ellos. Bajo ninguna circunstancia debe el software de configuración permitir que las contraseñas del software o del concentrador sean legibles como texto.
- Autenticación de acceso. Verificar que ninguna de las credenciales del sistema puedes ser transmitida en texto claro. El sistema no debe proveer mecanismos de autocompletado o permitir usuarios anónimos.

Autorización

La autorización es el derecho o permiso que es asignado a una entidad del sistema para acceder a un recurso del sistema (62443-1-1, 2015, pág. 13) a continuación se describen los requisitos:

- Autorización de Control de Acceso basado en Roles. Verificar que el concentrador tenga la capacidad de definir roles, definidos por el usuario. Cada rol tendrá la capacidad de tener cualquier combinación de diferentes funciones asignadas a este rol. Un rol se asignará a cada combinación de usuario/contraseña, así otorgando los permisos de dicho rol al usuario en el momento de ingresar.

Disponibilidad

La disponibilidad es la propiedad de ser accesible y utilizable por solicitud de una entidad autorizada (ISO27000, 2012, pág. 2) , a continuación se describen los requisitos:

- Verificar que todas las partes del sistema estén bajo supervisión, administración y control, en la supervisión del comportamiento del sistema se deben detectar situaciones anormales y algunas acciones automáticas para contrarrestarlas, deben ser posibles.
- Sincronización. Verificar que se garantice la sincronización de la hora local de los medidores en sitio, o de manera remota a través del CGM.
- Monitorización de componentes. Verificar que solución cuente con mecanismos para monitorizar los eventos de los componentes que estén relacionados con Ciber Seguridad, en modalidad (7x24x365). Las herramientas deberán emitir alertas automatizadas que permitan detectar e informar incidentes de seguridad.

Integridad

La integridad es la propiedad de propiedad de proteger la exactitud y la completitud de los activos. (ISO27000, 2012, pág. 5) , a continuación se describen los requisitos:

- Verificar que el sistema sea capaz de garantizar la integridad de los datos intercambiados en todo momento. Es necesario asegurarse de que los datos no son modificados por cualquier entidad no autorizada durante la comunicación o el acceso a los datos. Para esto, se debe implementar algoritmos de encriptación.

- Verificar que el sistema cuenta con la capacidad de implementar un mecanismo anti-repetición (replay). Este mecanismo es necesario para evitar la repetición de mensajes para los comandos críticos, tales como desconexión, alarma, etc.
- Verificar que el sistema permita la utilización de mecanismos de control clásicos (incluyendo fecha y hora o la numeración con el vector inicial) para garantizar la identificación de cada mensaje y su singularidad.
- Pérdida de comunicación remota. Verificar que en el caso de que no se disponga de comunicación remota, se deberá contar con una funcionalidad para que una vez se realice la interrogación local del medidor a través del software propietario o de terceros, se permita el cargue de la información del archivo descargado en sitio al CGM, generando la respectiva trazabilidad del evento en el sistema (registro en medidor y CGM).
- Perfil de auditorías de Logs. Verificar que el concentrador de medida registrará, en un búfer circular secuencial (primero ingresa, primero sale), un registro de logs o históricos en el orden en que ocurran. No existirá la posibilidad de borrar o modificar estos logs, ya que debe guardar completamente y mantener la integridad para los propósitos de auditoria y comprobación.
- Capacidad de almacenamiento. Verificar que los Logs deberán almacenar por lo menos 2048 eventos antes de que la memoria empiece a sobrescribir los eventos más antiguos con los eventos más nuevos. No será posible quitar el soporte de almacenamiento de los logs sin dañar permanentemente el concentrador de medida más allá de poder ser reparado.
- Registro de Almacenamiento. Verificar que por cada evento de log, se registrará la siguiente información:

- Número de registro de Evento: El número de secuencia del evento generado automáticamente.
- Hora y Fecha: Hora y Fecha del evento, incluyendo año, mes, día, hora, minuto, y segundo.
- Identidad del usuario: La identificación del usuario ingresada en el concentrador de medida en el momento del evento.
- Tipo de Evento y alertas: El proveedor del concentrador de medida deberá listar los tipos de eventos y alertas que almacena en logs e históricos.

- Características Específicas Criptográficas. Verificar que para los concentradores que implementan funciones de comunicación específicas sobre redes basadas en IP, se implementan las siguientes técnicas criptográficas y versiones en estos:
  - La funcionalidad del servidor Web suministrada por debe ser de Hypertext Transfer Protocol Secure (HTTPS).
  - La funcionalidad de transferencia de archivos suministrada por el concentrador debe ser Secure File-Transfer Protocol (SFTP).
  - Comunicación oreintada a texto usando una conexión de terminal virtual sobre una red de Ethernet debe ser secure shell (SSH).
  - Single Network Management Protocol (SNMP), implementado en el concentrador debe ser SNMPv3.
  - Funcionalidad de túnel seguro suministrado por el concentrador debe ser una red privada virtual (virtual private network (VPN))

- Técnicas Criptográficas. Verificar que una o más de las técnicas a continuación pueden ser implementadas en los dispositivos:
  - Cifrado en bloque
  - Firmas digitales
  - Autenticación de entidad
  - Funciones de derivación de clave
  - Autenticación de mensaje
  - Creación de números aleatoria
  - Hash seguro
  - Establecimiento de clave
- Técnicas Criptográficas. Verificar que para los concentradores que ofrezcan alguna de las características criptográficas mencionadas en el requisito anterior, cumplan con los requisitos especificados por la División de Seguridad Informática NIST. Como las técnicas y versiones de técnicas pueden cambiar como consecuencia de los nuevos descubrimientos, avances en tecnología y amenazas, los concentradores deben cumplir con los requisitos actuales en el momento de su fabricación.
- Garantía de Calidad de Firmware. Verificar que la garantía de calidad de firmware debe cumplir con IEEE Std C37.231, sobre recomendaciones de prácticas para el control de equipos de firmware con protección de microprocesador.

Confidencialidad

La confidencialidad propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (ISO27000, 2012, pág. 2) a continuación, se describen los requisitos:

- Verificar que el sistema sea capaz de gestionar los derechos de acceso a cualquiera de sus componentes.
- Verificar si el sistema permite la utilización de "certificados" para activar las funciones de seguridad.
- Mecanismos de Vulneración de Contraseñas. Verificar que el concentrador de medida no tenga ningún medio, no divulgado a la organización, donde el control de identidad/contraseña creado por el usuario pueda ser vulnerado. Esto incluye, pero no está limitado a los siguientes mecanismos y técnicas:
    - Contraseña maestra incorporada
    - Rutina de diagnóstico de algún chip integrado que se ejecuta automáticamente en el evento de la falla del hardware o software
    - Derivación de hardware de contraseñas, tales como configuración de dip switches.
- Acceso de Tiempo de Espera. Verificar que el concentrador de medida tenga un mecanismo que automáticamente terminará una sesión de inicio por un usuario después de un periodo determinado de inactividad por el usuario. Se define la inactividad como la falta de entrada por mecanismos locales (pantalla) y/o la falta de actividad en el teclado de un computador conectado al puerto del concentrador de medida. El periodo de tiempo

antes que se activa el mecanismo de tiempo de espera será ajustable por el usuario, entre 1 minuto y 60 minutos en intervalos de 1 minuto.

  - Uso de Network Time Protocol (NTP). La funcionalidad de sincronización de tiempo de red debe ser implementado por NTP v3/4 o SNTP 3/4.

- Firma Digital. Verificar que el software de configuración del fabricante tenga la capacidad de generar una firma digital en la descarga de archivos de configuración y firmware, indicando que el archivo ha sido generado por un programa de configuración de software autorizada y por un usuario autorizado. El concentrador debe tener la capacidad de leer la firma digital aplicada a un archivo de configuración o firmware para verificar que el archivo ha sido creado por una entidad autorizada y que no ha sido alterado o corrupto. El concentrador solo aceptará archivos firmados adecuadamente.
- Acceso al puerto de comunicación. Verificar que todos los puertos de comunicación, así sean físicos o lógicos, excepto por el puerto de diagnóstico del concentrador de medida AMI, tendrán la capacidad de habilitarse o inhabilitarse a través de la configuración de estos dispositivos. Cuando se inhabilita por medio de la configuración, se imposibilita la comunicación a través del puerto inhabilitado.
- Acceso al puerto de comunicación. Verificar que los concentradores AMI tendrán inhabilitados todos los puertos con User Datagram Protocol (UDP) y Transmission Control Protocol (TCP), que no están siendo usados por una aplicación o que permita su deshabilitación.

- Verificar que se hayan implementado mecanismos para el control de acceso en todos los puntos de acceso del Perímetro de Seguridad Electrónica, garantizando al menos los siguientes criterios:
    - Denegar los accesos que vienen configurados por defecto, de manera que los permisos de acceso se deban especificar explícitamente.
    - Aplicar y mantener un mecanismo para asegurar el acceso telefónico a los Perímetros de Seguridad Electrónica.
- Registros de auditoria. Verificar que los sistemas, aplicaciones y demás elementos que conformen la solución de gestión, deberán generar registros o pistas de auditoría de las actividades de acceso de las cuentas de usuario, tanto fallidas como exitosas.

Construir una metodología de ciberseguridad la cual permita analizar el riesgo y el impacto en el servicio de medición avanzada en una empresa de energía en Colombia.

La evaluación de los requisitos de ciberseguridad se realizó calificando su cumplimiento con base en las pruebas realizadas para identificar y analizar las vulnerabilidades encontradas en los concentradores, utilizando los siguientes valores:

- **SI**. Cumple con el requisito.
- **NO**. No cumple con el requisito.
- **N/A**. No aplica.

Después de la verificación de cumplimiento se selecciona todos los requisitos no cumplidos y se realiza una evaluación de riesgos aplicando los siguientes criterios obtenidos del manual de gestión integral de riesgos de la empresa del sector eléctrico:

- Apetito de riesgo.
- Calificación de riesgo.
- Mapa de riesgo
- Priorización y tratamiento de riesgos.
- Identificación de oportunidades

Apetito de Riesgo

Es el nivel de riesgos que la empresa desea asumir en la consecución de sus objetivos.

Calificación del Riesgo

La calificación del riesgo está basada en un modelo cualitativo que usa criterios de calidad e impacto para estimar la exposición al riesgo, apoyado en la cuantificación del escenario de riesgo.

Los criterios de probabilidad consideran tres (3) elementos para el juicio experto al momento de asignar una calificación a un evento de riesgo identificado:

- **Porcentaje**. Se utiliza para determinar la probabilidad de ocurrencia de un evento en términos porcentuales y es especialmente muy útil, cuando se tienen datos históricos disponibles al realizar la evaluación de riesgos.
- **Frecuencia**. Se utiliza para determinar en número de veces, la probabilidad de ocurrencia de un evento.
- **Ocurrencias en proyectos**. Aplica para el análisis de riesgos en proyectos y fue definida con el fin de brindar a los administradores de proyectos una alternativa aplicable para la evaluación de la probabilidad en situaciones específicas del proyecto.

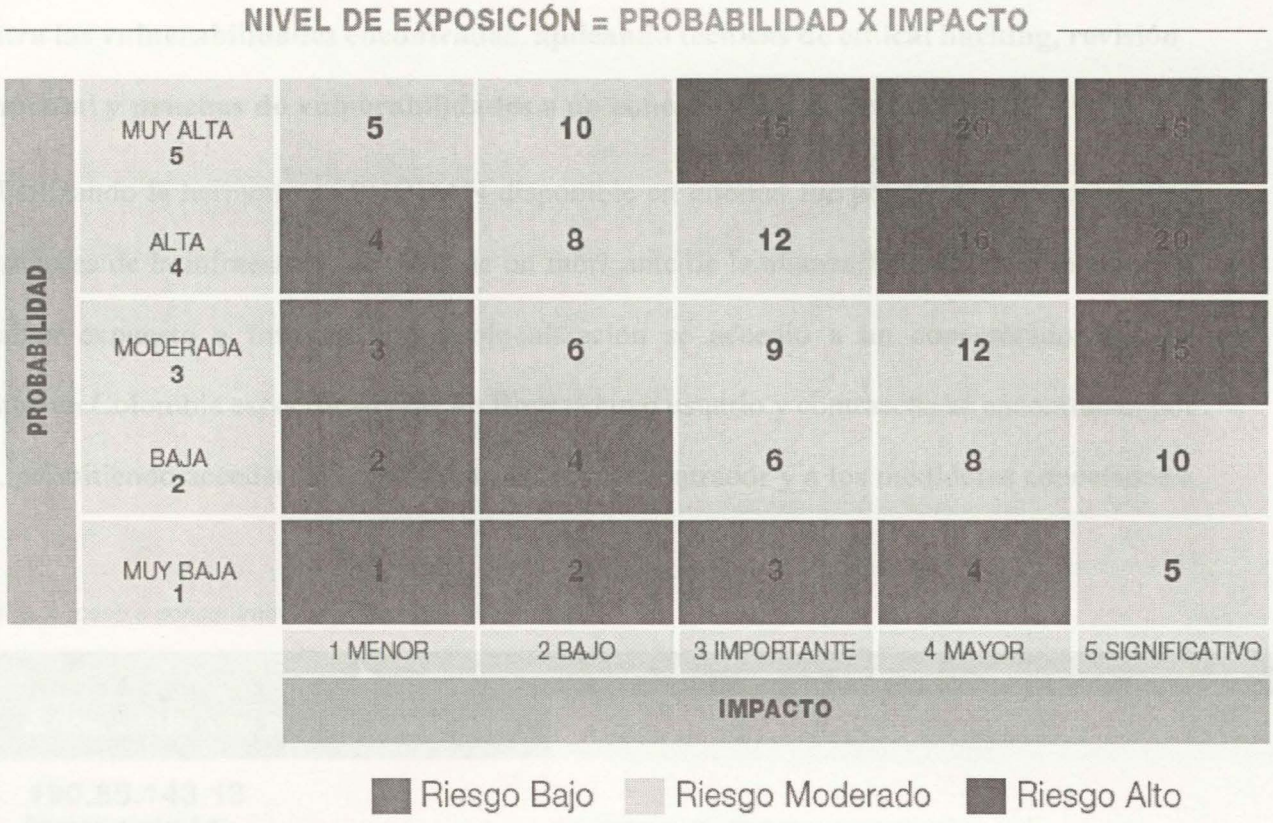
El impacto de la ocurrencia de un evento de riesgos puede afectar diferentes objetivos de negocio. Los criterios de impacto considerados son los siguientes:

- **Impacto Financiero**. (Corporativo y Proyectos), el impacto del riesgo es monetario y se debe analizar como una pérdida en términos de reducción del EBITDA.
- **Reputacional**. Impacto que afecta la imagen de la organización frente a los grupos de interés definidos o la sociedad en general.

- **Recursos humanos**. Impacto que ocasiona lesiones, incapacidades o pérdida de vidas humanas de los colaboradores o terceros.
- **Social**. Impacto que pueda afectar la calidad o condiciones de vida de la comunidad circundante a la zona donde se desarrolla las actividades de la compañía.
- **Regulatorio**. Impacto asociado al incumplimiento de regulaciones y estándares y que podría generar una acción del gobierno o entidad estatal independientemente si es económica o no.
- **Ambiental**. Impacto al medio ambiente generado por las operaciones.
- **Operacional**. Impacto en las operaciones (entendido como la interrupción de operaciones).

El mapa de riesgos es la representación gráfica del nivel de exposición al riesgo. El nivel de exposición es la multiplicación del valor de la probabilidad por el impacto. El mapa de riesgos esta dividido en tres (3) zonas de riesgo: bajo, moderado y alto.

Figura 8. Mapa de Riesgos



Fuente: Marco de trabajo de riesgos

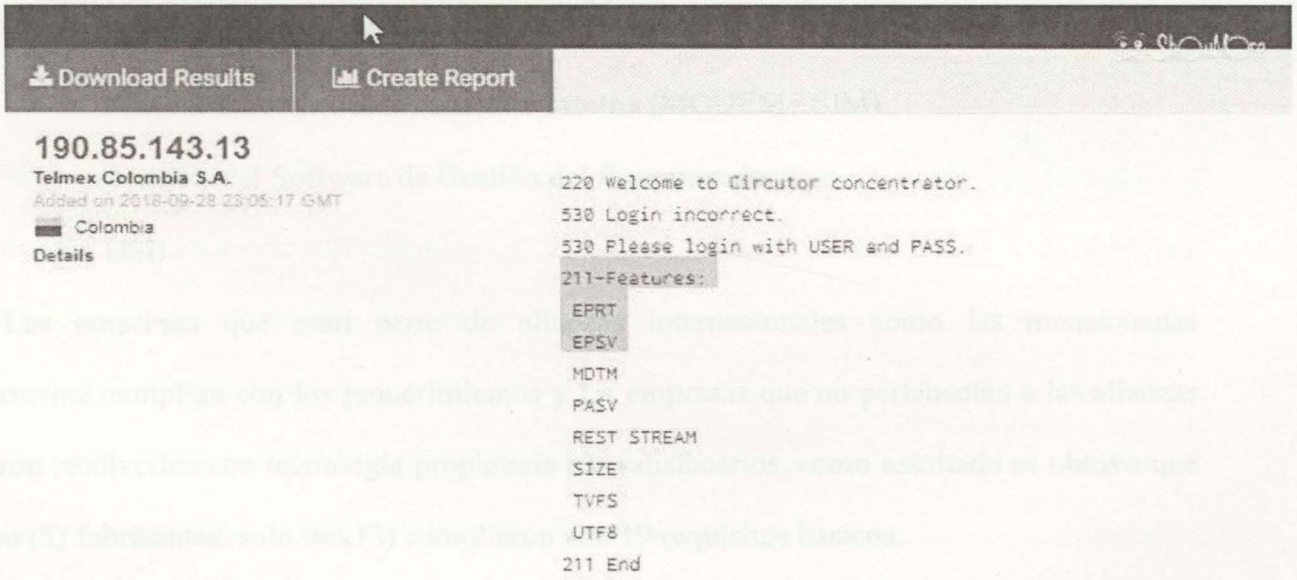
Los riesgos ubicados en la zona roja son los que requieren mayor priorización y requieren ser corregidos antes de salir a producción, los riesgos ubicados en las zona verde y amarilla requieren un plan de tratamiento de riesgos que el proveedor debe presentar al proyecto para aprobación.

Las oportunidades identificadas requieren una valoración mediante un caso de negocio en el evento de plantearse como una iniciativa o en su defecto un plan de acción que contribuya a la mejora continua.

Evaluar la metodología diseñada en una empresa de energía de Colombia, tomando como muestra las vulnerabilidades encontradas, aplicando técnicas de ethical hacking, revisión documental y pruebas de vulnerabilidades a un concentrador seleccionado.

Utilizando la herramienta SHODAN disponible en internet fue posible tener acceso a los concentradores de la infraestructura AMI de un fabricante de la alianza PRIME, debido a que se encontraban expuesto a Internet. Por geolocalización se accedió a un concentrador que se encontraba en Colombia específicamente en Bogotá cuyo usuario y contraseña se encontraban por defecto, permitiendo acceder a la configuración del concentrador y a los medidores conectados a él.

Figura 9. Acceso a concentradores publicados en Shodan.



Fuente: Propia

En un ejercicio de pruebas de penetración realizado a la infraestructura AMI de una empresa del sector eléctrico, conectado directamente al poste mediante un cable ethernet al puerto RJ45, debido a que las contraseñas se encontraban configuradas por defecto se accedió a la configuración del concentrador y mediante la conexión vía celular debido a una configuración inadecuada de las listas de acceso fue posible acceder a la red operativa de control, supervisión y adquisición (SCADA). Igualmente se accedió a la red corporativa y a las bases de datos.

El cumplimiento de los requisitos se verificó mediante revisión documental proporcionada por los fabricantes, las siguientes pruebas de vulnerabilidades y su explotación se realizaron en un ambiente controlado:

- Pruebas locales desde el módulo GPRS/ Ethernet / RJ45.
- Pruebas de conexión remota desde internet
- Pruebas remotas desde conexión externa (MODEM / SIM)
- Análisis del Software de Gestión del Concentrador.
- USB

Las empresas que eran parte de alianzas internacionales como las mencionadas anteriormente cumplían con los requerimientos y las empresas que no pertenecían a las alianzas intentaron resolverlos con tecnología propietaria sin satisfacerlos, como resultado se obtuvo que de cinco (5) fabricantes, solo tres (3) cumplieron con 19 requisitos básicos.

Opinión externa sobre la metodología en una empresa de energía de Colombia

Esta metodología está empezando a emplearse para los concentradores de la Infraestructura de Medición Avanzada de EPSA S.A. E.S.P. en el departamento del Valle del Cauca en Colombia: La Gerente de Gestión de Transmisión y Distribución leyó la metodología realizada en este proyecto de grado y manifestó lo siguiente:

El aporte al Control de riesgos de ciberseguridad en las tecnologías AMI ha sido muy importante pues son tecnologías con alto grado de dispersión y conectividad que requieren controlar los accesos a la información y conformidad de la medida. Ha sido un gran aprendizaje que le ha aportado mucho a los proveedores de AMI, a la empresa e incluso al sector.

El Gerente de Tecnología compartió lo expuesto a continuación después de la lectura de la metodología:

Hasta antes de la llegada de AMI, el sector utilizaba principalmente enlaces dedicados y privados para la gestión de sus teleprocesos. Con la llegada de la telemedida y de AMI las condiciones de la red cambiaron y se empezó a utilizar tecnología móvil celular sobre redes públicas. Esto incrementó el riesgo de seguridad de la información sobre las redes operativas. Adicionalmente, también se incrementó las posibilidades de robo de la información con propósitos delictivos ya que ahora es posible conocer el perfil de consumo de los usuarios y en la práctica es posible determinar el comportamiento del cliente y conocer en qué momentos la vivienda se encuentra sola. Por otro lado, con el acuerdo 788 del Concejo Nacional de Operación (CNO) que establece las condiciones de ciberseguridad para los activos críticos del sector, las condiciones de

seguridad para estos activos cambiaron y se hace necesario tomar medidas que garanticen la integridad y no repudio de la información extremo a extremo.

El trabajo realizado por Sigifredo nos permitió validar que si cada uno de los fabricantes que se contrataron cumplían con los requisitos de ciberseguridad para activos críticos, les permitió a estos proveedores realizar desarrollos y/o ajustes en sus soluciones para cumplir con nuestro requisito y al final asegurar el cumplimiento. Con esto logramos mitigar los riesgos tanto a nivel de plataforma como a través de los medios de comunicación utilizados. Asimismo, queda definido el requisito para futuras implementaciones.

El responsable de planeación compartió lo siguiente, después de la lectura de la metodología:

Gracias a la participación del área de ciberseguridad en el proyecto de Implementación de Medición Inteligente en la compañía, se logró tener un producto maduro y robusto en los elementos del sistema AMI, se logró tener más exigencias desde la operación y mantenimiento, logrando confiablidad en la información a los clientes, desde la facturación hasta la información enviada a las bases de datos, quienes son utilizados por áreas de la compañía para la generación de nuevos negocios, de la misma manera la seguridad de la operación y de los activos que están en riesgo de un ciberataque, gracias a esta metodología, EPSA fue tenida en cuenta en el comité Icontec 144 de medidores, para el desarrollo del módulo de ciberseguridad en la NTC 6079.

A partir de esta participación, se definió que, para futuras implementaciones técnicos y tecnológicos, es obligatorio la participación del área de ciberseguridad para las especificaciones técnicas; fue tan grata la participación en el proyecto, que se ha recibido muy buenos comentarios

de los proveedores de proyecto AMI, que incluso desde la fábrica de los equipos se recibieron buenos comentarios, pues no se habían tenido en cuenta por ellos.

Metodología propuesta aplicable a cualquier Dispositivo Electrónico Inteligente

La metodología que se propone para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano puede ser aplicable a cualquier dispositivo electrónico inteligente desarrollando las siguientes fases:

1. **Fase 1. Identificar**: Identificar y analizar las vulnerabilidades del dispositivo electrónico inteligente actual que soporta la infraestructura de la tecnología de la operación.

   Entregables: Reporte de análisis de vulnerabilidades y ethical hacking.

2. **Fase 2. Establecer:** Establecer los requisitos de ciberseguridad para el dispositivo electrónico inteligente que soportara la infraestructura de la tecnología de la operación.

   - Aplicando el concepto de ciberseguridad por diseño elaborar una propuesta de los requisitos de ciberseguridad para el dispositivo electrónico inteligente que soportara la tecnología de la operación, abordando los controles de autenticidad, autorización, disponibilidad, Integridad, confidencialidad.
   - Los requisitos deberían ser elaborados considerando como mínimo el estándar NIST, NERC, 62443, el acuerdo 788 del Concejo Nacional de Operación (CNO), la norma técnica ICONTEC NTC 6079 y normativa aplicable vigente.

Entregables: Requerimientos de ciberseguridad los dispositivos electrónicos inteligentes que soportaran la tecnología de la operación.

3. **Fase 3. Construir:** Construir una metodología de ciberseguridad que permita analizar los riesgos, oportunidades y el impacto en el servicio de la tecnología de la operación que estará soportado por los dispositivos electrónicos inteligentes.
    - Los proveedores deberían incorporar los requerimientos en el diseño del dispositivo electrónico inteligente.
    - El cumplimiento de los requisitos debería evaluarse mediante una actividad de ethical hacking con los proveedores seleccionados.

    Entregables: Resultados de las pruebas de ethical hacking realizadas.
4. **Fase 4. Evaluar:** Evaluar la metodología tomando como muestra las vulnerabilidades encontradas, aplicando técnicas de ethical hacking, revisión documental y pruebas de vulnerabilidades a el dispositivo electrónico inteligente adquirido.
    - Los resultados deberían ser presentados al proyecto mediante un mapa de calor de riesgos, como parte de los criterios de selección del proveedor.
    - Los fabricantes deberían presentar los planes de acción para cumplir con los requisitos solicitados.
    - Finalmente se debería realizar un re-test para verificar si los fabricantes implementaron los requisitos faltantes.

    Entregables: Resultados del re-test.

Conclusiones

En el presente trabajo se propuso una metodología para el análisis y evaluación de la ciberseguridad para los concentradores que soportan la infraestructura AMI, basada en normas internacionales. Esta metodología busca indicarles a las áreas de telecomunicaciones y técnicas que soportan la infraestructura AMI de las empresas de energía, pasar del "QUE" de las normas internacionales y buenas prácticas, al "COMO" en la implementación de medidas que mitiguen el riesgo de un ataque cibernético.

Para la ciberseguridad en infraestructura crítica se invierte la pirámide de los pilares de confidencialidad, integridad y disponibilidad pasando la confidencialidad que se encuentra en el top para las infraestructuras de TI a la base para la tecnología de la operación quedando como mayor prioridad la disponibilidad, más sin embargo mediante las pruebas realizadas se encontró que mediante una afectación a la confidencialidad fue posible realizar ataques que afectaron la disponibilidad del servicio, la integridad de los datos y acceder a la información del cliente, lo que permitió identificar que los fabricantes no incluían buenas prácticas de ciberseguridad en la configuración de los concentradores

Una vez aplicada la metodología propuesta, las empresas que eran parte de alianzas internacionales como las mencionadas en el marco teórico cumplían con los requerimientos y las que no pertenecían a las alianzas intentaron resolverlos con tecnología propietaria sin satisfacerlos, como resultado se obtuvo que de cinco (5) fabricantes, solo tres (3) cumplieron con 19 requisitos básicos.

Sin embargo, durante la verificación del cumplimiento de los requisitos en sitio, conectados directamente al poste mediante un cable ethernet al puerto RJ45, debido a que las contraseñas se encontraban configuradas por defecto se accedió a la configuración del concentrador y mediante la conexión vía celular debido a una configuración inadecuada de las listas de acceso fue posible acceder a la red operativa de control, supervisión y adquisición (SCADA). Igualmente se accedió a la red corporativa y a las bases de datos.

En una red eléctrica interconectada de la cual forman parte los concentradores AMI, un ataque podría originarse desde cualquier lugar, en cualquier momento, pasando desapercibido por días o meses, teniendo un alto grado de dificultad detectarlo y responder al ataque de forma oportuna y efectiva.

Recomendaciones y Trabajos futuros

La aplicación de la metodología para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura AMI permite disminuir la superficie de un ciber ataque y minimizar sus riesgos. Esta metodología podría adecuarse en la evaluación de otros protocolos tales como PRIME, Meters and More, DLMS/COSEM, G3-PLC, OSGP.

Futuros proyectos de adquisición de concentradores AMI en las empresas de energía del sector eléctrico, podrán incluir los requisitos de ciberseguridad propuestos en la metodología en los requerimientos para ofertar y de esta forma podrán asegurarse de que cuando los concentradores salgan a producción los incluyan desde su fabricación.

Los requisitos de ciberseguridad propuestos en el desarrollo del presente trabajo podrían ser un insumo para la actualización de la norma técnica NTC6079, que permita robustecer el capitulo "*6.2 requisitos de la unidad concentradora*".

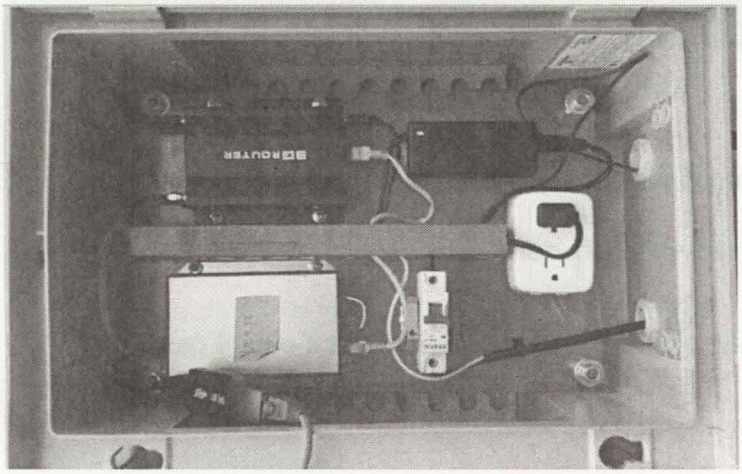
La metodología que se propone para el análisis y evaluación de ciberseguridad para los concentradores que soportan la infraestructura de Medición Avanzada en el Sector Eléctrico Colombiano pueden ser aplicable a cualquier dispositivo electrónico inteligente que soporta la infraestructura de la tecnología de la operación.

Anexos

Anexo 1. Trabajo de campo realizado

Identificación del Equipo

Se realiza reconocimiento de equipos utilizados en el proyecto, hojas de datos y software nativo de configuración, así como plataforma de administración en la capa superior.

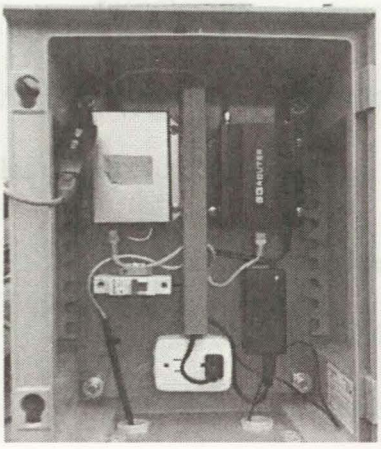


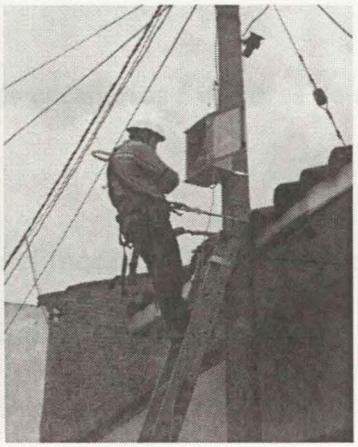
Concentrador de Datos

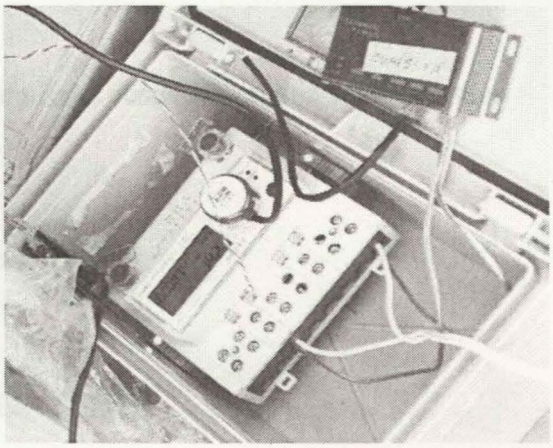
El equipo dispone de:

- Comunicaciones RS485.
- Puerto Ethernet.
- Red WIFI.
- USB
- RF XBEE
- Puerto de Alarma

Escenarios de pruebas de seguridad







Para el desarrollo de las pruebas internas a los concentradores, es necesario tener los siguientes privilegios de acceso físico y lógico a los dispositivos:

- Acceso Físico a la arquitectura de red AMI / Medida Centralizada.
- Ubicación física de los concentradores
- Destapar físicamente los módulos y los equipos, para identificar los módulos GPRS, módulos de I/O, gabinetes físicos.
- Subir con escaleras a cada uno de los postes de energía eléctrica.
- Constar con los permisos adecuados, para acceso físico al perímetro físico de seguridad de los concentradores y medidores.
- Utilizar cableado UTP de más de 50 Mt, equipo portátil industrial, herramientas de trabajo y validación para identificar la tecnología.
- Es posible conexión inalámbrica, Radiofrecuencia y otros tipos de medios inalámbricos para detectar a cada uno de los componentes.

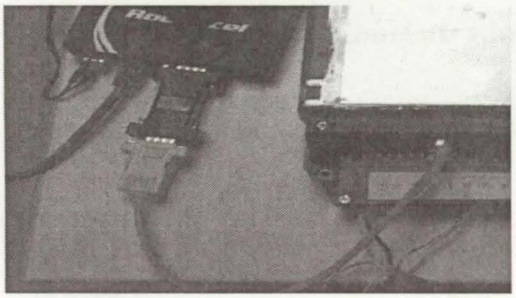
- Sin este nivel de autorización, un atacante cibernético no puede visualizar le tipo de tecnologías.

A continuación, se definen los escenarios / vectores de análisis, desde las cuales se desarrollan las pruebas de seguridad:

- Pruebas locales desde el módulo GRPS/ Ethernet / RJ45.
- Pruebas desde conexión remota desde internet
- Pruebas remotas desde conexión externa (MODEM / SIM)
- Análisis del Software de Gestión del Concentrador.

Puerto físico RS232 en concentrador de datos

Puerto físico de comunicación entre concentrador y modem de comunicación, este modem es externo al concentrador y para administrar localmente el concentrador es necesario desconectar el modem, conectar el puerto RS232 al computador personal y ejecutar el software AMRS2013.



Medio de comunicación PLC en medidores y concentrador

PLC (Power Line Communication), sistema de comunicación que usa el medio de distribución eléctrica para trasmitir la señal de comunicación a una frecuencia de 453 kHz, un ataque debe ser concebido con más recursos de tiempo y capacidad de herramientas tecnológicas.

Prueba de seguridad local puerto RS232 en concentrador

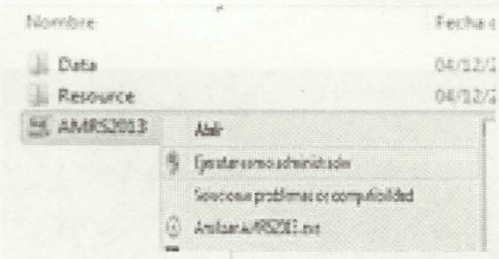
Se traza como objetivo principal infiltrar las comunicaciones con el concentrador vía RS232, reconocer las tramas, modificarlas e inyectarlas al medio para observar el comportamiento del medidor.

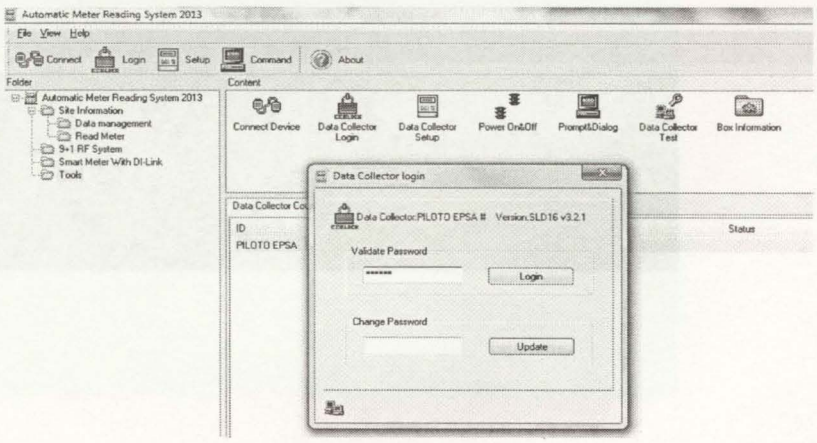
Se inicia con un SNNIFING al puerto serial al momento de la comunicación entre el medidor y el software nativo de configuración local al medidor.

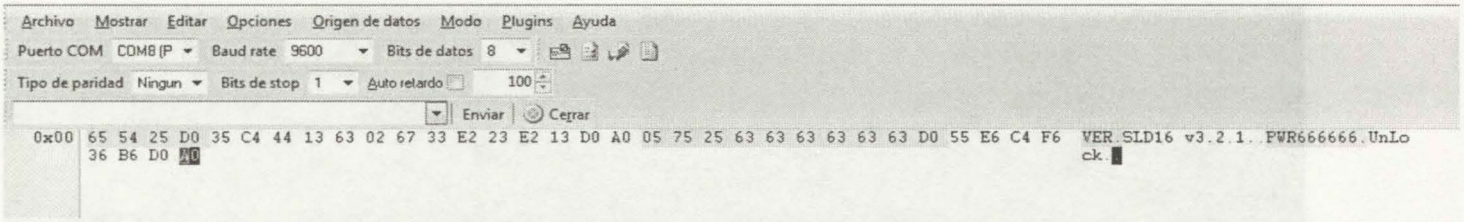
- Se accede al medidor, se solicita una lectura de energía instantánea, como se observa en la imagen a continuación.
- Se capturan las tramas de comunicación en orden en que curren, se realiza análisis de protocolo.
- Se inyectan tramas utilizando los parámetros verificados.
- Se realiza análisis de tramas para tratar de identificar los datos enviados

Administración Local Concentrador – AMRS2013.

- Software no solicita licencia ni credenciales de inicio de sección







Se realiza la inyección de tramas, desde la primera línea de datos enviada, resaltadas en amarillo, se evidencia que el concentrador responde a los comandos, como si estos fueran enviados directo del software ARMS2013, esto es prueba de la falta de un certificado, que le permita al concentrador identificar su software nativo. De la misma manera, no tiene la capacidad de ocultar la información enviada, ya que esta viaja por el medio en texto claro.

Pruebas de seguridad local mediante el uso de puerto USB

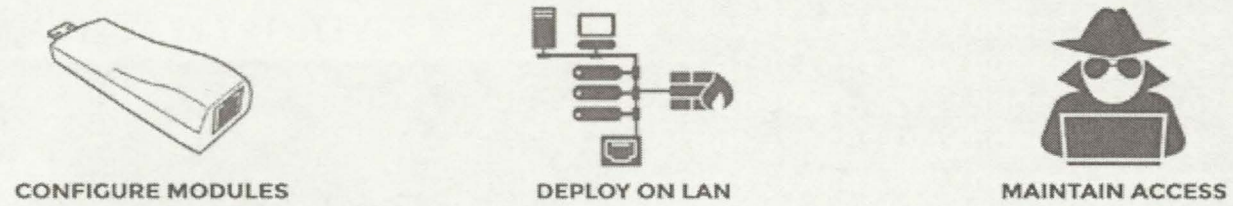
Ataques USB (Rubber Dukky, Lan Tortle)


```
└─#─└▸ lsusb
Bus 002 Device 002: ID 8087:8000 Intel Corp.
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:8008 Intel Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 061: ID 10c4:ea60 Cygnal Integrated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light
Bus 003 Device 003: ID 04f2:b39a Chicony Electronics Co., Ltd
Bus 003 Device 012: ID 8087:07dc Intel Corp.
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

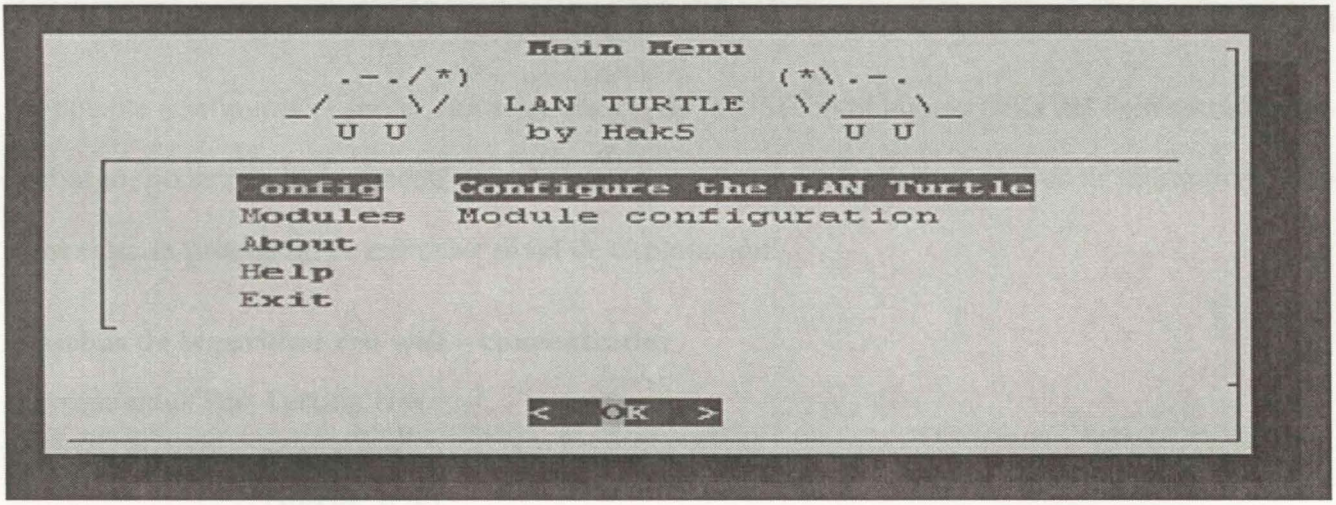
```
[62406.861976] usb 3-6: USB disconnect, device number 58
[62462.781659] usb 3-2: new full-speed USB device number 61 using xhci_hcd
[62462.923153] usb 3-2: New USB device found, idVendor=10c4, idProduct=ea60
[62462.923155] usb 3-2: New USB device strings: Mfr=1, Product=2, SerialNumber=3
[62462.923157] usb 3-2: Product: CP2102 USB to UART Bridge Controller
[62462.923157] usb 3-2: Manufacturer: Silicon Labs
[62462.923158] usb 3-2: SerialNumber: 0001
[62462.924076] cp210x 3-2:1.0: cp210x converter detected
[62462.924524] usb 3-2: cp210x converter now attached to ttyUSB1
```

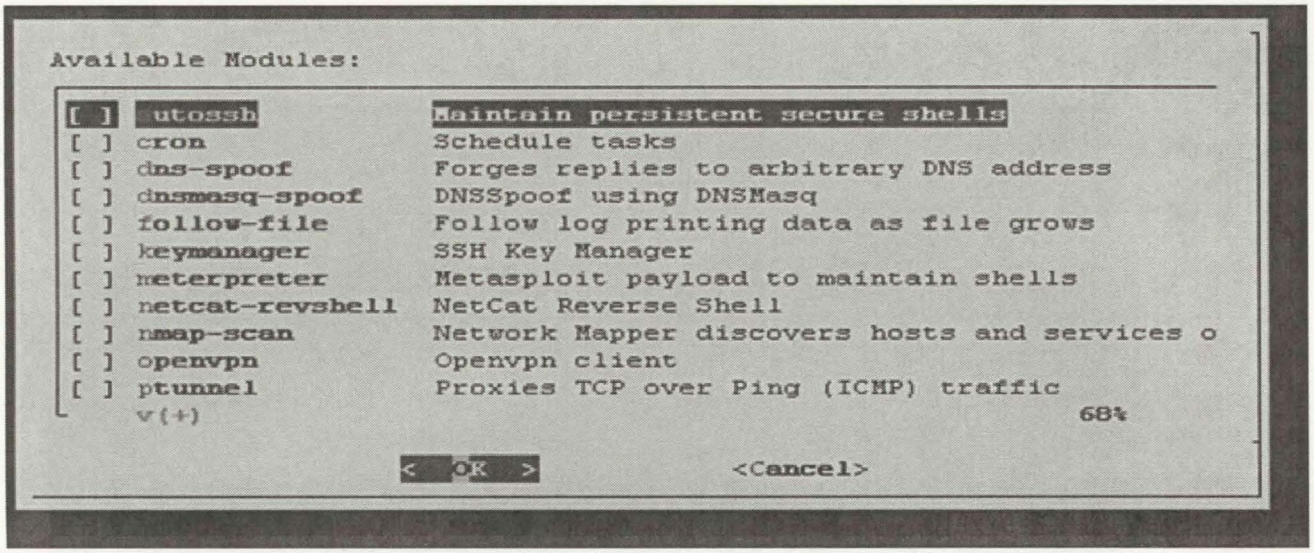
Mediante la implementación de dos técnicas de ataques físicos por medio de los puertos USB, se identifica información del concentrador, sistema operativo, configuraciones, procesador características de la plataforma.

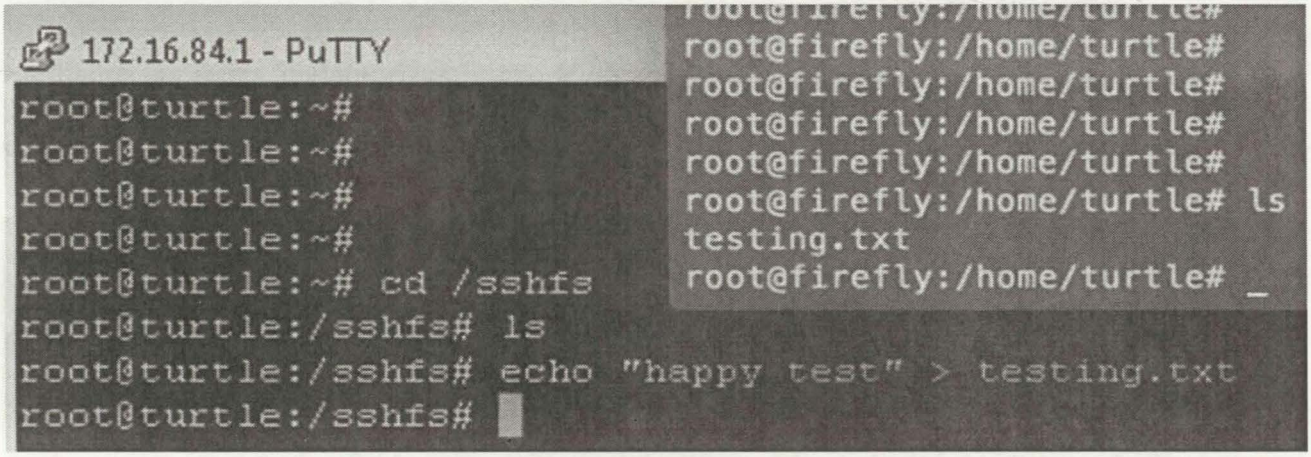
técnica explotación y web server remoto con la USB LAN TORTLE:



Configuración de módulos, interfaz lan a través del puerto USB y configuración de exploit para intentar acceder al sistema operativo del concentrador:







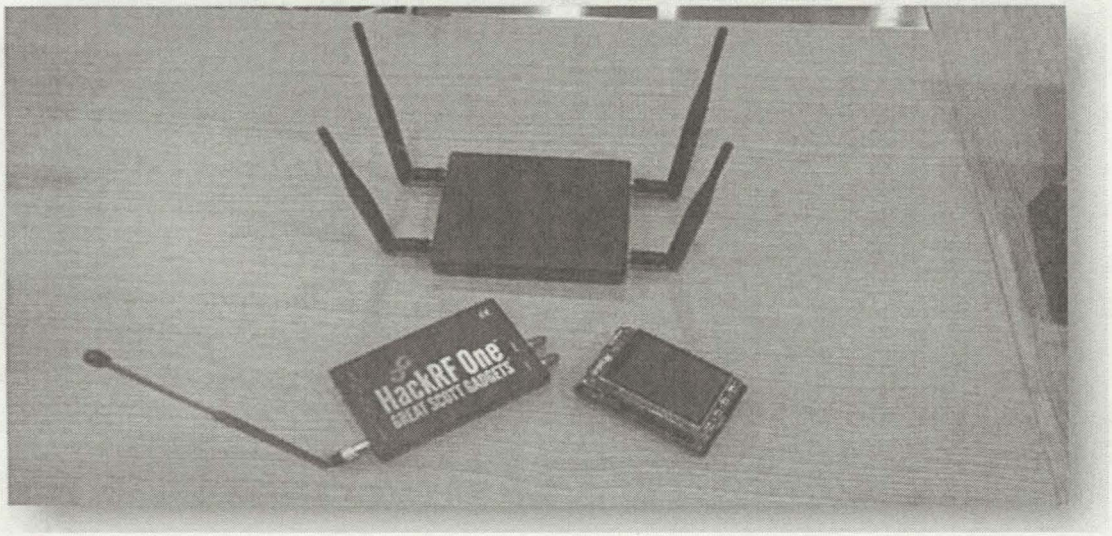
Es posible configurar el server con la conexión de la USB en el puerto USB del concentrador, sin embargo, no es posible conectar con el sistema operativo y se generan errores de comunicación y conexión, la prueba no es exitosa a nivel de explotación.

Pruebas de seguridad red wifi – concentrador

Herramientas Pen Testing HW:

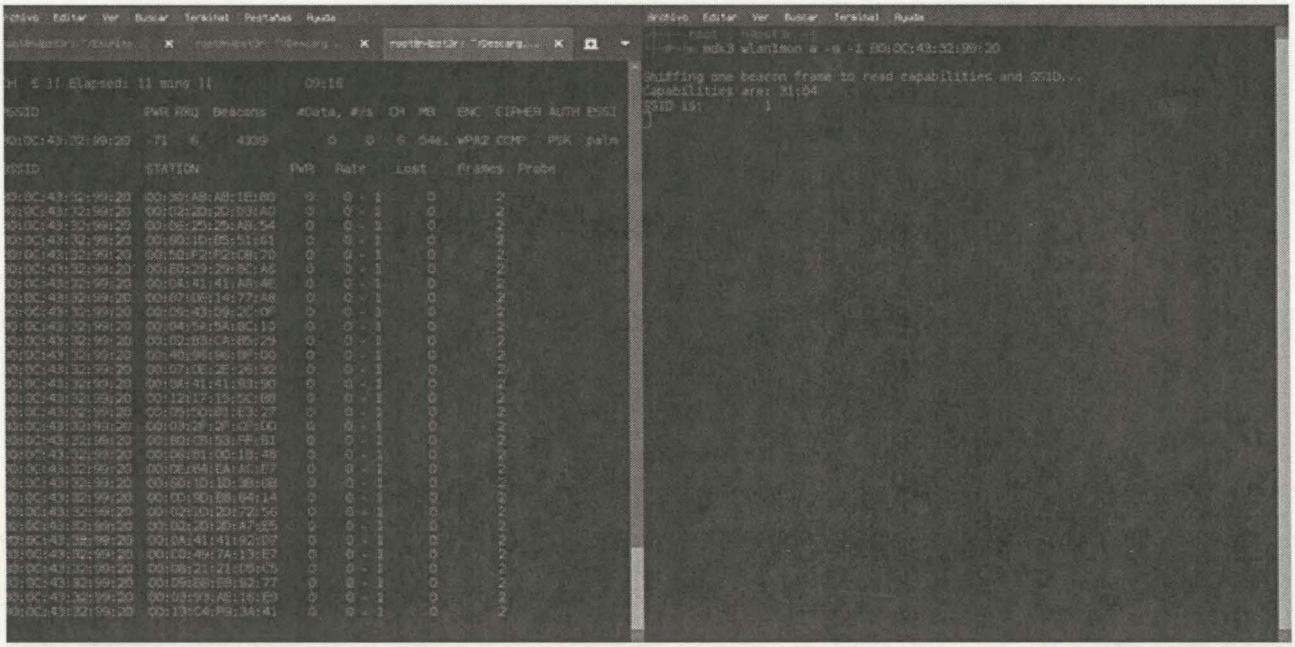
- Piña WiFi
- Antena WiFi
- Hackrf

- Rasperry



Mediante las redes inalámbricas, mapeos de señal se identifica la red WIFI Ciudad1, la cual corresponde a la emisión WIFI de la conexión hacia el concentrador AMS.

```
CH  6 ][ Elapsed: 12 s ][                09:05
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
B0:0C:43:32:99:20  -79 100      105        0    0   6  54e. WPA2 CCMP   PSK  palmira1
BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```



```
09:08:02  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|47 ACKs]
09:08:02  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|54 ACKs]
09:08:03  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|52 ACKs]
09:08:03  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:04  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 1|37 ACKs]
09:08:04  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|39 ACKs]
09:08:05  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|47 ACKs]
09:08:05  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:06  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|51 ACKs]
09:08:06  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 1|49 ACKs]
09:08:07  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 5|39 ACKs]
09:08:07  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|35 ACKs]
09:08:08  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|34 ACKs]
09:08:08  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|47 ACKs]
09:08:09  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:09  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|48 ACKs]
09:08:10  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|52 ACKs]
09:08:10  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|54 ACKs]
09:08:11  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 2|47 ACKs]
09:08:11  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:12  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|54 ACKs]
09:08:13  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:13  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:14  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|48 ACKs]
09:08:14  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|55 ACKs]
09:08:15  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|51 ACKs]
09:08:15  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|56 ACKs]
09:08:16  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|50 ACKs]
09:08:16  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|53 ACKs]
09:08:17  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|51 ACKs]
09:08:17  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|49 ACKs]
09:08:18  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|44 ACKs]
09:08:18  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|40 ACKs]
09:08:19  Sending 64 directed DeAuth. STMAC: [00:11:22:33:44:55] [ 0|41 ACKs]
```

```
# mdk3 wlan1mon a -m -i B0:0C:43:32:99:20

Sniffing one beacon frame to read capabilities and SSID...
Capabilities are: 31:04
SSID is:        1
```

Identificación de la configuración de la red WIFI: Sede1.

```
Bus 003 Device 063: ID 10c4:ea60 Cygnal Integrated Products, Inc. CP210x UART Bridge / myAVR mySmartUSB light
Device Descriptor:
  bLength                18
  bDescriptorType         1
  bcdUSB               1.10
  bDeviceClass            0 (Defined at Interface level)
  bDeviceSubClass         0
  bDeviceProtocol         0
  bMaxPacketSize0        64
  idVendor           0x10c4 Cygnal Integrated Products, Inc.
  idProduct          0xea60 CP210x UART Bridge / myAVR mySmartUSB light
  bcdDevice            1.00
  iManufacturer           1 Silicon Labs
  iProduct                2 CP2102 USB to UART Bridge Controller
  iSerial                 3 0001
  bNumConfigurations      1
  Configuration Descriptor:
    bLength                9
    bDescriptorType        2
    wTotalLength          32
    bNumInterfaces         1
    bConfigurationValue    1
    iConfiguration         0
    bmAttributes        0x80
      (Bus Powered)
    MaxPower             100mA
    Interface Descriptor:
      bLength              9
      bDescriptorType      4
      bInterfaceNumber     0
      bAlternateSetting    0
      bNumEndpoints        2
      bInterfaceClass    255 Vendor Specific Class
      bInterfaceSubClass   0
      bInterfaceProtocol   0
      iInterface           2 CP2102 USB to UART Bridge Controller
      Endpoint Descriptor:
        bLength            7
```

Se identifica las características del canal, SSID, tipo señal, frecuencias y datos de la red WIFI, se identifican configuraciones de seguridad de tipo WPA2.

```
Enter Action Selection: 14
Running: Fuzz Security Code Function
Current password:  \xaa\xbb\xcc\xdd\xee\xff\x00\x11\x22\x33\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
    Enter Y if you would like to use password list from file:
Not using password file.

   Logon as User Number. Hit enter for default.
   Enter number (0-65535):
Logging on as User:  2
Using login_setup which combines ident_setup and nego_setup
Sending: ident: \xee\x00\x00\x00\x00\x01\x20\x13\x10
read_response: did not receive ack byte:
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
```

Ataques de autenticación y desautenticación con la suite de AIRCRAK, antenas especializadas y Access Point Falsos:

```
Enter Action Selection: 1
Running: Test Negotiation Function

   Logon as User Number. Hit enter for default.
   Enter number (0-65535):
Logging on as User:  2
Sending: ident: \xee\x00\x00\x00\x00\x01\x20\x13\x10
read_response: did not receive ack byte:
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
read_response: did not receive ack byte:
    Sent NACK
read_response: did not receive ack byte:
```

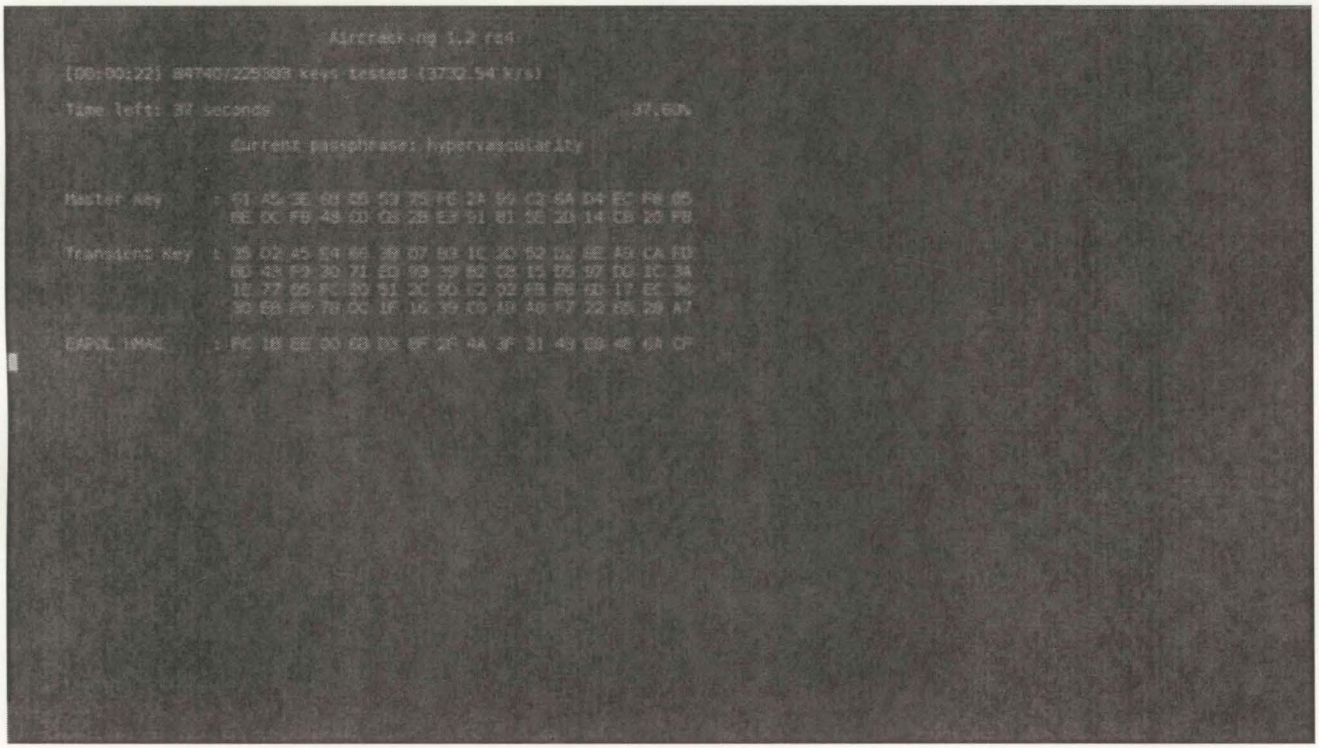
```
Module Options
==============

  Name             Value      Description
  ----             -----      -----------

termineter (get_info) > run
CRITICAL failed 3 times to correctly send a frame
[-] Caught C1218IOError: 'failed 3 times to correctly send a frame'
termineter (get_info) >
```

```
CH  6 ][ Elapsed: 5 mins ][                09:34 ][ WPA handshake: B0:0C:43:32:99:20

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B0:0C:43:32:99:20  -69 100     3002      187    0   6  54e. WPA2 CCMP   PSK  palmiral

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

B0:0C:43:32:99:20  48:51:B7:D6:09:4D  -76    1e- 6e     0      8999
```

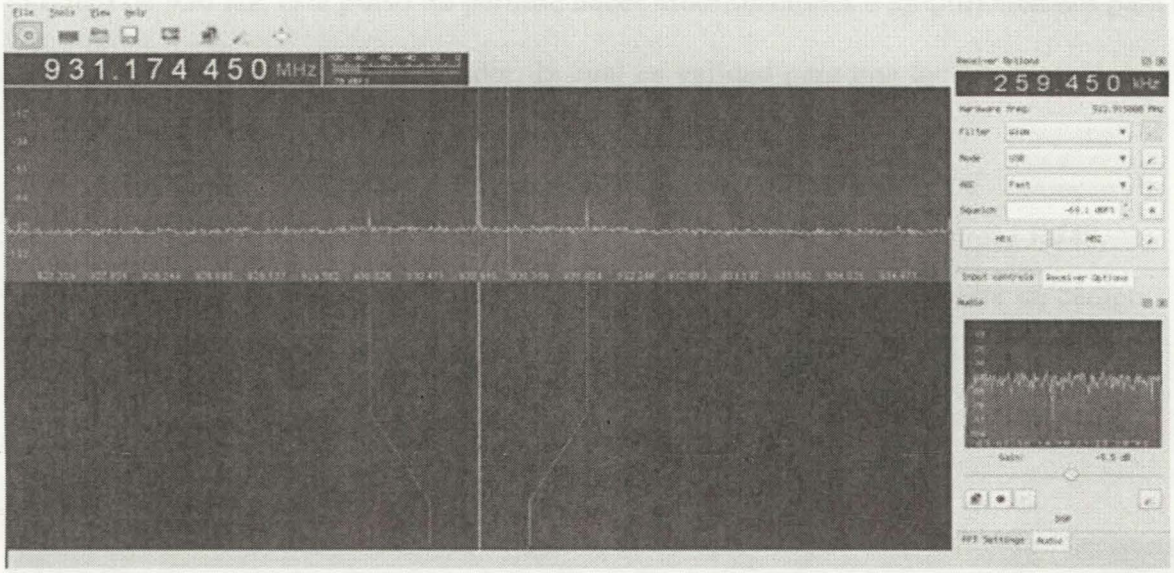
```
root@n4pst3r: ~ 168×22
09:34:01  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [25|57 ACKs]
09:34:02  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [20|56 ACKs]
09:34:02  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 6|58 ACKs]
09:34:03  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 8|55 ACKs]
09:34:03  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 6|55 ACKs]
09:34:04  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 5|54 ACKs]
09:34:04  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [14|45 ACKs]
09:34:05  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [13|54 ACKs]
09:34:05  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 8|49 ACKs]
09:34:06  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 0|55 ACKs]
09:34:07  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 9|38 ACKs]
09:34:07  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [12|53 ACKs]
09:34:08  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 6|53 ACKs]
09:34:08  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 9|53 ACKs]
09:34:09  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 7|45 ACKs]
09:34:09  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [11|56 ACKs]
09:34:10  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 2|57 ACKs]
09:34:10  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 4|57 ACKs]
09:34:11  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 3|32 ACKs]
09:34:11  Sending 64 directed DeAuth. STMAC: [48:51:B7:D6:09:4D] [ 6|53 ACKs]
```

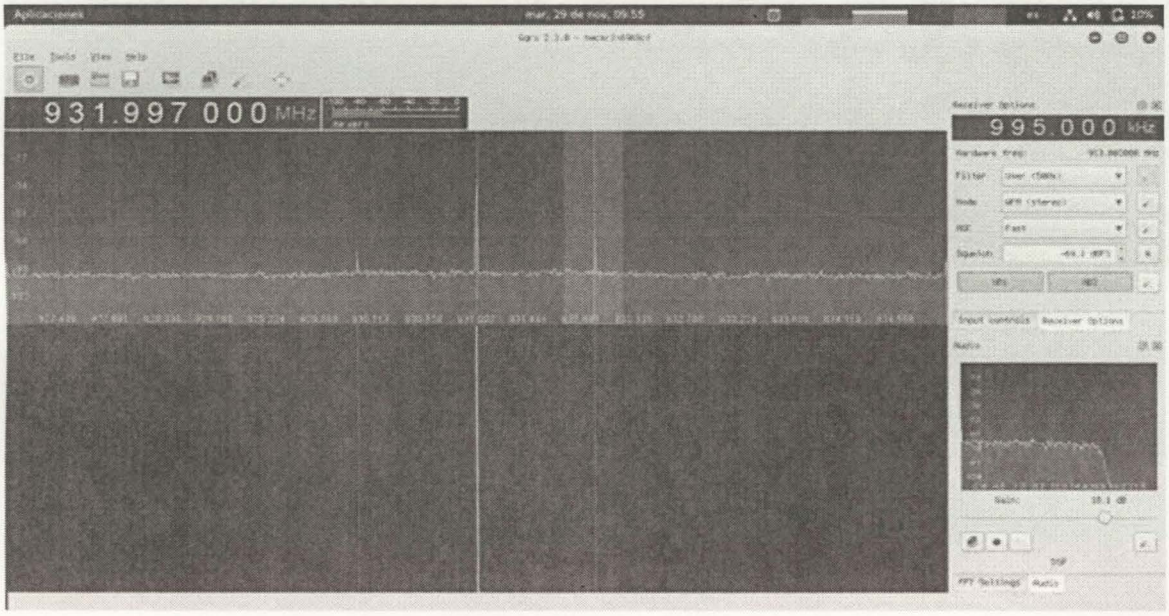
```
└──#─┤▶ aircrack-ng          -01.cap
Opening palmira1-01.cap
Read 27981 packets.

   #  BSSID              ESSID                     Encryption

   1  B0:0C:43:32:99:20                            WPA (1 handshake)

Choosing first network as target.

Opening palmira1-01.cap
Please specify a dictionary (option -w).
```

Ataques de criptoanálisis para identificación del password una vez obtenidas las llaves y los handshake wpa de la red WIFI, esta técnica requiere de procesamiento, tablas precocumputadas y procesamiento de las herramientas de un ciberatacante.



Pruebas de seguridad RF– Concentrador.





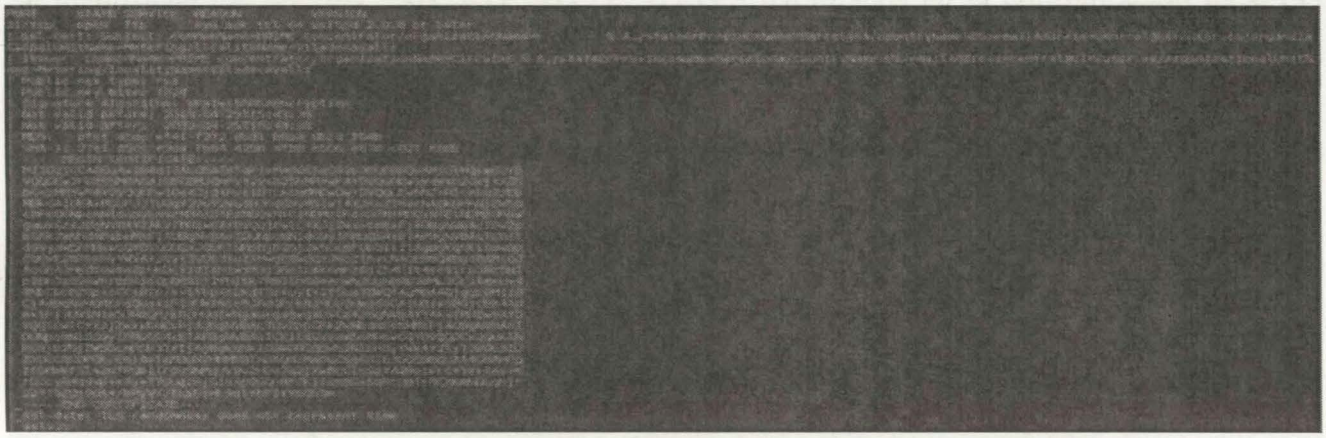
Mediante la implementación de HACKRF, solo se identifican un pulso de pequeña magnitud en el rango de 930 Hz, este pulso no permite hacer modificaciones o amplificaciones para modificar la señal RF que llega al concentrador, la cual es validad para una lectura a nivel de display del concentrador.

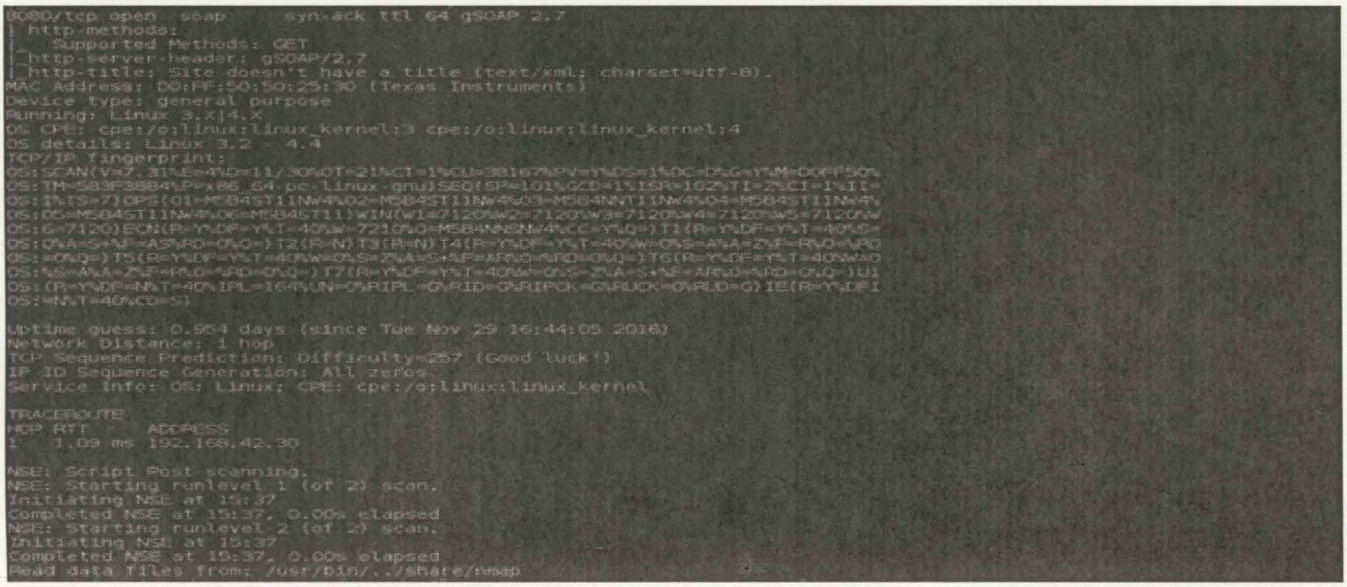
Pruebas locales desde la conexión serial – ethernet – modem /Ethernet / RJ45.

Conexión local mediante acceso LAN a Web Service de Concentrador en campo

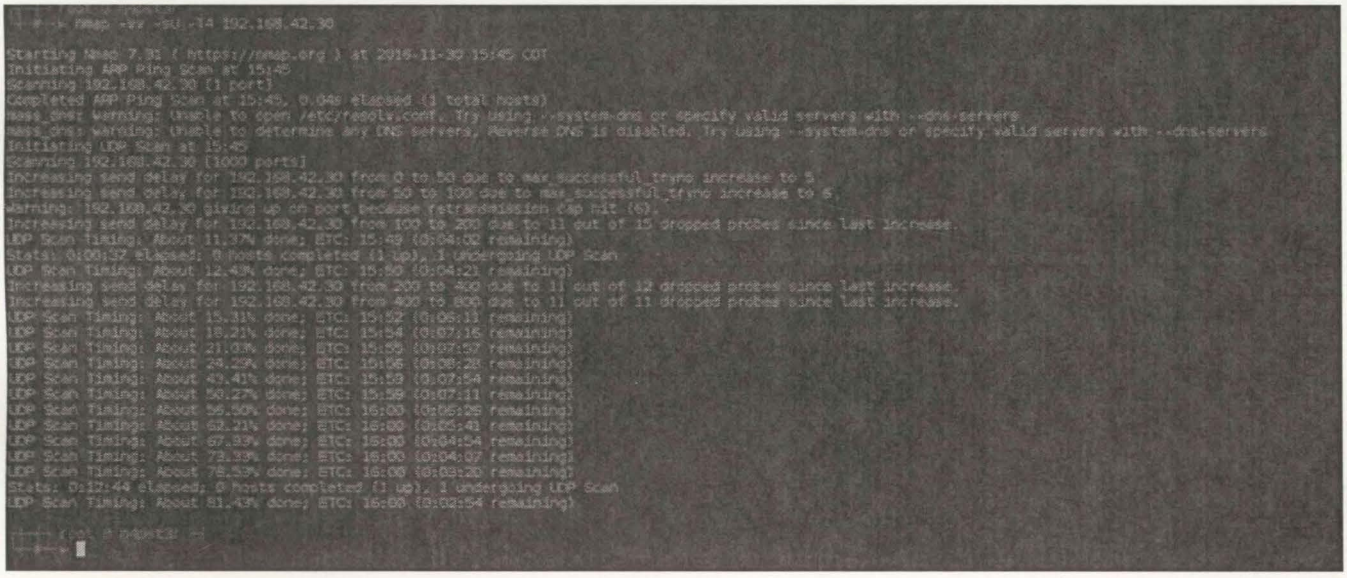
IP: 192.168.42.30 Mascara: 255.255.255.0 Host: N/A

Escáner de puertos y servicios remotos:



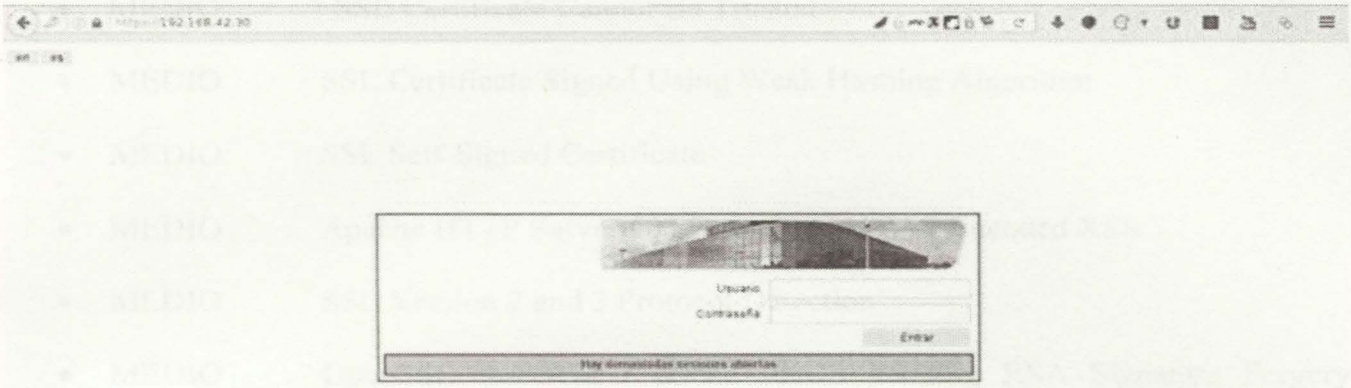


Se identifican los puertos SSH, FTP, HTTP, HTTPS habilitados en la configuración local del módulo de comunicaciones del concentrador.



No se identifican conexiones por protocolo ethernet en los medidores.

Puerto 80 y 443: identificación de la aplicación WEB interna del concentrador.



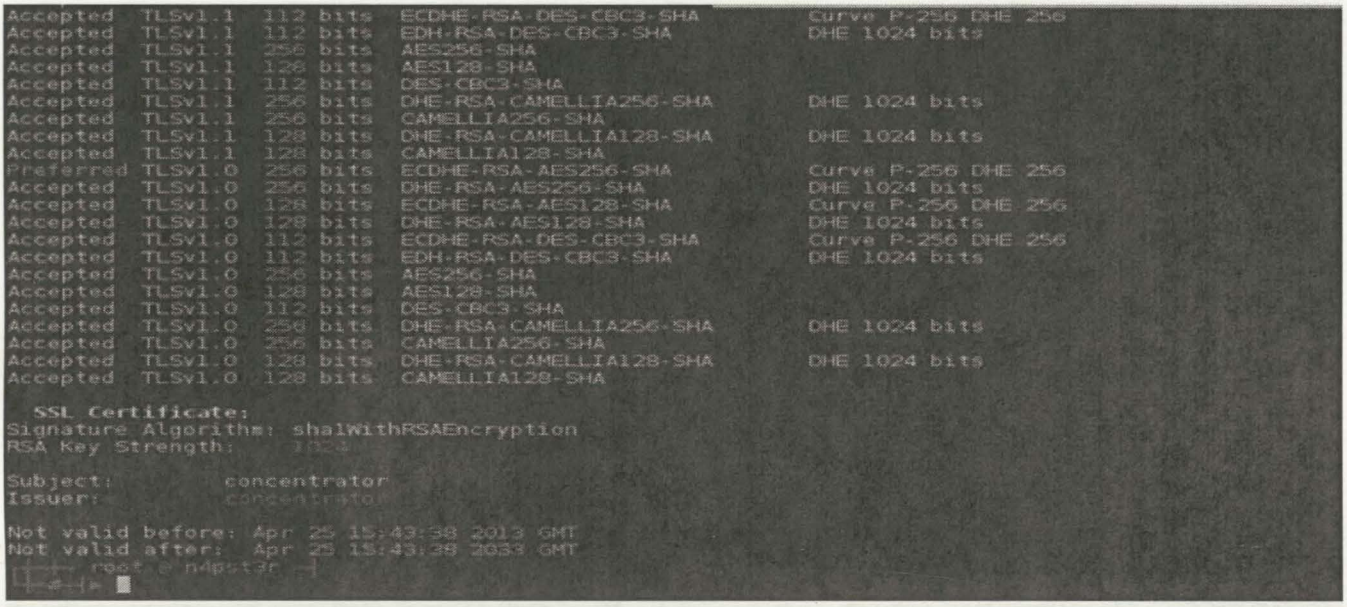
Mediante la ejecución de herramientas de escáner de vulnerabilidades como lo son (NESSUS, Acunnetix WEB Vulnerability, W3af, entre otras), se identifican vulnerabilidades de seguridad:

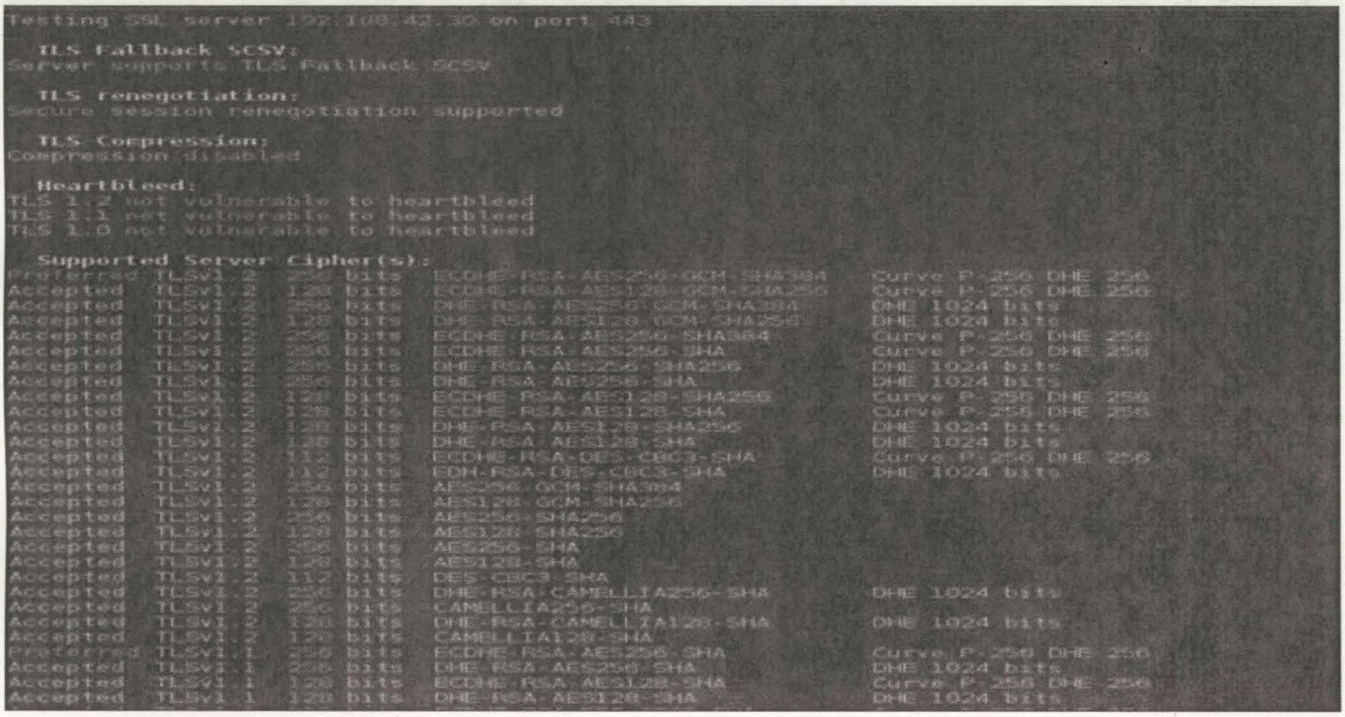
- Crítico Apache mod_proxy Content-Length Overflow
- Crítico OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities
- Crítico OpenSSL Unsupported
- Crítico PHP Unsupported Version Detection
- ALTO Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handling Overflow
- ALTO Apache mod_ssl ssl_engine_log.c mod_proxy Hook Function Remote Format String
- ALTO mod_ssl ssl_util_uuencode_binary Remote Overflow
- ALTO OpenSSL < 0.9.8f Multiple Vulnerabilities
- ALTO PHP < 5.3.12 / 5.4.2 CGI Query String Code Executio
- ALTO OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

- ALTO Unsupported Web Server Detection
- MEDIO " SSL Certificate Cannot Be Trusted
- MEDIO SSL Certificate Signed Using Weak Hashing Algorithm
- MEDIO SSL Self-Signed Certificate
- MEDIO Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
- MEDIO SSL Version 2 and 3 Protocol Detection
- MEDIO OpenSSL < 0.9.7k / 0.9.8c PKCS Padding RSA Signature Forgery Vulnerability
- MEDIO PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
- Bajo SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- Bajo SSH Server CBC Mode Ciphers Enabled
- Bajo SSH Weak MAC Algorithms Enabled

Se identifican múltiples vulnerabilidades asociadas a servicios y configuraciones desactualizadas:

- Nivel del código PHP desactualizado.
- Servidor WEB APACHE desactualizado.
- Configuraciones con los certificados SSL identificados en la aplicación WEB desactualizadas.
- Configuraciones con los certificados OpenSSL identificados en la aplicación del servicio SSH desactualizadas.



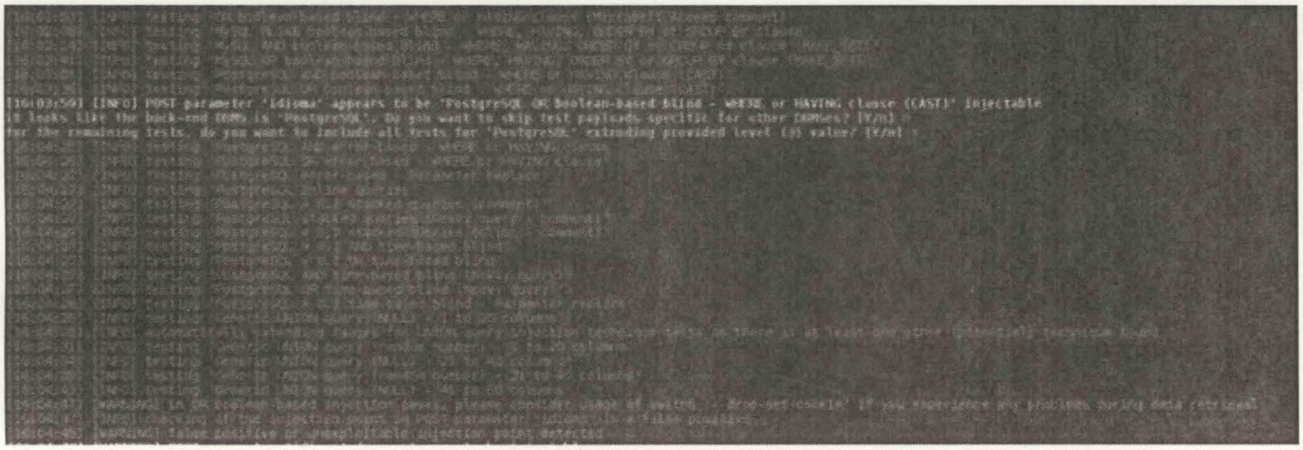


Servicio SSH identificado:

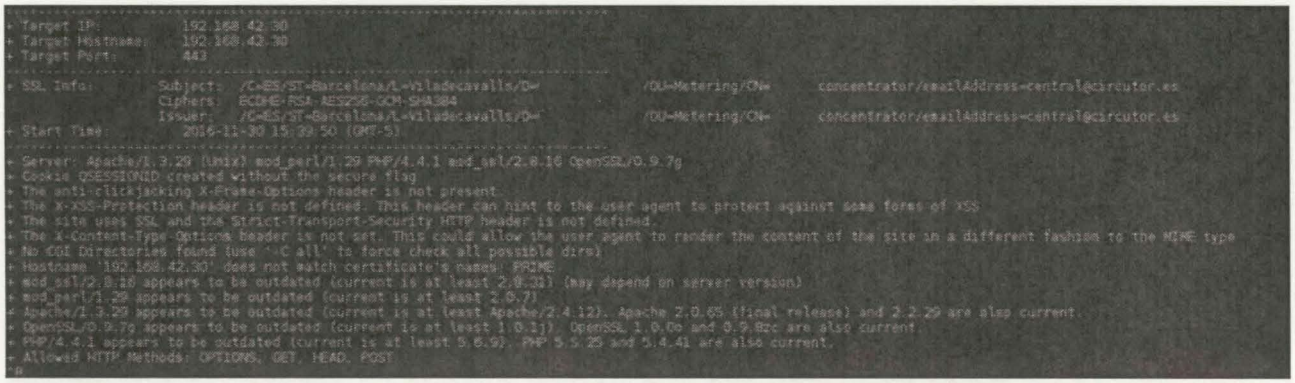
```
└─#─▶ ssh 192.168.42.30
The authenticity of host '192.168.42.30 (192.168.42.30)' can't be established.
RSA key fingerprint is SHA256:05V1qsXAFGnEg6lElRD7SewwuDtsbHTfRgtXiYQbaxc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.42.30' (RSA) to the list of known hosts.
root@192.168.42.30's password:
Permission denied, please try again.
root@192.168.42.30's password:
Permission denied, please try again.
root@192.168.42.30's password:
Permission denied (publickey,password).
```

No es posible obtener acceso con credenciales por defecto y ataques de password defecto, passsword cracking en el tiempo del desarrollo de la prueba.

Posibles Inyecciones SQL a la aplicación WEB del Concentrador:



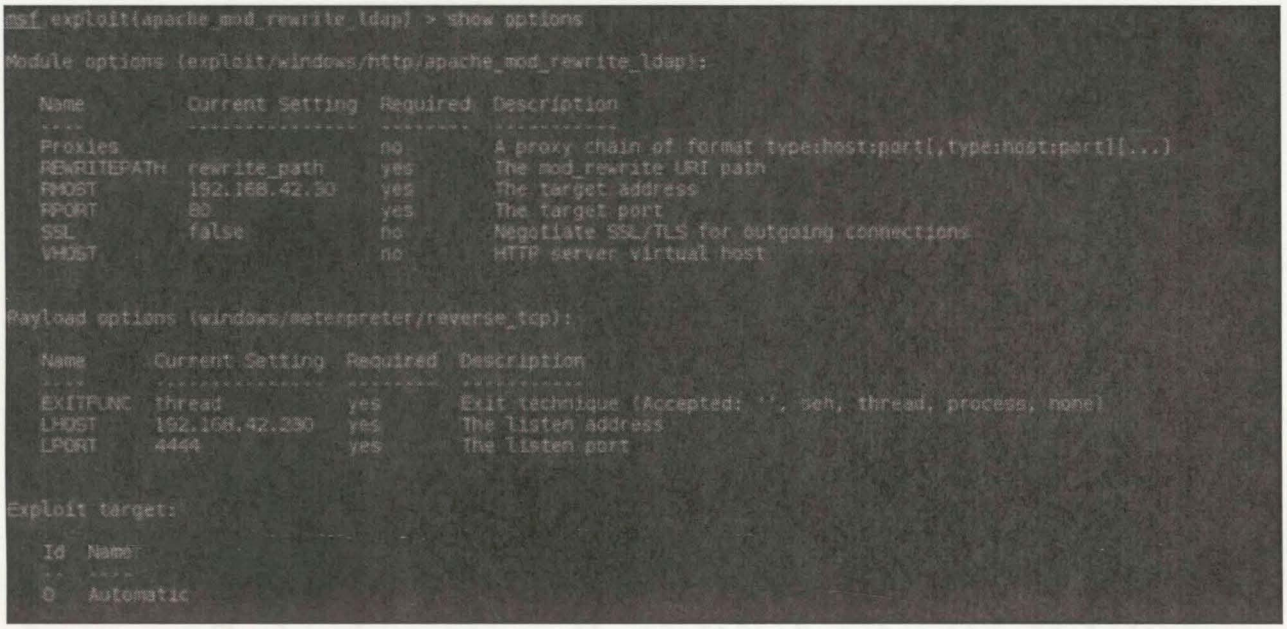
Mediante la herramienta SQLMAP, se ejecutan inyecciones de código SQL a la aplicación WEB de gestión del concentrador, se identifica la existencia de las debilidades y con más recursos y tiempos es posible que la aplicación pueda revelar información a través de inyecciones SQL.



Mediante inyecciones SQL, es posible identificar información de los siguientes componentes:

- Base de datos
- Métodos HTTP de la aplicación (Trace, Options, etc).
- PHP versiones, OpenSSL, etc.
- Información de la plataforma.
- Otro tipo de información confidencial.

Explotación de Vulnerabilidades: Metasploit , Armitage, etc.



```
msf exploit(apache_mod_rewrite_ldap) > show options

Module options (exploit/windows/http/apache_mod_rewrite_ldap):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   REWRITEPATH  rewrite_path     yes       The mod_rewrite URI path
   RHOST        192.168.42.30    yes       The target address
   RPORT        80               yes       The target port
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                         no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.42.230   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

En la anterior evidencia se identifica la posibilidad de inyectar exploit que puedan aprovechar la debilidad de las configuraciones desactualizadas de los componentes de la prueba de seguridad, esta explotación se desarrolla a través del puerto 80 y configurar un backdoor en el web services del concentrador.

Otro tipo de técnicas se puedan desarrollar desde la red internet y desde la conexión local al concentrador en campo.

Anexo 2. Requisitos de ciberseguridad para los concentradores instalados sobre una infraestructura de medición avanzada en una empresa de energía en Colombia

3.1 AUTENTICIDAD G

No.	Nombre	Requisito	NIST	NERC	62443	NTC 6079
1.3	Requisitos de control de acceso y uso	Los usuarios del sistema deben ser autenticados y autorizados para acceder solo a los componentes del sistema para los que tienen derecho de acceso. Por ejemplo, la autenticación fuerte es necesaria para los comandos críticos (como el comando de desconexión).	Control de Acceso (PR.AC)	CIP-002: Definición de ciber activos críticos	62443-2-1:2009 4.3.3.4	6.1.5: Requisitos de desconexión y conexión
5.2	Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el CGM	Verificar que la clave sea única por nivel de acceso en cada medidor/concentrador.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11	6.5.4: Requisitos de control de acceso, integridad y confidencialidad de datos
6.1.1	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Control de Acceso Electrónico. Verificar que todo acceso electrónico al concentrador de medida, así sea localmente a través de un panel de control o físicamente a través de un puerto de comunicación/diagnóstico con un conjunto de pruebas o un computador personal o remotamente a través de medios de comunicación, sean protegidos por una identificación de usuario único (ID) y combinaciones de contraseñas. Una vez que el usuario ha configurado una combinación apropiado, no será posible tener acceso al dispositivo sin una la combinación del ID/contraseña generado por el usuario.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11	6.5.4: Requisitos de control de acceso, integridad y confidencialidad de datos
6.3.1	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Construcción de Contraseña. Verificar que las contraseñas creadas sigan un conjunto de reglas a las cuales deberán adherirse en la creación de cada contraseña. Validar que use como mínimo ocho caracteres y la contraseña sea sensible a mayúsculas y minúsculas. Al momento de codificar en texto común, las contraseñas deben contener los siguientes caracteres.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
		· Por lo menos una letra mayúscula y una minúscula	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
		· Por lo menos un número	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
		· Por lo menos un carácter no alfanumérico (ej. @, %, &, *)	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
6.3.2	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Construcción de Contraseña. Verificar que cualquier intento de crear una contraseña que infrinja las normas descritas en el requisito anterior, será capturado al momento del intento de creación y el usuario será notificado.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
6.5	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Visualización de Contraseña. Verificar que sólo se podrá visualizar la identificación de los usuarios en las pantallas, logs, área de memoria o archivos, y otros archivos de registro y configuración. No será posible visualizar las contraseñas de los concentradores de medida por cualquier medio, incluyendo pantallas de visualización local, software de configuración (local o remota, en línea y fuera de línea), navegador y acceso al terminal.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
6.12	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Autenticación. Verificar que se tenga un medio para verificar que el software de configuración siendo usado para tener acceso o cambiar la configuración, es una aplicación que ha sido autorizada por el proveedor/fabricante. Se debe evitar que se usen copias no autorizados para acceder a cualquiera de sus características.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
6.14	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Control de Identificación/Contraseña. Verificar que el software de configuración es controlado por una identificación/contraseña para que no se pueda acceder al software sin la propia combinación de ellos. Bajo ninguna circunstancia debe el software de configuración permitir que las contraseñas del software o del concentrador/medidor sean legibles como texto.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.2: Requisitos de control de acceso y de uso
8.1.2	Condiciones mínimas de Ciberseguridad para el software de gestión – Controles de Acceso	Autenticación de acceso. Verificar que ninguna de las credenciales del sistema puedes ser transmitida en texto claro. El sistema no debe proveer mecanismos de autocompletado o permitir usuarios anónimos.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.4: Requisitos de control de acceso, integridad y confidencialidad de datos

3.2 AUTORIZACIÓN						
No.	Nombre	Requisito				
6.4	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Autorización de Control de Acceso basado en Roles. Verificar que el concentrador tenga la capacidad de definir roles, definidos por el usuario. Cada rol tendrá la capacidad de tener cualquier combinación de diferentes funciones asignadas a este rol. Un rol se asignará a cada combinación de usuario/contraseña, así otorgando los permisos de dicho rol al usuario en el momento de ingresar.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	62443-2-1:2009 4.3.3.4	6.5.4: Requisitos de control de acceso, integridad y confidencialidad de datos
3.3 DISPONIBILIDAD						
No.	Nombre	Requisito				
4.1	Requisitos de disponibilidad de los recursos	Verificar que todas las partes del sistema estén bajo supervisión, administración y control, en la supervisión del comportamiento del sistema se deben detectar situaciones anormales y algunas acciones automáticas para contrarrestarlas, deben ser posibles.	Monitoreo Continuo de Seguridad (DE.CM)	CIP-009: Planes de recuperación para ciber activos críticos.	ISA 62443-3-3:2013 SR 6.1	6.5.5: Requisitos de disponibilidad de recursos
5.6	Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el CGM	Sincronización. Verificar que se garantice la sincronización de la hora local de los medidores en sitio, o de manera remota a través del CGM.	Monitoreo Continuo de Seguridad (DE.CM)	CIP-009: Planes de recuperación para ciber activos críticos.	ISA 62443-3-3:2013 SR 3.2	6.5.5: Requisitos de disponibilidad de recursos
8.5	Condiciones mínimas de Ciberseguridad para el software de gestión – Monitorización de Acceso y Estado de Seguridad	Monitorización de componentes. Verificar que solución cuente con mecanismos para monitorizar los eventos de los componentes que estén relacionados con Ciber Seguridad, en modalidad (7x24x365). Las herramientas deberán emitir alertas automatizadas que permitan detectar e informar incidentes de seguridad.	Monitoreo Continuo de Seguridad (DE.CM)	CIP-009: Planes de recuperación para ciber activos críticos.	ISA 62443-3-3:2013 SR 3.2	6.3.3: Requisitos de gestión de eventos y alarmas
3.4 INTEGRIDAD						
No.	Nombre	Requisito				
2.1	Requisitos de integridad de datos	Verificar que el sistema sea capaz de garantizar la integridad de los datos intercambiados en todo momento. Es necesario asegurarse de que los datos no son modificados por cualquier entidad no autorizada durante la comunicación o el acceso a los datos. Para esto, se debe implementar algoritmos de encriptación.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	6.5.3: Requisitos de integridad de datos
2.3	Requisitos de integridad de datos	Verificar que el sistema cuenta con la capacidad de implementar un mecanismo anti-repetición (replay). Este mecanismo es necesario para evitar la repetición de mensajes para los comandos críticos, tales como desconexión, alarma, etc.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	6.5.3: Requisitos de integridad de datos
2.5	Requisitos de integridad de datos	Verificar que el sistema permita la utilización de mecanismos de control clásicos (incluyendo fecha y hora o la numeración con el vector inicial) para garantizar la identificación de cada mensaje y su singularidad.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	6.5.3: Requisitos de integridad de datos
5.5	Condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el CGM	Pérdida de comunicación remota. Verificar que en el caso de que no se disponga de comunicación remota, se deberá contar con una funcionalidad para que una vez se realice la interrogación local del medidor a través del software propietario o de terceros, se permita el cargue de la información del archivo descargado en sitio al CGM, generando la respectiva trazabilidad del evento en el sistema (registro en medidor y CGM).	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	6.3.3: Requisitos de gestión de eventos y alarmas
6.7	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Perfil de auditorías de Logs. Verificar que el concentrador de medida registrará, en un búfer circular secuencial (primero ingresa, primero sale), un registro de logs o históricos en el orden en que ocurran. No existirá la posibilidad de borrar o modificar estos logs, ya que debe guardar completamente y mantener la integridad para los propósitos de auditoria y comprobación.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2	6.3.3: Requisitos de gestión de eventos y alarmas
6.8	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Capacidad de almacenamiento. Verificar que los Logs deberán almacenar por lo menos 2048 eventos antes de que la memoria empiece a sobrescribir los eventos más antiguos con los eventos más nuevos. No será posible quitar el soporte de almacenamiento de los logs sin dañar permanentemente el concentrador de medida más allá de poder ser reparado.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.3.3: Requisitos de gestión de eventos y alarmas
6.9	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Registro de Almacenamiento. Verificar que por cada evento de log, se registrará la siguiente información:	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.3.3: Requisitos de gestión de eventos y alarmas
6.9.1		Número de registro de Evento: El número de secuencia del el evento generado automáticamente.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10	6.3.3: Requisitos de gestión de eventos y alarmas
6.9.2		Hora y Fecha: Hora y Fecha del evento, incluyendo año, mes, día, hora, minuto, y segundo.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10	6.3.3: Requisitos de gestión de eventos y alarmas
6.9.3		Identidad del usuario: La identificación del usuario ingresada en el concentrador de medida en el momento del evento.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10	6.3.3: Requisitos de gestión de eventos y alarmas
6.9.4		Tipo de Evento y alertas: El proveedor del concentrador de medida deberá listar los tipos de eventos y alertas que almacena en logs e históricos.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-2-1:2009 4.3.2.6.7	6.3.3: Requisitos de gestión de eventos y alarmas

6.10	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Características Específicas Criptográficas. Verificar que para los medidores o concentradores que implementan funciones de comunicación específicas sobre redes basadas en IP, se implementan las siguientes técnicas criptográficas y versiones en estos:	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.10.1		a) La funcionalidad del servidor Web suministrada por debe ser de Hypertext Transfer Protocol Secure (HTTPS).	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.10.2		b) La funcionalidad de transferencia de archivos suministrada por el medidor y/o concentrador debe ser Secure File-Transfer Protocol (SFTP).	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.10.3		c) Comunicación orientado a texto usando una conexión de terminal virtual sobre una red de Ethernet debe ser secure shell (SSH).	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.10.4		d) Single Network Management Protocol (SNMP), implementado en el IED debe ser SNMPv3.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.10.6		f) Funcionalidad de túnel seguro suministrado por el medidor y/o concentrador debe ser una red privada virtual (virtual private network (VPN))	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
6.11.1	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Técnicas Criptográficas. Verificar que una o más de las técnicas a continuación pueden ser implementadas en los dispositivos:	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.8	6.4.1: Requisitos generales de comunicaciones
		a) Cifrado en bloque	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		b) Firmas digitales	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		c) Autenticación de entidad	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		d) Funciones de derivación de clave	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		e) Autenticación de mensaje	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		f) Creación de números aleatoria	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		g) Hash seguro	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.3: Requisitos de integridad de datos
		h) Establecimiento de clave	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.2: Requisitos de control de acceso y de uso
6.11.2	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Técnicas Criptográficas. Verificar que para los medidores y para los concentradores que ofrezcan alguna de las características criptográficas mencionadas en el requisito anterior, cumplan con los requisitos especificados por la División de Seguridad Informática NIST. Como las técnicas y versiones de técnicas pueden cambiar como consecuencia de los nuevos descubrimientos, avances en tecnología y amenazas, los concentradores deben cumplir con los requisitos actuales en el momento de su fabricación.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.5.2: Requisitos de control de acceso y de uso
6.17	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Garantía de Calidad de Firmware. Verificar que la garantía de calidad de firmware debe cumplir con IEEE Std C37.231, sobre recomendaciones de prácticas para el control de equipos de firmware con protección de microprocesador.	Seguridad de Datos (PR.DS)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.4, SR 4.1	6.4.1: Requisitos generales de comunicaciones

3.5 CONFIDENCIALIDAD						
No.	Nombre	Requisito				
1.3	Requisitos de control de acceso y uso	Verificar que el sistema sea capaz de gestionar los derechos de acceso a cualquiera de sus componentes.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8	6.5.2: Requisitos de control de acceso y de uso
3.2	Requisitos de control de acceso, integridad y confidencialidad	Verificar si el sistema permite la utilización de "certificados" para activar las funciones de seguridad.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8	6.5.2: Requisitos de control de acceso y de uso
6.2.1	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Mecanismos de Vulneración de Contraseñas. Verificar que el concentrador de medida no tenga ningún medio, no divulgado a la organización, donde el control de identidad/contraseña creado por el usuario pueda ser vulnerado. Esto incluye, pero no está limitado a los siguientes mecanismos y técnicas:	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
		• Contraseña maestra incorporada	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
		• Rutina de diagnóstico de algún chip integrado que se ejecuta automáticamente en el evento de la falla del hardware o software	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
		• Derivación de hardware de contraseñas, tales como configuración de dip switches.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
6.6	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Acceso de Tiempo de Espera. Verificar que el concentrador de medida tenga un mecanismo que automáticamente terminará una sesión de inicio por un usuario después de un periodo determinado de inactividad por el usuario. Se define la inactividad como la falta de entrada por mecanismos locales (pantalla) y/o la falta de actividad en el teclado de un computador conectado al puerto del concentrador de medida. El periodo de tiempo antes que se activa el mecanismo de tiempo de espera será ajustable por el usuario, entre 1 minuto y 60 minutos en intervalos de 1 minuto.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
6.10.5	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	e) Uso de Network Time Protocol (NTP). La funcionalidad de sincronización de tiempo de red debe ser implementado por NTP v3/4 o SNTP 3/4.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
6.13	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Firma Digital. Verificar que el software de configuración del fabricante tenga la capacidad de generar una firma digital en la descarga de archivos de configuración y firmware, indicando que el archivo ha sido generado por un programa de configuración de software autorizada y por un usuario autorizado. El concentrador/medidor debe tener la capacidad de leer la firma digital aplicada a un archivo de configuración o firmware para verificar que el archivo ha sido creado por una entidad autorizada y que no ha sido alterado o corrupto. El concentrador/medidor solo aceptará archivos firmados adecuadamente.	Control de Acceso (PR.AC)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
6.16.1	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Acceso al puerto de comunicación. Verificar que todos los puertos de comunicación, así sean físicos o lógicos, excepto por el puerto de diagnóstico del concentrador de medida o medidor AMI, tendrán la capacidad de habilitarse o inhabilitarse a través de la configuración de estos dispositivos. Cuando se inhabilita por medio de la configuración, se imposibilita la comunicación a través del puerto inhabilitado.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	6.4.1: Requisitos generales de comunicaciones
6.16.2	Características de Ciberseguridad de un Medidor inteligente o Concentrador de medida	Acceso al puerto de comunicación. Verificar que los medidores AMI y/o concentradores AMI tendrán inhabilitados todos los puertos con User Datagram Protocol (UDP) y Transmission Control Protocol (TCP), que no están siendo usados por una aplicación o que permita su deshabilitación.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6	6.4.1: Requisitos generales de comunicaciones
8.2	Condiciones mínimas de Ciberseguridad para el software de gestión – Controles de Acceso	Verificar que se hayan implementado mecanismos para el control de acceso en todos los puntos de acceso del Perímetro de Seguridad Electrónica, garantizando al menos los siguientes criterios:	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
		a) Denegar los accesos que vienen configurados por defecto, de manera que los permisos de acceso se deban especificar explícitamente.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.5.2: Requisitos de control de acceso y de uso
		b) Aplicar y mantener un mecanismo para asegurar el acceso telefónico a los Perímetros de Seguridad Electrónica.	Control de Acceso (PR.AC)	CIP-005: Perímetros de seguridad electrónica	ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9	6.1.1.1: Requisitos eléctricos
8.4	Condiciones mínimas de Ciberseguridad para el software de gestión – Monitorización de Acceso y Estado de Seguridad	Registros de auditoría. Verificar que los sistemas, aplicaciones y demás elementos que conformen la solución de gestión, deberán generar registros o pistas de auditoría de las actividades de acceso de las cuentas de usuario, tanto fallidas como exitosas.	Mejoras (RC.IM)	CIP-003: Controles en la gestión de seguridad e información	ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10	6.1.2: Requisitos de operación y mantenimiento local

Referencias

62443-1-1. (2015). Security for Industrial Automation and Control Systems. 13.

Alan T. Murray, T. G. (2007). Introduction. In A. T. Murray, T. H. Grubesic, A. T. Murray, & T. H. Grubesic, *Critical Infrastructure: Reliability and Vulnerability* (p. 2). Berlin, Heidelberg: Springer Berlin Heidelberg.

CCI. (2018). Organización de la Ciberseguridad Industrial. *Estudio sobre la ciberseguridad industrial en Colombia*, 11-14-16-19-20.

CCI, C. d. (2016). Prólogo. *Estudio sobre la Ciberseguridad Industrial en Colombia*, 8.

CE13, C. d. (2008). Directiva 2008 /114/CE del Concejo. *Diario Oficial de la Unión Europea*, 2.

CERTSI, C. d. (2015, Agosto 25). *Instituto Nacional de Ciberseguriad de España S.A.* Retrieved from https://www.certsi.es/blog/iec62443-evolucion-isa99

CERTSI, C. d. (2017). Protocolos y puntos de análisis. *Guía de Seguridad en Protocolos Industriales Smart Grid*, 7-23.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *computers & s e c u r i t y 56*, 2.

CIER_Edenor, C. d. (2018). Caso EDENOR, Argentina. *CIER Comisión de Integración Energetica Regional*, 7-8.

CIER_ONS, C. d. (2018, Octubre 25). CIER, Brasil, caso ONS. *CIER Comisión de Integración Energetica Regional*, 14. Retrieved from http://www.cier.org/es-uy/Paginas/Ciberseguridad-evento.aspx

CNO1004. (2017). Acuerdo 1004. In C. N. Operación. Bogotá: Concejo Nacional de Operación.

CNO1043. (n.d.). Acuerdo 1043. In C. N. Operación. Bogotá: Concejo Nacional de Operación.

CNO701. (2014). Acuerdo 701. In C. N. Operaciones. Bogotá: Concejo Nacional de Operaciones.

CNO788. (2015). Acuerdo 788. In C. N. Operación. Bogotá: Concejo Nacional de Operación.

CONPES 3701, M. (2011, Julio 23). Lineamientos de política para la Ciberseguridad y Ciberdefensa. *MINTIC GOBIERNO DE COLOMBIA*, 39. Retrieved from https://www.mintic.gov.co/portal/604/w3-article-3510.html

DLMS/COSEM, U. A. (2018, Julio 2). *DLMS/COSEM – Meter data exchange for all energies*. Retrieved from http://www.dlms.com/index2.php

ESDEGUE, E. S. (2019). La Seguridad en el ciberespacio un desafio para Colombia. Bogotá: Escuela Superior de Guerra.

Foreman, J. C., & Gurugubelli, D. (n.d.). Cyber Attack Surface Analysis of Advanced Metering Infrastructure. *School of Engineering Technology;* , 1.

G3-PLC, A. (2018, Julio 7). *G3-PL, Alliance*. Retrieved from http://www.g3-plc.com/

GRP, W. E. (2018). The Global Risk Landscape 2018. *The Global Risks Report 2018, 13th Edition*, 3.

Hathaway, M. (2018). Comprender el riesgo cibernético. *OEA, Gestión del riesgo cibernético nacional*, 15-16.

Hawk C., & Kaushiva A. (2014). Cybersecurity and the Smarter Grid. *The Electricity Journal*, 84-95.

ICCN, C. C. (2017, Noviembre 21). Infraestructuras Críticas Cibernéticas en Colombia. *Comando Conjunto Cibernético*, 4. Retrieved from https://www.ccoc.mil.co/ciberdefensa/maquetacion/biblioteca_publica/catalogo_nacional_infraestructuras_285

IMSYS, I. M. (2018, Julio 2). *Integrated Measurement Systems*. Retrieved from http://imsys.com.co/

INCIBE. (2015). IEC62443: Evolución de la ISA 99. *INCIBE*, 2.

ISO / IEC 27019, I. O. (2017, Octubre). Information technology - Security techniques - Information security management guidelines based on ISO 27002 for process control systems specific to energy utility industries. In I. O. Standardization, *ISO IEC 27019* (p. 1). Switzerland: International Organization for Standardization. Retrieved from https://www.iso.org/standard/68091.html

ISO 27001, I. (2013, Octubre). Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. In ICONTEC, *Norma Técnica Colombiana NTC-ISO-IEC 27001* (pp. 1-34). Bogotá: ICONTEC. Retrieved from https://www.iso.org/standard/54534.html

ISO/IEC 27002, I. O. (2015, Ocrubre). Information technology — Security techniques — Code of practice for information security controls. In ICONTEC, *International Organization for Standardization* (pp. 1-114). Bogotá: ICONTEC. Retrieved from https://www.iso.org/standard/54533.html

ISO27000, I. (2012). Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2.

K. C. Budka, J. G. (2014). Architecture Framework. In J. G. K. C. Budka, *Communication Networks for Smart Grids* (p. 151). New Providence, United States: Alcatel-Lucent (United States).

LEY1273. (2009). Artículo 269E. USO DE SOFTWARE MALICIOSO. *LEY 1273 DE 2009*, 2.

Meters and More, M. a. (2018, Julio 2). *meters and more open technologies*. Retrieved from http://www.metersandmore.com/about-us/?#aboutus

Microsoft-OEA. (2018). Resultados destacados de la encuesta. *Protección de la infraestructura crítica en América Latina y el Caribe*, 25-26.

MINMINAS. (2018, Enero 29). Res. 40072 dle Ministerio de Minas y Energía. 4. Retrieved from https://www.minminas.gov.co/normatividad?idNorma=47695

MINMINAS, M. D. (2018). *RESOLUCIÓN 40072 DE 29 DE ENERO DE 2018*, 1.

Miyashita, M., & Takada, J. (2013). Characteristics of AMI using DLMS/COSEM and IEEE 802.15.4g Multi-hop Wireless Communication. *2013 IEEE International Conference on Smart Grid Communications*, 324-329.

Neetesh Saxena1, B. J. (2017). Secure and Privacy-Preserving Concentration of Metering Data in AMI Networks. *IEEE ICC 2017 SAC Symposium Communications for the Smart Grid Track*, 1.

NERC, N. A. (2012). *North American Electric Reliability Corporation*. Retrieved from https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

NTC6079. (2014). Requisitos de Seguridad. In ICONTEC, *Requisitos para sistemas de infraestructura de medición avanzada (AMI) en redes de distribución de energía eléctrica* (p. 24). Bogotá: INCONTEC.

Obermeier, S. &. (2015, Julio 2). Assessing the Security of IEC 62351. *ResearchGate*, 2. Retrieved from https://www.researchgate.net/publication/300343725_Assessing_the_Security_of_IEC_62351 [accessed Jul 02 2018].

OSGP, A. (2018, Julio 2). *OSGP Alliance*. Retrieved from http://www.osgp.org/en

PRIME, P. I. (2018, Julio 2). *PRIME (PoweRline Intelligent Metering Evolution)*. Retrieved from http://www.prime-alliance.org/

S. Khaithan, J. M. (2015.). *Cyber Physical Systems Approach to Smart Electric Power Grid.* Springer-Verlag GmbH,.

Sahu, A., Tippanaboyana, H. N., Hefton, L., & Goulart, A. (2017). Detection of rogue nodes in AMI networks. *2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, 2.

Schneier, B. (1999). "Attack Trees,". *Dr. Dobb's Journal*, 21–29.

Stefanov, A. &. (2014). Cyber-Physical System Security and Impact Analysis. *IFAC*, 11238.

TrendMicro, & OEA. (2015). Políticas de Ciberseguridad. *Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*, 32.

UKCyber. (2011). Which feeds growth. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, 12.

UPME Parte 4, S. G. (2016). Amenazas para los sistemas físicos. *Estudio: Smart Grids Colombia Visión 2030 - Mapa de ruta para la implementación de redes inteligentes en Colombia*, 3.

UPME Parte I, S. G. (2016, Mayo 22). Tecnologías y funcionalidades de las redes inteligentes. *Estudio: Smart Grids Colombia Visión 2030 - Mapa de ruta para la implementación de redes inteligentes en Colombia Parte I*, 11. Retrieved from http://www1.upme.gov.co/DemandaEnergetica/Smart%20Grids%20Colombia%20Visi%C3%B3n%202030/1_Parte1_Proyecto_BID_Smart_Grids.pdf

UPME Parte3, S. G. (2016). Medidores de energía eléctrica. *Estudio: Smart Grids Colombia Visión 2030 - Mapa de ruta para la implementación de redes inteligentes en Colombia*, 61.