ATAQUES INFORMÁTICOS A LA INFRAESTRUCTURA CRÍTICA DEL SECTOR ELÉCTRICO COLOMBIANO

PEDRO JULIO MENDOZA VILLAMIL
ÁLVARO DÍAZ ARDILA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2019

ATAQUES INFORMÁTICOS A LA INFRAESTRUCTURA CRÍTICA DEL SECTOR ELÉCTRICO COLOMBIANO

ING. PEDRO JULIO MENDOZA VILLAMIL
ING. ÁLVARO DÍAZ ARDILA

Monografía para optar al título de
Especialistas en Seguridad Informática

Director del proyecto
ING. JUAN JOSÉ CRUZ GARZÓN
Especialista en Seguridad Informática

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA
2019

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bucaramanga (18, 3, 2019)

DEDICATORIA

Esta meta tan anhelada en nuestras vidas es dedicada muy especialmente a nuestras familias, su apoyo incondicional contribuyó al logro de este titulo

AGRADECIMIENTOS

Primeramente, gracias a Dios por iluminar y bendecir nuestras vidas. Gracias a todas las personas que facilitaron nuestro aprendizaje y en especial gracias a todos los directores de curso que acompañaron nuestro desarrollo académico

GLOSARIO

0-day: Día Cero, Explotación de una vulnerabilidad en un sistema o en un dispositivo para la cual el fabricante no ha publicado parches o estrategias para mitigar el daño que puede producir el atacante informático. Generalmente los ataques de día cero se producen en conjunto de un malware, troyano o virus.

APT: Grupos de Amenaza Persistente Avanzada “APT Groups”.

C&C: Servidor utilizado por atacantes informáticos como centro de comando y control.

CID: Archivo propio del estándar IEC61850, contiene la configuración del IED.

Acuerdo CNO 788: Guía de ciberseguridad aplicable a la industria eléctrica colombiana. Aprobada para mitigar los riesgos de ciberseguridad en el sector eléctrico y en el sistema Interconectado nacional SIN.

CNO: Es el organismo colombiano que acuerda con los agentes del sector eléctrico los aspectos técnicos para la óptima operación del sistema interconectado nacional.

Compes 3701: Documento que establece la política de seguridad cibernética y ciber defensa de Colombia.

DRAGONFLY: Libélula en español. En este documento se refiere al grupo de ciberespionaje que actúa en el sistema eléctrico mundial, especialmente en E.U y Europa.

GOOSE: Generic Object Oriented Substation Events. Es un tipo de mensajería que utiliza en el estándar IEC 61850 para transmitir eventos que tiene prelación alta y por lo tanto necesitan un medio de comunicación rápido. Los disparos enviados desde los IED´s a los interruptores de maniobra es un ejemplo de esto.

IA: Inteligencia artificial.

ICD: Archivo propio del estándar IEC61850, contiene la estructura de los datos y los nodos lógicos que están configurados en el IED.

IEC 61850: Estándar internacional para el sector de subestaciones eléctricas.

IED: Dispositivo Electrónico Inteligente.

INDUSTROYER: Malware dirigido a las subestaciones eléctricas, se caracteriza por ser modular y permite ser personalizable.

MALWARE: Es un software malicioso que en su estructura se encuentra código informático que tiene como función causar daño a los sistemas informáticos.

MMS: Manufacturing Message Specification. Servicio de mensajería en la industria.

Nodo Lógico: Unidad de información básica del estándar IEC 61850. Permite el intercambio de información y la formación de funciones.

OPC: OLE for Process Control. Es un estándar de comunicación con la tecnología propia de Microsoft, ampliamente utilizado en los sistemas de control industrial para integrar dispositivos con hardware y software individual y que permite que se compartan los datos.

SAS: Sistema de automatización de Subestaciones eléctricas.

SCADA: Supervisory Control And Data Acquisition. Herramienta de software que se utiliza para controlar y supervisar dispositivos a distancia, mediante el envío de señales análogas y digitales tratadas por el equipo RTU o los convertidores de protocolo Gateway.

SCD: Archivo propio del estándar IEC61850, describe la configuración de la subestación. Contiene todos los IED configurados en el proyecto de la subestación

SCL: Lenguaje utilizado por el estándar IEC 61850 para describir la configuración de subestaciones.

SIN: Sistema Interconectado Nacional.

STUXNET: malware que afecto la central nuclear de Nataz.

TIC: Tecnología de información y las comunicaciones.

TO: Tecnología de operación.

Wipe: Acción característica que se realiza cuando se borra información en un dispositivo de computo.

RESUMEN

Los ataques a la infraestructura crítica del sector eléctrico colombiano aún no han tenido pronunciamiento oficial de parte de las entidades gubernamentales que manejan dichos activos. En el último foro de riesgos 2018 “RIMS” celebrado en México el funcionario encargado para hacer la presentación por parte del sector eléctrico colombiano dio a conocer la política de seguridad nacional colombiana del sector eléctrico contra los ataques del ciberespacio, sin referirse puntualmente a un ataque en especial.

En este trabajo se presenta un enfoque internacional de los ataques que se han registrado a través de la historia Stuxnet, DragonFly, BlackEnergy, Industroyer y que sirve de guía para abordar este riesgo latente en nuestro sistema interconectado nacional “SIN”.

Como tema especial tratado en este documento y dada la gran acogida y aceptación dentro de la ingeniería colombiana del estándar IEC 61850 en las arquitecturas de los sistemas de automatización de subestaciones eléctricas, se hizo un estudio detallado del contenido del estándar en sus 10 capítulos y se estructuró una implementación para subestación de alta tensión abordando los conceptos necesarios para su comprensión, adicionalmente todas las ideas aquí presentadas tratan de correlacionar el ataque realizado en Ucrania en el año 2016 con los protocolos de comunicación que se están utilizando en Colombia, entre ellos el OPC y el estándar IEC 61850.

Palabras clave: RIMS, Stuxnet, DragonFly, BlackEnergy, Industroyer, SIN, IEC 61850, OPC

ABSTRACT

Attacks on the critical infrastructure of the Colombian electricity sector have not yet had an official pronouncement from the government entities that handle such assets. In the last risk forum 2018 "RIMS" held in Mexico, the official in charge of making the presentation by the Colombian electricity sector announced the national security policy of the Colombian electricity sector against cyber-attacks, without referring to a specific special attack.

This paper presents an international approach to the attacks that have been recorded throughout history Stuxnet, DragonFly, BlackEnergy, Industroyer and that serves as a guide to address this latent risk in our national interconnected system "SIN".

As a special topic discussed in this document and given the great acceptance and acceptance within Colombian engineering of the IEC 61850 standard in the architecture of the electrical substation automation systems, a detailed study was made of the content of the standard in its 10 chapters and I structure an implementation for high voltage substation addressing the concepts necessary for its understanding, additionally all the ideas presented here try to correlate the attack carried out in Ukraine in 2016 with the communication protocols that are being used in Colombia, among them the OPC and the IEC 61850.

Keywords: RIMS, Stuxnet, DragonFly, BlackEnergy, Industroyer, SIN, IEC 61850, OPC

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

INTRODUCCIÓN

Los avances tecnológicos que antes se medían en largos periodos de tiempo, hoy se suceden con una velocidad impresionante, en corto tiempo la humanidad ha cambiado su forma de vivir y las cosas que antes dependían de los ajustes mecánicos hoy dependen de la movilidad e interconexión y en muy poco tiempo de la inteligencia artificial IA.

En la actualidad, la mayoría de las personas llevan en su poder un ordenador inteligente “Smart” conectado de forma permanente a la red que le guía en su día a día y le facilitan tareas cotidianas en las que antes tenía que programar desplazamientos o determinar una hora del día para llevarlas a cabo, hoy gracias a que las empresas privadas y las gubernamentales ofrecen servicios en línea las veinticuatro horas del día se pueden realizar a cualquier hora sin tener que esperar eternas colas.

Las tecnologías de la información y las comunicaciones TIC han sido pioneras de cambio, ofrecen a usuarios, bancos en línea, tiendas virtuales, servicios de correo electrónico, consulta médica en línea, asesorías de abogados, pago de matrículas, plataformas de pago, WhatsApp, Facebook, Instagram, YouTube, Twitter entre muchas más que les obliga a estar permanentemente disponibles y que las pone en riesgo ante posibles ataques cibernéticos a sus sistemas de información. Históricamente esto ha sido así y cada una de las lecciones aprendidas en los diferentes campos ha llevado a las TIC a cierto nivel de madurez que se refleja en seguridad de los servicios ofrecidos.

Los sistemas de control industrial hacen parte de este cambio, centrales de generación de energía, subestaciones eléctricas, control de semáforos, control de transporte masivo, plantas de tratamiento de agua, el sector petrolero, entre otros han experimentado las ventajas de tener sus sistemas conectados y disponibles para gestión en línea, con la gran incertidumbre y a diferencia de las TIC que las consecuencias producto de un ataque cibernético pueden afectar directamente el mundo lógico y además el mundo físico con resultados devastadores para una nación. En la pasada cumbre Latinoamérica de septiembre de 2017 celebrada en Argentina los especialistas de Kaspersky revelaron que se producen 33 ataques por segundo y 117 por hora siendo los países más afectados Brasil, México y Colombia.

Así como existen las tecnologías de la información y comunicaciones TIC, en el sector industrial existen las tecnologías Operativas TO, encargadas de la automatización, control y supervisión de procesos industriales que en la mayoría de los casos en Colombia hacen parte de las infraestructuras críticas. Las TO no tienen la misma madurez vistas desde la seguridad informática que los sistemas

comerciales en línea que conocemos, por lo que la reglamentación, la madurez y formación en ciberseguridad industrial es un camino que se debe emprender lo más pronto posible.

En este documento se presentan diferentes aspectos de la ciberseguridad industrial en el mundo y en Colombia en particular, con la óptica de presentar y alertar los peligros que puede traer un ataque a la infraestructura crítica.

La reseña histórica presentada de los ataques más relevantes en el sector industrial y en el sector eléctrico mundial como Stuxnet, DragonFly, BlackEnergy, Industroyer, Triton, pretende adaptar lecciones aprendidas que deben ser tenidas en cuenta para evitar amenazas similares en el sector eléctrico colombiano.

Finalmente, en este documento y dada la creciente popularidad de los sistemas de supervisión y automatización de subestaciones eléctricas basadas en el estándar IEC 61850 en Colombia y la utilización de dispositivos electrónicos inteligentes Siemens SIPROTEC y ABB que tienen vulnerabilidades ampliamente documentadas, se aborda en detalle el contenido del estándar y su implementación en subestaciones de alta y ultra alta tensión. También se aborda su amenaza latente materializada en Ucrania el 17 de diciembre de 2016 Win32/Industroyer – CrashOverride.

1. TITULO

ATAQUES INFORMÁTICOS A LA INFRAESTRUCTURA CRÍTICA DEL SECTOR ELÉCTRICO COLOMBIANO

Área de investigación: Especialización en Seguridad Informática

Línea de Investigación: Infraestructura tecnológica y seguridad en redes

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

La infraestructura crítica de un país comprende todos los procesos relevantes para su sostenimiento en la actualidad y en el tiempo, es decir, todos los procesos que son indispensables para su funcionamiento, en otras palabras, que no se pare el país a falta de alguna de ellas en grandes poblaciones o en el país entero. En caso de faltar o dejar de prestar el servicio una infraestructura de estas, habría un Caos con grandes consecuencias, por ejemplo, la falta de; el suministro de agua potable, el suministro de energía, el suministro de combustible, el suministro de transporte aéreo, terrestre, fluvial y marítimo, las comunicaciones, la salud, el sistema judicial, legislativo y ejecutivo, todas las fuentes de energía vitales para el sostenimiento y desarrollo de un país, entre otras.

De acuerdo a lo anterior, el país ha hecho grandes esfuerzos en colocarse a la vanguardia de otros países en cuanto a la utilización de las tecnologías de la información, comunicaciones y operaciones de estas infraestructuras críticas y por tanto se vuelven estratégicas para su desarrollo y funcionamiento[1].

El incremento considerable que ha tenido el uso de la tecnología digital en Colombia ha permitido el mejoramiento de las comunicaciones en todos los escenarios, celular, telefonía, televisión, internet, comunicaciones en procesos de infraestructura crítica, entre otros.

La utilización de las comunicaciones y la tecnología digital en la infraestructura crítica nos coloca a la vanguardia de estos procesos en lo referente a su manejo a nivel mundial, pero también nos coloca en gran riesgo debido a que se han presentado muchos ataques a la infraestructura critica en todo el mundo, por lo tanto, se tienen que hacer grandes esfuerzos en el país en cuanto a la seguridad de estas infraestructuras críticas[2].

---

[1] Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT. {En Línea}. {12 diciembre 2018}. Disponible en: http://www.colcert.gov.co/?q=acerca-de

[2] HERNANDEZ, José. Infraestructura Crítica Cibernética. {En línea}. {12 diciembre 2018} Disponible en: http://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

2.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los métodos que utilizan los Ciber delincuentes para atacar la Infraestructura Crítica del Sector Colombiano?

2.3 DESCRIPCIÓN DEL PROBLEMA

Con base en el planteamiento anterior y para dar respuesta a nuestra pregunta ¿Cuáles son los métodos que utilizan los Ciber-delincuentes para atacar la infraestructura Crítica del sector eléctrico colombiano?, nuestro proyecto nos permitirá conocer y estudiar estos ataques, saber de qué manera podemos ser atacados, la forma, los métodos que utilizan para impactarnos considerablemente en mayor o menor proporción por un ciber-ataque o ataque informático a estas infraestructuras tan importantes y necesarias para el funcionamiento y desarrollo de un país.

Partiendo de ese estudio y análisis, podríamos dimensionar el grado de afectación de este servicio público esencial y valorar la importancia que se le da por parte de estas empresas prestadoras del servicio a este problema y se podrá conocer también porque no, las posibles mitigaciones si las hay que salgan de este trabajo de análisis[3].

[3] REALPE. Milena LA CIBERDEFENSA EN COLOMBIA {En línea}. {12 diciembre 2018} Disponible en: https://www.cci-es.org/documents/10694/468834/3.+CCOC+PLAN+NACIONAL.pdf/84da120e-3bd6-478c-99c8-1f88c3543355;jsessionid=5E61914D5E08633E7DD315CB4A68FC94?version=1.0

3. JUSTIFICACIÓN

La seguridad de la infraestructura critica de un país es fundamental, no sobra decir lo grave que sería un ataque informático para cualquier infraestructura crítica en Colombia, para el caso del sector eléctrico colombiano, nos podríamos ver en una situación de apagón como ocurrió en ucrania donde los atacantes dejaron a miles de personas sin energía en una noche fría de invierno, en nuestro caso no tenemos estas estaciones extremas pero si necesitamos la energía como todo el mundo para mover nuestra economía, necesitamos energía en nuestros hogares, en las industrias, en las universidades, en los hospitales y Clínicas, en el transporte, en el comercio, etc.

La afectación a la infraestructura eléctrica por un ciberataque podría también afectar a poblaciones enteras porque la energía esta toda conectada y tanto las compañías que la generan como las que la transportan podrían tener graves consecuencias si se afectan sus sistemas, se afectarían las grandes empresas generadoras de energía como las chicas y así mismo ocurriría con todas las que la transportan en grande o menor proporción, si no se afecta un transportador grande pero se afecta a los que la reciben o la distribuyen, de nada sirve tenerla sino tiene a quien entregársela, en conclusión todos estamos en la cadena de afectación.

De acuerdo a lo anterior, toma mayor importancia el conocer de qué manera podemos ser afectados o impactados considerablemente en mayor o menor proporción por un ciberataque o ataque informático a estas infraestructuras críticas. Por tanto si bien la afectación se da en perder la energía de una población y se afectan muchas personas, también está el impacto en la construcción de conocimiento, es importante comprender la forma como se realizan estos ataques, conocer la estructura de sus ataques, la estrategia utilizada, los métodos que utilizan los Ciber-delincuentes, conocer las técnicas de alta ingeniería utilizadas para encontrar las brechas y las vulnerabilidades de los sistemas instalados, de los equipos de comunicación y control y de los protocolos que utilizan para comunicarse y manejarlos a su antojo, pudiendo generar activaciones de órdenes de ejecución en horas específicas, de activación y desactivación de equipos y hasta tomar el control total de un sistema de estos con afectaciones incalculables para atacar la infraestructura Critica de este sector.

A raíz de lo anterior, toma relevancia el estudio a los ataques hechos a las diferentes estructuras críticas a nivel mundial porque dejó ver que el sistema es muy vulnerable por las comunicaciones que se utilizan, en este caso hablamos de los protocolos utilizados, como la norma IEC 61850 que es muy utilizada en el sector eléctrico por empresas generadoras, transportadoras y distribuidoras de la energía eléctrica.

Con base en lo anterior, este proyecto pretende dimensionar el grado de afectación de este servicio público esencial y valorar la importancia de generar conocimiento sobre los ataques efectuados, conociendo la estructura, la forma y la estrategia de estos ataques, con esto también se podrá conocer también porque no, las posibles medidas preventivas para mitigarlos si las hay, o por lo menos saber a qué estamos expuestos y poder así tomar las medidas preventivas posibles.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Hacer un estudio a los ataques informáticos a la infraestructura crítica del sector eléctrico en Colombia

4.2 OBJETIVOS ESPECÍFICOS

1. Conocer la información referente a los ataques informáticos en infraestructura Crítica.

2. Analizar los ataques informáticos a la infraestructura crítica del sector eléctrico en Colombia.

3. Estudiar el estándar IEC61850 en los sistemas de Infraestructura Crítica.

4. Presentar un análisis comparativo de los ataques realizados y sus características (DragonFly, BlackEnergy, Stuxnet, Industroyer 2016).

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

El pasado, el presente y el futuro de la humanidad estarán enmarcados por grandes cambios y diferente forma de vida. De gran interés es para los especialistas conocer el comportamiento de las personas, observar el modo de actuar y de vivir en nuestros días y más aún cuando la era digital ha penetrado los diferentes escenarios del diario vivir.

Se podría afirmar que después del colapso económico de los años 2007 – 2008 que sacudió la economía de los Estados Unidos y sus coletazos a nivel de todo el mundo, las cosas han cambiado, producto de la aparición casi simultánea de una gran variedad de inventos, y algunas tecnologías disruptivas que han llegado y se quedaran hasta los próximos cambios generacionales.

El mundo entero disfruta hoy muy placenteramente de los cambios hechos en el audio, en el video, en la fotografía y de la portabilidad móvil gracias a los aportes a la humanidad hechos por Steve Jobs con la invención del iPhone, así como también la sociedad experimenta nuevas formas de intercambiar contenidos con la popularidad de las redes sociales.

Se suman a las ideas innovadoras de S. Jobs los cambios propuestos con la aparición del Twitter, las facilidades de portabilidad que ofrece el sistema operativo Android, el aumento de velocidad en la computación, la impresión 3D, la robótica, el aporte de Satoshi Nakamoto con el Bitcoin y el concepto de activo digital, el Blockchain como la gran “tecnología” disruptiva unida con la Inteligencia Artificial, las ciudades inteligentes y la gran era de Industria 4.0.

Ya de esta época digital y grandes cambios hemos recorrido a la fecha más de una década. Las economías y las industrias en todos sus niveles han tenido que adaptar cambios en sus procesos que los ha llevado a renovar métodos y en algunos casos han desarrollado nuevas profesiones en el ejercicio de sus actividades. La economía, la industria, la bolsa de negocios, el Internet de Todo, el Uber, Airbnb, el Rapi, el mercado de energía, los sistemas Scada, los sistemas SAS entre muchos más, han utilizado o utilizaran las tecnologías de la información y las comunicaciones como medio de intercambio de información y de datos. Las tecnologías de la información están utilizadas masivamente en muchos de los escenarios de la vida cotidiana y han cerrado brechas y acercado las personas, pero toda esta actividad tiene inmersos riesgos y peligros que afectan los derechos de la humanidad, la seguridad de los pueblos, la era digital y puntualmente las infraestructuras críticas de los países.

La mayoría de los medios de comunicación mundiales constantemente están entregando información a sus receptores acerca de temas como ataques informáticos, computación en la niebla, almacenamiento en la nube, ciberseguridad, “hacker”, infraestructuras críticas, ciberataques, ciberguerra, espionaje y los medios más especializados dan a conocer noticias sobre la actividad de grupos hacktivistas, sobre cibercriminales y sobre grupos de amenaza persistente avanzada APT, y en general se conocen noticias de las actividades a nivel mundial y nacional de personas o comunidades con pensamiento malicioso, sus ataques y sus logros.

En 2016 cuando aún la comunidad de investigadores analizaba el éxito malicioso de Stuxnet y algunos ataques más al sector energético como Flamer, Dragonfly, Blackenergy, el mundo entero y en especial el sector eléctrico se extrémese con los vectores de ataque utilizados por el malware Industroyer. El malware industroyer y sus autores atacaron el sistema eléctrico de Ucrania el 17 de diciembre de 2016 y de él, se conoce que en su diseño se utilizaron técnicas de ataque convencionales como backdoor, combinadas con un gran conocimiento en la ingeniería de los sistemas de control, utilizados en las subestaciones eléctricas en todo el mundo, incluidas las subestaciones eléctricas en Colombia. Industroyer es capaz de desplazar el control y supervisión de una subestación eléctrica y a cambio de esto replica puertos de comunicación, protocolos de control, protocolos de comunicación y demás dispositivos del sistema SAS para posteriormente ser controlados desde un servidor de C&C alojado probablemente en la red Tor. Este tipo de ataque tomo el control literal de la subestación e hizo imposible a los operadores del sistema la toma de decisiones en términos operativos Equipos de la empresa Siemens de la referencia Siprotec utilizados en el sistema de control quedaron altamente comprometidos en el ataque de Ucrania, los atacantes en el mismo paquete ejecutaron la técnica de denegación de servicio DDoS sobre el módulo de comunicación EN100 en el cual Siemens implementa la gestión remota del IED y también parte de la arquitectura del estándar IEC 61850, explotaron la vulnerabilidad CVE-2015 5374 y jocosamente se refirieron a ella como un regalo del ataque realizado.

Los ataques informáticos, el espionaje entre naciones, la ciber seguridad, son términos normalmente manejados por ingenieros y personal técnico, pero con el auge que han tenido los ataques informáticos, estos temas han penetrado las sesiones de políticos, el interés de gobernantes y naciones en general, toda esta temática está estrechamente relacionada con las infraestructuras críticas. El sistema eléctrico interconectado de Colombia está catalogado como infraestructura critica, la generación y la distribución de energía eléctrica es para los ciudadanos un servicio esencial.

Desde lo cotidiano se puede afirmar que una infraestructura crítica soporta un servicio esencial que es usado por la comunidad a diario y que cuando este servicio no está presente, afecta directamente la vida del ser humano. Las centrales generadoras, las líneas de trasmisión de extra alta tensión en 500kV, las de alta tensión en 230kV, sus respectivas subestaciones eléctricas y demás equipos asociados hacen parte de la infraestructura eléctrica del país.

En Colombia, el sistema eléctrico Interconectado ha tenido grandes progresos, se ha incorporado tecnología de punta en los equipos de maniobra, así como también se han tenido grandes avances en los equipos de supervisión y control de subestaciones eléctricas. La topología en malla empleada en la interconexión eléctrica del país ha desplazado los sistemas radiales para aumentar el porcentaje de confiabilidad en el servicio de energía eléctrica en los hogares y la industria, lo cual le da mucha más importancia al servicio prestado, razón por la cual el gobierno ha incrementado los sistemas de protección y planes de acción en lo que refiere a la ciberseguridad de estas infraestructuras.

Concierte de tan importante servicio, el gobierno colombiano basado en los lineamientos de ciberseguridad y ciberdefensa contenidos en el Compes 3701 de 2011, encargo al CNO de difundir entre los agentes operadores del sistema y generadores, la guía de ciberseguridad del acuerdo 788 de 2015. Esta guía es un marco de referencia basado en los estándares NERC aplicados en E.U

Ataque informático a infraestructura critica. La mayoría de los sistemas industriales e infraestructuras críticas están controladas por sistemas de control diseñados de acuerdo a la pirámide de control (Niveles de operación), estos sistemas, además de contener lógicas cableadas y/o lógicas blandas suministran una interfaz humana máquina para facilitar la operación. El interés de algunas personas con pensamiento malicioso es poder obtener acceso a estos equipos y explotar las distintas vulnerabilidades (volcado de memoria, desbordamiento de buffer, ataques de DDoS etc.) ampliamente conocidas en el medio donde se mueven.

Los ataques más representativos a la infraestructura critica eléctrica a nivel mundial, se puede decir que inician en Ucrania en el diciembre del año 2015, los atacantes afectaron a miles de personas que quedaron sin electricidad, este ataque consistió en entrar a través de redes corporativas utilizando los correos electrónicos para infiltrar el malware BlackEnergy el cual toma el control del sistema SCADA (Supervisory Control And Data Acquisition) utilizado para la operación remota de subestaciones, desconectar a varias subestaciones del

sistema y causar otros daños en los demás equipos aislándolos del sistema.[4]

De acuerdo al interés del atacante, la forma de atacar y de actuar, los ataques se dividen en:

Ataques de cibercriminales. Estos ataques están dirigidos a personas del común que utilizan las tecnologías de la información

Ataques de Hacktivistas. Estos ataques generalmente tienen tintes políticos, sus objetivos son las infraestructuras críticas, el gobierno los servicios secretos.

Ataques por ciberespionaje. Estos ataques están dirigidos a la industria como objetivo concreto, roba las bases de datos para después controlar los sistemas

Grupos de Amenaza Persistente Avanzada “APT Groups”. Desde estos grupos que son patrocinados por gobiernos, por asociaciones delictivas por empresas específicas etc. salen ciber ataques y se realiza ciberespionaje a las infraestructuras críticas para robar, interrumpir operaciones o destruir infraestructuras indistintamente en todas las naciones. El ataque desde un APT se distingue por que contienen un arsenal de vectores de ataque y todo un proceso planificado y milimétrico a través de un tiempo continuo, es patrocinado por un tercero que tiene un objetivo específico. Un APT invierte una gran cantidad de recursos técnicos, económicos y de conocimiento

Algunos APT que hacen historia.[5]

APT 1 = Atribuido a China, dirige ataques en Estados Unidos, su actividad ha sido detectada en el espionaje a la industria y las grandes empresas tecnológicas.

APT 10 = Atribuido a China, dirige ataques en Estados Unidos, Japón, India, Suecia, Francia, Reino Unido Brasil, Noruega, su actividad ha sido detectada en el espionaje en las tecnologías de la información

APT 12 = Atribuido a China, dirige ataques en Japón, Taiwán, su actividad ha sido detectada en el espionaje en las fábricas de productos electrónicos y empresas de telecomunicaciones

---

[4] PREZ, David. La verdadera historia detrás del virus informático que provocó un apagón en Ucrania. {En línea}. {12 diciembre 2018}. Disponible en: https://omicrono.elespanol.com/2017/11/virus-informatico-provoco-apagon-en-ucrania/

[5] AVILA, Fred Y. Grupos avanzados de amenazas persistentes. {En línea}. {10 marzo 2019}. Disponible en: https://securityhacklabs.net/articulo/grupos-avanzados-de-amenazas-persistentes-apt-groups

APT 15 = Atribuido a China, dirige ataques en la marina de los Estados Unidos y en el reino Unido, su actividad ha sido detectada en el espionaje de entidades gubernamentales y en las tecnologías de la información

APT 28 = Atribuido al gobierno ruso, es uno de los grupos más tenidos pues sus objetivos están en las altas esferas de los gobiernos, realiza espionaje del más alto nivel, atacaron el partido demócrata de los Estados Unidos y se presume que su próximo ataque estará en Alemania y Francia

APT 33 = Atribuido a Irán, dirige ataques en Arabia Saudita, Estados Unidos, Corea del Sur, su actividad ha sido detectada en el sector de la aviación, el sector de la energía y el sector petroquímico.

APT 34 = Atribuido a Irán, dirige ataques en el Oriente Medio, su actividad ha sido detectada en el sector químico, el sector gubernamental, las infraestructuras críticas, el sector de la energía y las finanzas.

APT 37 = Atribuido a Corea del Norte, dirige ataques a Corea del Sur, Japón, Vietnam y Oriente Medio, su actividad ha sido detectada en el sector de la salud, la industria, las infraestructuras críticas, en el campo de la electrónica.

5.2 MARCO CONCEPTUAL

La ley 142 (servicios públicos domiciliarios) y 143 (Ley Eléctrica) de 1994[6] definió las reglas de juego para todo el sector eléctrico y separó las diferentes actividades en cuatro áreas que son: Generación de Energía, Transporte de energía, Distribución de Energía y Comercialización de energía, estas cuatro actividades están reguladas por estas leyes y funcionan dentro de un sistema eléctrico a nivel nacional, el cual se llama Sistema Interconectado Nacional (SIN), de acuerdo al área o actividad se encuentran varios agentes u operadores involucrados, entre ellos empresas de transporte de energía, de generación, de distribución y de comercialización y mixtas como las electrificadoras rurales y urbanas que están en varias actividades a la vez.

El sector eléctrico en Colombia es privado, pero tiene una estructura institucional definida, el estado controla este sistema y está organizado en el siguiente orden jerárquico del nivel superior al menor; en la Dirección se encuentra el Ministerio de Minas y Energía quien a su vez depende de la presidencia de la república,

6 LEY 142 DE 1994 {En línea}. {12 diciembre 2018} Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html

seguidamente en la Planeación se encuentra la Unidad de Planeación Minero Energética UPME[7] quien depende del ministerio de minas y energía, le sigue en su orden la Regulación que está a cargo de la Comisión de Regulación de Energía y Gas CREG[8] quien depende del ministerio de minas y energía, el ministerio de Hacienda y el Departamento nacional de Planeación, luego en el Consejo y Comité está el Consejo Nacional de Operación CNO y el comité asesor de Comercialización CAC quienes dependen de la CREG, en el Control de Vigilancia se encuentra la Superintendencia de Servicios públicos quien depende de la presidencia de la República y por último en la Operación y Administración del Mercado de Energía se encuentra el Centro Nacional de Despacho CND el cual está a cargo de la empresa XM expertos en mercado de propiedad del grupo empresarial Interconexión Eléctrica E.S.P. ISA.

El Sistema Interconectado Nacional (generadores, transportadores y distribuidores de energía eléctrica) está compuesto por Plantas generadoras (hidráulicas, térmicas, eólicas, etc.), líneas de transmisión de 500 kV, 230 kV, 115 kV, y 34,5 kV, subestaciones eléctricas de 500 kV, 230 kV, 115kV y 34,5 kV respectivamente y dentro de las plantas generadoras y subestaciones eléctricas se encuentran los diferentes equipos necesarios para su funcionamiento, los cuales para las diferentes comunicaciones entre ellos o con los centros de control utilizan unos protocolos estándares de comunicación de la norma estándar IEC 61850 muy utilizada en este sector y la cual será estudiada en el desarrollo de este proyecto.

Las empresas del sector eléctrico mencionadas anteriormente, pertenecen a la infraestructura crítica del país debido a que están conectadas al SIN y cualquier ataque informático dentro de estas empresas podrían afectar gravemente causando un apagón total o apagones estratégicos en diferentes zonas industriales, hospitales, militares, zonas de altos volúmenes de población, etc.

5.3 ESTADO ACTUAL

Es importante resaltar que en Colombia hasta ahora no se han producido ataques del tipo industrial como los mencionados anteriormente a nivel mundial en las infraestructuras críticas estratégicas, en Colombia los ataques que se han hecho a las infraestructuras críticas eléctricas han sido solo para extracción de información

[7] UPME Unidad de Planeación Minero Energética {En línea}. {12 diciembre 2018}. Disponible en: http://www1.upme.gov.co/Paginas/default.aspx

[8] CREG Comisión de Regulación de Energía y Gas. {En línea}. {12 diciembre 2018}. Disponible en: http://www.creg.gov.co/

sin causar daño, no se ha publicado información de otro tipo de ataques a estas infraestructuras, pero no podemos quedarnos tranquilos por ello porque en Colombia se utilizan los mismos equipos que han sido atacados a nivel mundial y se manejan los mismos protocolos estándares IEC 61850.

De acuerdo a lo anterior, estos protocolos son vulnerables porque se diseñaron hace décadas para automatizar procesos y permitir las comunicaciones entre equipos propios de potencia con los de control de las subestaciones y las centrales eléctricas, pero se suponían que iban a estar aislados de internet o de cualquier tipo de red de conexión externa[9].

Normalmente los ataques más presentados a la infraestructura critica son por las formas más comunes, ataques Web, SQL Injection, Denegación de Servicios, (DDoS), por medios físicos de usuarios internos (USB), XSS (Cross-site scripting), etc.

Los ataques presentados en varias partes del mundo a las infraestructuras críticas se han hecho a equipos Siemens S5, los cuales son muy utilizados en Colombia, por tanto, existe altas posibilidades de ataques informáticos a nuestra infraestructura critica estratégica del sector eléctrico.

Como ven el panorama no es muy alentador, queda mucho por hacer porque la situación actual de la seguridad de las infraestructuras críticas a nivel mundial y nacional está en riesgo debido al uso cada vez más de estas tecnologías en sistemas remotos de control con equipos que no cumplen altos estándares de seguridad y que están cuestionados porque no fueron diseñados para conexiones por internet o del tipo externas.

Con el desarrollo de este proyecto se podría contribuir primero que todo al conocimiento real de la magnitud del problema, se podría contar con el planteamiento por parte de sus autores del reconocimiento de que existe un problema por resolver, conocer la forma actual como se ve o como se está enfrentando, conocer cómo van los avances en cuanto a la defensa actual de esta infraestructura crítica esencial para el país, se podrá conocer e indagar hasta donde llegan los conocimientos de los atacantes en estos protocolos que pueden afectar a estos sistemas informáticos complejos, dimensionar el grado de afectación del servicio, indagar que tanta importancia se le da al problema, conocer y entender las diferentes técnicas y formas de ataque utilizadas para

[9] CORPORACIÓN COLOMBIANA DIGITAL. Las amenazas informáticas son capaces de controlar los sistemas de energía eléctrica de una nación. {En línea}. {12 diciembre 2018}. Disponible en: https://colombiadigital.net/actualidad/noticias/item/9805-las-amenazas-informaticas-son-capaces-de-controlar-los-sistemas-de-energia-electrica-de-una-nacion.html

afectar gravemente estas infraestructuras criticas estratégicas y se platearan las posibles recomendaciones que salgan de este trabajo de análisis medidas.

6. ESQUEMA TEMÁTICO

6.1 CONOCIMIENTO DE LA INFORMACIÓN DE ATAQUES INFORMÁTICOS A LA INFRAESTRUCTURA CRÍTICA Y ANÁLISIS A LOS ATAQUES HECHOS AL SECTOR ELÉCTRICO EN COLOMBIA

6.1.1 Conocimiento de Información de las Infraestructuras Críticas.

6.1.1.1 Que son infraestructuras críticas. Una infraestructura critica es un conjunto de elementos o conjunto de servicios que se caracteriza por tener una función esencial en el desarrollo y funcionamiento de un país determinado, las infraestructuras críticas de un país garantizan el cumplimiento de los derechos constitucionales de los ciudadanos, el aumento de la competitividad, la prosperidad económica, política y social que en conjunto aumentan la calidad de vida de los ciudadanos, cabe anotar que dentro de la actividad económica y desarrollo industrial de los países se encuentran sistemas de control de diferentes tecnologías y topologías, pero puede ser, que de acuerdo a la clasificación de las autoridades competentes para tal fin no estén clasificadas como críticas y por el contrario estén clasificadas como infraestructuras estratégicas.

Algunos sectores que presentan servicios esenciales para el correcto funcionamiento de un país pueden ser los siguientes:

- Plantas de tratamiento de agua
- Sector administrativo
- Sector energético
- Sector químico
- Industria nuclear
- Sector salud
- Sector transporte
- Sector de la tecnología de la información de las comunicaciones “TIC” y la tecnología de operación “TO”
- Sistema financiero y tributario
- Centros de investigación gubernamental
- Sector de alimentación

6.1.1.2 Legislación existente para infraestructuras críticas en el mundo. Para la protección de los sectores esenciales definidos por los diferentes gobiernos e impedir que se interrumpan los servicios o se destruyan las infraestructuras criticas existen a nivel mundial una serie de políticas y normas que facilitan la legislación y protección en cada uno de los países.

Los estados unidos han sido pioneros de la construcción y desarrollo de esta regulación y legislación, seguidos por los países de la unión europea con Francia, Alemania, España. América Latina con Argentina, Brasil, Ecuador, Colombia. Los ataques informáticos a las infraestructuras críticas no se localizan en un sector geográfico determinado, están para todo el mundo a lo largo y a lo ancho en nuestros países y es por esta razón que las leyes y reglamentos de ciberseguridad están determinados por los sistemas legales y las diferentes tendencias políticas. En estados unidos las iniciativas por establecer las leyes que deben cumplir y adoptar los sectores que prestan servicios esenciales comenzó en los inicios de los años 1990, pero este interés ha venido creciendo en los últimos quince años ya que los ataques cibernéticos han sido considerados como una amenaza para todos los habitantes de la nación. El 22 de mayo de 1998 se creó PDD-63 (Directiva de Decisión Presidencial), cuyo asunto único y principal es la protección de la infraestructura crítica que sirve entre otras de soporte para las actividades económicas del país y las actividades militares del ejército.

EL 2 de febrero de 2006 los estados unidos implementaron la ley eléctrica y con ella reguló el transporte de energía, la comisión federal reguladora de energía "Federal Energy Regulatory Commission FERC"[10] se encarga desde sus inicios de la regulación de las empresas estatales de gas, petróleo y la trasmisión de energía eléctrica, así como también de la administración y gestión de las normas de ciberseguridad. La comisión reguladora FREC certificó a la corporación para la fiabilidad de la red eléctrica NERC y en el año 2008 se aprobaron las normas de protección de la infraestructura crítica que son un conjunto de estándares, normas, instrucciones y políticas de ciberseguridad de obligatorio cumplimiento de las empresas del sector eléctrico para enfrentar el desafío creciente de la ciber guerra. En Europa la actividad del ciber espacio y la ciber guerra ha sido tan dinámica como en el resto del mundo. La comunidad europea consciente del peligro latente en el ciber espacio ha realizado diversos avances desde el año 2004 con respecto a la protección de la infraestructura crítica. Puntualmente en junio de 2004 el concejo europeo solicitó la elaboración de una estrategia global para la protección de infraestructuras críticas europeas y nacionales "PEPIC".

6.1.2 Marco legislativo de PEPIC

- Contiene un procedimiento de identificación de infraestructuras críticas europeas con enfoque común de evaluación y mejora de la seguridad.

[10] FEDERAL ELECTRIC REGULATORY COMMISSION. FERC. 2018. {En línea}. {12 diciembre 2018}. Disponible en: https://www.ferc.gov/

- Contiene una serie de medidas destinadas a facilitar la aplicación del PEPIC en las que figuran los planes de acción, la aplicación de la red de advertencias de infraestructuras críticas CIWIN, la creación de grupos expertos en análisis y diagnóstico de infraestructuras críticas.

- Facilita y ayuda a los miembros de la comunidad europea a asegurar su infraestructura crítica y ayuda por petición a diseñar planes de intervención.

- Facilita los recursos económicos para aplicar medidas nacionales relacionadas con la protección de infraestructuras críticas.

En todos los estados miembros de la unión europea se implementa y protege la infraestructura crítica mediante una red de información basada en internet, esta plataforma es la que se conoce con el nombre de CIWIN “Critical infrastructure warning information network CIWIN” red de información de advertencias de infraestructura crítica en donde se publican investigaciones, análisis y estudios de expertos e intercambio de información sobre infraestructura crítica. CIWIN tuvo su origen con la adopción del libro verde del programa europeo para la protección de infraestructura crítica publicado en julio de 2001 en donde se exponía la posibilidad de crear una red de información sobre el estado de las infraestructuras críticas europeas.

6.1.2.1 Ley PIC de España. Protección de infraestructuras críticas. La ley PIC española fue creada en agosto de 2011 y se creó por la necesidad de establecer las obligaciones de los primeros operadores críticos. Esta ley propone los siguientes aspectos:

- Creación del sistema nacional de protección de infraestructuras críticas “CNPIC” que maneje el concepto de asociación público – privado y una base de confianza entre entidades.

- Creación de un sistema de planificación. La ley crea un conjunto de normas que definen las medidas para la protección de infraestructuras críticas. Las normas definen los procedimientos que deben llevar a cabo los integrantes del sistema de protección de las infraestructuras.

Los planes contemplados en la ley son:

- Planes estratégicos sectoriales. “PES” Desarrollados por diferentes grupos de trabajo para conocer los servicios esenciales.

- Planes de seguridad del operador. “PSO” Documentos estratégicos Implementado por los operadores críticos para garantizar la seguridad.

- Planes de protección específico. “PPE”. Documentos operativos Implementado por los operadores críticos para asegurar la seguridad física y lógica de las infraestructuras críticas.

- Planes de apoyo operativo. “PAO” Documentos operativos que contienen las medidas que debe implementar la administración pública para apoyar los operadores críticos de infraestructura.

- Creación de un catálogo nacional de infraestructuras estratégicas. En este catálogo se encuentran las características de cada una de las infraestructuras críticas existentes, cada operador crítico pide interactuar con el sistema a través de una plataforma de internet conocido como proyecto “Hermes”.

- Gestión de incidentes. En colaboración con todos los entes afines con la seguridad informática crea CERT organismo especializados con la gestión de incidentes a nivel nacional.

6.1.2.2 Documento COMPES 3701 y acuerdo CNO 788 en Colombia. El documento COMPES 3701[11] emitido por el gobierno colombiano el 14 de julio de 2011, establece la política de seguridad cibernética y ciberdefensa de Colombia, en este documento están contenidos los lineamientos que deben seguir las entidades públicas y privadas involucradas en la operación de la infraestructura crítica para desarrollar una estrategia que contrarreste las amenazas informáticas potenciales que pueden causar daño y desestabilizar el país, así como también generar mecanismos que permitan garantizar la seguridad de la información nacional utilizando normas técnicas y estándares nacionales e internacionales relacionados con la protección de infraestructuras críticas.

El acuerdo del concejo Nacional de Operación CNO No 788 aprobado el 3 de septiembre de 2015 es la guía de ciberseguridad aplicable a la industria eléctrica colombiana aprobada para mitigar los riesgos de ciberseguridad en el sector eléctrico y en el sistema Interconectado Nacional “SIN”. Esta guía de ciberseguridad está basada en la norma NERC – y los estándares CIP 002 y 009 North American Electric Realability Corporation. – Critical Infraestructure

[11] Documento Compes 3701. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. {En Línea}. {12 diciembre 2018}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Protection aplicada en los estados unidos de Norteamérica desde el año 2008 para tecnologías de activos críticos.

Dentro del contenido de la guía de ciberseguridad aprobada por el concejo nacional de operación se tienen los siguientes aspectos:

- Identificación de activos críticos. Los activos deben ser identificados de acuerdo a los criterios contenidos en el anexo A del acuerdo CNO 788.

- Gestión de la seguridad de ciber activos críticos. Define los controles y la gestión que deben realizar las entidades responsables del activo crítico como son el acceso lógico, el acceso físico, la protección de los perímetros, la seguridad electrónica del sitio donde residen los activos críticos.

- Seguridad física de ciber activos críticos. Define la implementación de un programa de seguridad física para la protección del ciber activo crítico.

- Plan de recuperación de ciber activos críticos. Define la implementación de planes de recuperación que correspondan a las técnicas y prácticas establecidas para la continuidad del negocio.

- Anexo A. Criterio de activos críticos. Se definen 15 criterios de activos críticos.

6.1.2.3 Estrategia nacional de algunos países de Latinoamérica para la protección de infraestructuras críticas. A continuación, se listan las estrategias nacionales utilizadas por algunos países vecinos de Latinoamérica.

- En Perú, nombre de la estrategia perCert implementada en 1999

- Venezuela, nombre de la estrategia VenCert implementada en 2008

- Uruguay, nombre de la estrategia CERTUy implementada en 2008

- Brasil, nombre de la estrategia CIRT-GOV implementada en 2004

- Chile, nombre de la estrategia CICERT implementada en 2001

- Argentina, nombre de la estrategia ArCert implementada en 1999

6.1.3 Ataques Informáticos a las Infraestructuras Críticas y Análisis de ataques al sector eléctrico en Colombia.

6.1.3.1 Ataques Informáticos a las Infraestructuras Críticas. En las tecnologías de la información y las comunicaciones "TIC" en años atrás, no se escuchaba tan comúnmente hablar de sistemas "Scada" y aún menos de Sistemas de Automatización de Subestaciones eléctricas "SAS" por ser términos utilizados en la Tecnología de Operación "TO". En nuestros días, términos como "Scada" y SAS están a la orden del día debido a la gran popularización que han tenido en los diferentes medios de comunicación por cuenta de los ciber ataques a sistemas industriales que en algunos casos pertenecen a infraestructuras críticas a nivel mundial. Es muy común iniciar una búsqueda de ciber ataques en internet y encontrar palabras como "Stuxnet", "Petya" e "Industroyer" y aunque son los ataques más conocidos no son los únicos que se han materializado. Para conocer un poco más de los ataques y la contra inteligencia a continuación se relacionan algunos aspectos sucedidos años atrás.

6.1.3.2 Ataques en los años 70´s. guerra fría. Con el propósito de obtener información científica y técnica industrial de los países occidentales (América, África y Europa), la Unión Soviética a través de un grupo de espías denominados "El Directorio T" agrupados en la agencia de inteligencia KGB robo información y además construyó una red de informantes denominada "Línea X" en empresas y laboratorios del enemigo. El grupo "Directorio T" operó con una eficiencia casi perfecta, solo se descubrió su hazaña en el año de 1981 cuando el coronel de alto rango Vladimir L. Vetrov integrante del grupo de inteligencia entregó más de 4000 documentos a la inteligencia de Francia, en un acto que es conocido en la historia como la entrega de documentos "Dossier Farewell" (documentación de despedida). El presidente francés Francois Mitterand aprovechó la cumbre de las potencias industriales "G7" celebrada en julio de 1981 en Ottawa Canadá para entregar el "Dossier Farewell" al presidente de los estados unidos de américa Ronald Reagan. Toda la documentación "Dossier Farewell"[12] terminó en manos de la OTAN y la CIA y fue allí donde se analizó en detalle el contenido de los 4000 documentos encontrando lo siguiente:

- Se encontró la lista de los 250 oficiales de la KGB que conformaban la llamada "Línea X".

- Se encontró la descripción y todo el detalle de la operación Directorio T

[12] The "FAREWELL DOSSIER": Geopolitical consequences on the end of the Cold War Posted on August 19, 2017. {En línea}. {12 diciembre 2018}.
Disponible en: https://gosint.wordpress.com/2017/08/19/the-farewell-dossier-geopolitical-consequences-on-the-end-of-the-cold-war/

- Se encontró la lista de 170 agentes de la KGB residentes en los distintos países.

- Se encontró información de más de 100 contratos celebrados y planes futuros de robo de tecnología denominada “Lista de Compras”.

- Después de esto, a simple vista se puede decir que la Unión Soviética infiltró la información de muchos países de occidente y que la tecnología usada en este país fue robada de dichos países.

6.1.3.3 Contra inteligencia a los documentos Dossier Farewell por parte de la CIA. Una vez conocidos los detalles de la infiltración de información, el presidente Ronald Reagan exigió respuestas a esta agresión y fue así que autorizó al ingeniero experto en tecnología Gus W. Weiss el suministro de software manipulado para que fuera maliciosamente expuesto a los agentes de KGB.

La Unión Soviética desarrollaba en el año 1982 un proyecto de gasoducto entre Siberia - Europa occidental y como parte de este proyecto pretendía implementar un sistema de automatización y control que le permitiera desempeñar la actividad comercial, los equipos y el hardware necesario para el proyecto ya los había comprado, pero tenía pendiente obtener mediante filtración el software que le permitía finalizar el proyecto. Con este panorama el Ingeniero Weiss ideó la exposición del software manipulado a los agentes rusos para que lo robaran e implementaran en el proyecto. El software manipulado contenía una bomba lógica que transcurrido cierto tiempo ordenaría cerrar las válvulas de gasoducto y aceleraría las bombas provocando así el aumento de presión y el estallido de las tuberías. La bomba lógica estallo a finales de año 1982 y como caso curioso no hubo pronunciamiento oficial de ninguna de las partes, solo se tiene el recuerdo que fue uno de los mayores estallidos no nucleares. Todo el software tecnológico en la Unión Soviética se declaró sospechoso y como coletazo de esto la economía entró en una parálisis general.

6.1.3.4 Ataque intencional y específico por parte de una persona conocedora de un sistema de control industrial en el año 2000. En el año 2000 específicamente el 23 de abril el señor Vitek Boden, el ex empleado de montaje del proyecto de la planta de tratamiento de aguas residuales de la población Morrochy Shire ubicada en del estado de Queensland Australia, atacó el sistema Scada que controla el alcantarillado de aguas residuales compuesto por 142 estaciones de bombeo y dos equipos de cómputo servidores que utilizan tres frecuencias de radio.

El proyecto de Supervisión y Control de la planta de aguas residuales fue ejecutado por la compañía Hunter Watertech Pty Ltda y en este proyecto utilizó tecnología PDS Compact 500 para permitir la gestión, el control y supervisión de las estaciones de bombeo a través de una estación de monitoreo utilizando portadoras con un enlace de radio analógico y bidireccional. V. Boden hombre de 49 años, en un acto de venganza ante la respuesta negativa recibida de parte del concejo de la región en la cual le rechazan la solicitud de ser operario de la planta de tratamiento se infiltró en el sistema de control utilizando equipos y herramientas de software que conoció cuando estuvo como empleado en las actividades de montaje del proyecto. La infiltración al sistema se llevó a cabo a través de un computador externo a la red, desde donde se tomó el control de algunas estaciones de bombeo y se pudo establecer comunicación con el servidor central de monitoreo. Las tramas de comunicación de las estaciones de bombeo fueron modificadas y como consecuencia de esta intervención maliciosa el sistema entro a funcionar con errores, las bombas no encendían en su ciclo normal, el sistema de alarmas local en las estaciones de bombeo perdió comunicación con la estación central y se iniciaron constates pedidas del enlace de comunicación entre los diferentes dispositivos. Como consecuencia de este ataque V Boden fue llevado a la cárcel por un periodo de tiempo considerable desde el 31 de octubre de 2001.

Los investigadores del ataque sr.Yager y el sr. Lewer, coincidieron en afirmar que después de la puesta en operación se observa una gran actividad y tráfico de datos entre el sistema Scada y un punto de bombeo No 14 simulado desde un computador PDS Compact 500 desde donde se manipulo y se hizo colapsar el sistema: V.Boben consiguió el equipo de cómputo mediante robo a la compañía del proyecto meses atrás y en el re-instaló todo el software de gestión y las herramientas de configuración de estaciones de bombeo, del canal de comunicación y del servidor central para poder ingresar como un punto normal de red y desde este punto modificar los set point de controladores y bombas. Después de más de 30 intentos de ingreso no autorizado logro colapsar el sistema, las bombas dejaron de funcionar y se vertió agua residual contaminada a campos, ríos y océano. El sr Janelle Bryant de la Agencia de Protección Ambiental se pronunció en los medios de comunicación

"La vida marina murió, el agua del arroyo se volvió negra y los olores eran insoportables para los residentes", dijo Janelle Bryant de la Agencia de Protección Ambiental de Australia.[13]

---

[13] Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. {En línea}. {12 diciembre 2018}. Disponible en: http://www.scadahackr.com/library/Documents/Case_Studies/Case%20Study%20-%20NIST%20-%20Maroochy.pdf

6.1.3.5 Ataques preparados para las tecnologías de la información "TI" que han afectado los sistemas de control industrial. La gran mayoría de los sistemas de control industrial han sido diseñados e implementados utilizando software y dispositivos tradicionales, entre ellos se pueden mencionar computadores protegidos mecánicamente para evitar interferencias electromagnéticas con funciones de IHM, servidores que contienen el software necesario para gestionar los diferentes protocolos de los clientes, Switches de red y hub para realizar las diferentes interconexiones de los dispositivos que componen la arquitectura de los sistemas.

Los diseñadores y administradores de los sistemas de control han presentado la solución a muchos problemas, pero quizás con el uso de los elementos y dispositivos de las TIC han abierto una gran puerta y han expuesto los sistemas a las grandes campañas de malware que circulan en la red y que pueden causar el mismo daño en TIC o en TO sin tener que preparar campañas especiales.

Entre las campañas de malware que han afectado los sistemas de control industrial se tiene:

Slammer: Se conoce que en el año 2003 este gusano provocó denegación de servicio explotando una vulnerabilidad de desbordamiento de búfer en un producto de Microsoft llamado SQl server. SQL Slammer afecto la planta nuclear de Ohio Davis- Basse desactivando el sistema de supervisión durante 5 horas continuas.

Sobit: En el año 2003 se tuvo noticia de Sobit, un troyano que los atacantes hacían circular vía correo electrónico embebido en un adjunto. Afectó directamente la empresa CSX Jacksonville encargada en el manejo de trenes causando retrasos en los recorridos afectando directamente a los usuarios.

Sasser: En el año 2004 apareció el gusano Sasser que explotaba la vulnerabilidad de desbordamiento de búfer en LASSS (Local Security Autority Subsystem Service) del sistema Windows. Específicamente atacó las IHM de las petroleras del golfo de México, algunas en el Reino Unido y algunos DCS de petroquímicas

Conficker: En el año 2009 la marina francesa se vio atacada por este malware, se hizo circular en una USB infectada que pertenecía a un marinero que conformaba la tropa. Este ataque impidió el despegue de algunos cazabombarderos necesarios en la estrategia militar de los franceses.

6.1.3.6 Ataques al sector energético Night Dragon. Algunos atacantes de la republica China se dieron a conocer con este ataque, afectaron compañías del selector petrolero, del sector de la energía y el sector petroquímico. Establecieron su centro de operaciones en servidores ubicados en Estados Unidos y en Holanda desde donde planeaban, y actuaban utilizando Remote Acces Tool (llamado

zwShell) y DNS dinámicos para obtener acceso remoto ilícito de los computadores infectados y descargar archivos y documentos. En primera instancia Night Dragon atacó la seguridad perimetral de los sistemas informáticos utilizando SQL injection en los servidores de la extranet de las campañas combinado con phishing para obtener las cuentas de usuario y contraseñas de las VPN corporativas.

En la segunda fase Night Dragon aprovechó que ya podía navegar dentro de las redes atacadas y obtuvo cuentas de administrador para crear puertas traseras utilizando proxy inverso y troyanos, así pudo saltar medidas de seguridad como firewalls y desactivar antivirus.

Cuando los atacantes chinos lanzaban zwShell aparecía una caja de dialogo en la máquina indicando un error donde se debería ingresar la contraseña que posteriormente fue publicada por los investigadores del ataque “zw.china”, al ingresarla se ejecutaba el control remoto y se permitía la creación del troyano, la configuración de los puertos y la selección del servidor holandés o en los Estados Unidos.

6.1.3.7 El gran ataque: stuxnet año 2010. Este malware es el “boom” de los ataques contra las infraestructuras críticas, y una definición palpable de la ciberguerra. Ataca directamente la capa física e intenta actuar sobre las salidas binarias de los PLC siemens S7 que controlan los rotores utilizados en las centrifugadoras de gas para el enriquecimiento de uranio utilizado como combustible nuclear en armas nucleares y los reactores en la central de Natanz, núcleo del programa nuclear de Irán.

Aunque el ataque está dirigido directamente al mundo real, es decir lo que se pretende es modificar el control, de las centrifugadoras se utilizaron 3 capas para obtener la infección y el ataque.

- Capa para desplegar y expandir el malware: en esta capa se utilizaron 4 vulnerabilidades de día cero es decir no tenían parches que la solucionaran y hasta el día del ataque eran desconocidas, y técnicas de infección que son de uso reservado para la estrategia de algunos gobiernos.

- Capa de Control: para manipular el sistema, pero sin detenerlo. El ataque fue tan ingenioso que cuando se producía la modificación del Set Point por parte del troyano para aumentar la velocidad de los rotores el operario no podía advertir ni darse cuenta porque los datos que se mostraban en las IHM correspondían a un funcionamiento normal del sistema.

- Capa física donde se pretende actuar sobre las salidas de los PLC Siemens.

Por las características militares de la central nuclear Natanz, Stuxnet fue ideado extra oficialmente por los Estados Unidos e Israel para repartirse en una USB con el malware instalado (contenía 2 accesos directos y 2 archivos temporales), la estrategia fue seleccionar uno de los científicos con acceso a los equipos objetivos que trabajaba dentro de la central y entregar el dispositivo infectado para que ingenuamente lo llevara dentro de la instalación. Inicialmente se creyó que esta infección tenía la propiedad de propagarse solo por las maquinas, pero investigadores coincidieron en afirmar que el código utilizado en Stuxnet no es capaz de realizarlo.

Cuando el usuario victima abría la carpeta en la USB se ejecutaba la primera de las vulnerabilidades de día cero ejecutando un programa en shell32.dll, además utilizando técnicas de rootkit desaparecía para impedir que la víctima sospechara del ataque, una de las técnicas utilizadas por Stuxnet que sorprende mucho es la capacidad de detectar comunicaciones entre registros tipo 4 del PLC S7 y los servidores del sistema de control.

Con este ataque a la central de Irán se pudieron afectar según informes alrededor de 1000 máquinas y la carrera nuclear de este país tuvo un retroceso significativo. Para finales de 2018 la recuperación y los avances son muy considerables. Cabe notar que el diseño de la central nuclear había sido robado en la guerra fría por Abdul Qadir Khan científico pakistaní.[14]

6.1.3.8 Sktwiper o flame o flamer año de 2012. Se conoce de este poderoso malware el 28 de mayo de 2012, se caracteriza por su forma de propagación, por la identificación de objetivos concretos, la explotación de vulnerabilidades 0day, por su evolución y por su arquitectura con que fue diseñado. Flame es muy sofisticado aunque no ataca directamente los equipos y dispositivos del bus de control en los sistemas industriales de control como lo hizo Stuxnet, tiene una serie de programas para realizar tareas de espionaje y sabotaje, para grabar conversaciones, permite control remoto en las maquinas infectadas, tiene un módulo de bluetooth que secuestra y maneja los teléfonos móviles aledaños, copia y transmite datos a un servidor remoto, se puede afirmar que cronológicamente Flame se sucedió después de Stuxnet pero la capacidad de infectar y destruir no solo se orienta al programa nuclear iraní, sino también a servicios públicos como las redes bancarias, los sistemas masivos de transporte, los sistemas aéreos, las centrales eléctricas, las redes de trasmisión de energía y muchos más.

[14] BOLIVAR. Infraestructuras críticas y sistemas industriales. Auditorias de seguridad y fortificación. Primera edición. Madrid. 0Xword. 2016. Páginas 67;70

Dentro de los programas que se encuentran en Flame está el archivo DLL mssecmgr.ocx, en las primeras investigaciones se encuentran archivos de gran tamaño con driver y programas adicionales (aproximadamente 6 MB) pero posteriormente la estrategia cambió y se redujo a tan solo 900 Kb de tal manera que el programa se instala y hace conexión con servidores remotos para terminar de instalar los componentes restantes que complementan el archivo DLL. Una vez instalados todos los módulos el malware se auto registra en el registro de Windows “Authentication packages = mssecmgr.ocx”

Este poderoso malware contiene módulos específicos para cada propósito y objetivo entre estos módulos se encuadran los siguientes:

Beetlejuice: Este módulo le permite a Flame enumerar los dispositivos alrededor de la máquina infectada.

Microbe: Con este módulo Frame lista todos los dispositivos multimedia de la máquina y de red, junto con sus configuraciones para ser utilizados en el momento adecuado.

Infectmedia: Con este módulo Frame infecta los dispositivos USB que sean utilizados en el sistema.

Limbo: Frame crea cuentas de usuario con este módulo.

Weasel: Con este módulo Frame crea un listado de las máquinas que ya han sido infectadas.

Gator: Frame supervisa contantemente las conexiones a Internet y cuando detecta una conexión disponible se conecta a los servidores remotos para bajar o actualizar nuevos módulos y al mismo tiempo sube los datos ya recogidos de la máquina víctima.

Security: Con este módulo Frame identifica los posibles peligros que puede encontrar en el sistema atacado como antivirus, Firewalls. IDS. IPS.

Flame utiliza el lenguaje de programación LUA como eje principal, LUA significa en portugués luna, es un programa muy veloz y estructurado que le permite utilizar sub rutinas de C++ y múltiples métodos de cifrado[15].

[15] BOLIVAR. Op.cit. Páginas 71;72

6.1.3.9 Dragonfly/ havex. Las campañas de ataques contra la industria farmacéutica, los sistemas de control industriales y sistemas Scada del sector energético en Europa y parte de los estados unidos continúan en el año 2013 - 2014 a cargo del grupo de ciber espionaje denominado DragonFly. Los investigadores comparan la técnica, brillantez y la ejecución estratégica que tienen los ataques de DragonFly con el boom de Stuxnet, (Dragonfly no utilizo 0-day).

Así como Stuxnet los ataques que ejecuta DragonFly se caracterizan por tener en su arsenal cargas dirigidas a los equipos del bus de control como son los PLC o IED´s en general. Posee alto potencial para extraer datos del Outlook, datos de sistemas de control industrial y datos de servidores OPC.

El ataque tiene dos componentes de malware los cuales se convierten en dos herramientas de acceso remoto RAT a la maquina infectada.

El primer componente de este ataque es Havex, algunos investigadores lo conocen también como backdoor Oldrea, su función principal es extraer datos de la libreta de direcciones del Outlook y datos contenidos en la computadora de gestión del sistema de control que estén relacionados con el software utilizado para el control y la supervisión del sistema. De Havex se tiene una variante de las 88 conocidas y es aquella que se caracteriza por buscar la información relacionada con los servidores OPC.

El segundo componente es el troyano Kragany, que le permite a DragonFly descargar y cargar archivos en las maquinas infectadas, adicionalmente este componente tiene funciones para descargar en los servidores de comando y control C&C previstos por DragonFly la información del sistema, recolecta contraseñas, toma captura de pantallas, elabora lista de documentos que serán utilizados para nuevos ataques.

DragonFly hace presencia en los sistemas industriales utilizando tres tipos de vectores de ataque.

Primer vector, campaña por correo electrónico: Explotación de la vulnerabilidad CVE- 2011-0611[16]. Ejecutivos e ingenieros de campo fueron atacados con archivos pdf´s adjuntos que contenían código malicioso.

Segundo vector, por visita a sitios web: Los sitios web que generalmente visitan las personas que trabajan en el sector eléctrico se infectaron, esto hacía que la consulta fuera redirigida a otros sitios comprometidos y que tienen un kit de

[16] CVE-20011-0611. {En línea}. {12 diciembre 2018}. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611

explotación con la propiedad de instalar las herramientas de acceso remoto RAT para su posterior uso.

Tercer Vector, descarga de software relacionado con los sistemas de control: DragonFly infectó algunos de los vendedores de software industrial e incluyó las herramientas de acceso remoto RAT[17].

6.1.3.10 Ataques al sector eléctrico en ucrania 2015, Blackenergy. La compañía AES Kyivoblenergo encargada de la comercialización y distribución regional de energía eléctrica en Ucrania, país de Europa oriental fue víctima de un ataque cibernético en tres de sus subestaciones principales simultáneos y coordinados el 23 de diciembre de 2015 desde las 15.35 horas y duró aproximadamente tres horas ocasionado desconexiones a sus clientes. Las autoridades de Ucrania afirmaron en comunicado oficial que los ataques se originaron desde los servidores de seguridad rusos.

En este ataque a la red eléctrica se afectaron siete subestaciones de 115 kV y veintitrés subestaciones de 34.5kV que dejaron sin energía eléctrica a aproximadamente 225000 clientes.

Se hizo uso de diversas capacidades de ataques, phishing, variantes de BlackEnergy2, manipulación de documentos de office, ingeniería social, robo de credenciales, uso de herramientas remotas para conexión con las IHM, modificación del Firmware en los dispositivos ethernet –serie, uso de KillDisk para borrar el arranque en frio de los sistemas, bloqueo de las UPS y denegación de servicio en el call center.

Meses atrás los administradores de la red corporativa de la compañía recibieron un correo electrónico con una macro en Word que contenía BlackEnergy3 y que facilitó la instalación del troyano. Con el troyano dentro del sistema se permitió la comunicación con los servidores de comando y control C&C, se escalaron privilegios y se obtuvieron las credenciales necesarias de la VPN para ingresar el sistema de control y supervisión de la compañía Kyivoblenergo.

Se desarrollaron dos herramientas para el ataque, el primer desarrollo permitió entender y establecer comunicación con los dispositivos que gestionan los sistemas de control y el segundo consistió en la creación de un firmware troyanizado para los conectores ethernet. Serie, utilizados en el bus de proceso del sistema. Estos dos desarrollos unidos con una serie de pasos y métodos de

[17] Dragonfly. Espía de la energía. {En línea}. {12 diciembre 2018}. Disponible en: https://www.symantec.com/es/mx/outbreak/?id=dragonfly

ciberataque permitieron bloquear los servidores de operación de las subestaciones eléctricas, quitando así el control y la operación al personal de la compañía para finalmente utilizar las IHM en cada subestación y realizar comandos de apertura sobre los interruptores de potencia que permiten la conexión de los usuarios con el sistema de energía.

Como ingrediente final de este ataque y quizás para generar aún más desconcierto y frustración entre usuarios y compañía, se generó una denegación de servicio DDoS en el call center impidiendo la comunicación de los usuarios para reportar los sucesivos cortes de energía.[18]

6.1.3.11 Ataques al sector eléctrico en ucrania 2016, Industroyer. En Ucrania en la capital Kiev, el 17 de diciembre a las 22:27 horas del 2016 aparece el primer malware diseñado específicamente para atacar plantas generadoras de energía y subestaciones eléctricas aprovechando la virtualización en nodos lógicos de los equipos de conmutación en alta potencia, curiosamente ninguna torre fue derribada, no se atentó contra el cable de potencia, no hubo explosiones en los equipos de instrumentación de las subestaciones, no hubo rastro de humo en los auto transformadores ni se escucharon fuertes detonaciones, pero si gran parte de la capital se quedó sin suministro de energía a causa de un ataque contra la red eléctrica del país.

La estrategia utilizada fue entrar a las estaciones de trabajo que utilizan sistema operativo Windows y una vez dentro del sistema, los ciber atacantes desplegaron toda una gran ingeniería para lograr explotar una vulnerabilidad presente CVE-2015-5374[19] en los dispositivos electrónicos inteligentes IED Siemens Siprotec 5 utilizados en el bus de proceso del sistema de supervisión y control de las subestaciones eléctricas. Además de dejar bloqueados e inservibles los IED´s utilizaron técnicas para borrar el rastro del ataque, sobre escribir archivos y bloquear el correcto reinicio de los servidores afectados impidiendo la restauración del sistema de control.[20]

---

[18]. BOLIVAR, Juan Francisco. Infraestructuras críticas y sistemas industriales. Auditorias de seguridad y fortificación. Primera edición. Madrid 0Xword. 2016. Páginas 74,78

[19] CVE-2015-5374. {En línea}. {12 diciembre 2018}. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5374

[20] INCIBE. CrashOverride: El malware para SCI ataca de nuevo. {En línea}. {12 diciembre 2018}. Disponible en: https://www.certsi.es/blog/crashoverride-el-malware-sci-ataca-nuevo

6.1.3.12 Análisis completo del Ataque al sector Eléctrico por Industroyer / Crashoverride. Después del corte de energía que duró aproximadamente una hora y 15 minutos sucedidos en la subestación eléctrica ubicada en la zona de Novi Petrivtsi al norte de Kiev capital de Ucrania el 17 de diciembre de 2016, los directivos de la compañía Kyivoblenergo contrataron formalmente a Eset y a Dragos, especialistas en ciberseguridad para aclarar los hechos sucedidos[21].

En los informes presentados por cada uno de ellos se refirieron al ataque cibernético como Win32 / industroyer por parte de Eset y CashOverrride por Dragos, Los investigadores coincidieron en informar que es una de las más grandes amenazas diseñadas para el sector eléctrico mundial por su característica modular, adaptable, personalizable y por la estrategia utilizada ya que no busca infectar el sistema si no busca tomar el control con comandos a los interruptores de potencia, desplazando los protocolos de comunicación previstos inicialmente para este fin[22].

6.1.3.13 Descripción del Malware. CrashOverride que en adelante llamaremos Industroyer para facilitar la comprensión, es un malware modular diseñado para atacar sistemas de control de infraestructuras críticas en las cuales se utilizan los estándares IEC 60870-5-101, 104, 61850 y OPC. Dentro de las acciones que se realizan en el ataque se puede tener las siguientes.

Bloqueo y desplazamiento de los puertos seriales en los servidores con SO Windows para impedir que el protocolo (101,104, 61850, OPC) implementado en la arquitectura inicial se comunique con los dispositivos del bus de control.

Envió de comandos de cierre y/o apertura de forma repetitiva sobre los interruptores de potencia, sobre los seccionadores de potencia, sobre los cambiadores de taps en los autos trasformadores y en general todos los comandos que estén configurados en la Unidad terminal remota RTU o en el Sistema de Automatización de Subestaciones SAS.

Realiza un escaneo de puertos en las computadoras o IED´s conectados en la red para identificar posibles protocolos de comunicación con otros dispositivos.

---

[21] DRAGOS. CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. {En línea}. {12 diciembre 2018}. Disponible en: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[22] CHEREPANOV, Anton. WIN32/INDUSTROYER A new threat for industrial control system. {En línea}. {12 diciembre 2018}. Disponible en: https://www.welivesecurity.com/wp-ontent/uploads/2017/06/Win32_Industroyer.pdf

Realiza borrado de archivos, log de eventos, borrado de registros, o de cualquier otra evidencia que permita rastrear el ataque, utilizando un módulo Wipe que garantiza que la información borrada no se puede recuperar.

Explota la vulnerabilidad CVE-2015-5374 en la variante de Firmware PROFINET IO para los módulos EN100 Ethernet de los equipos siemens Siprotec que provoca denegación de servicio dejando los IED´s sin posibilidad de interactuar con los demás equipos conectados en la red.

6.1.3.14 Funcionamiento. Los investigadores no han encontrado ningún rastro que les permita afirmar que Industroyer recicló o retomó alguna parte de código de los ataques de años anteriores al sector eléctrico; por su forma modular y por su funcionabilidad se puede afirmar que en él se refleja parte de Stuxnet por la forma en que conoce el sistema y determina como tomar el control, parte de DragonFly/havex por la forma como mapea los puertos y parte de BlackEnergy2 por la forma como interpreta los archivos y librerías contenidos en la API de la RTU o de la IHM para interpretar el entorno y conectarse lo más rápido posible con su centro de comando y control C&C alojados en la red TOR.

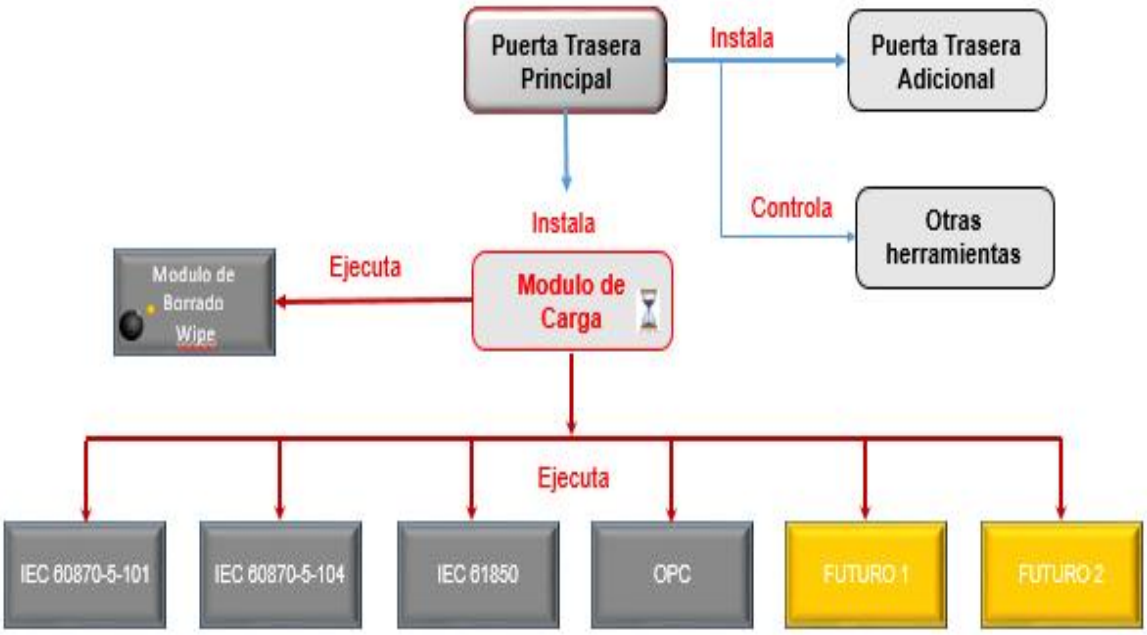
6.1.3.15 Vector de Ataque. La necesidad primordial de los autores del ataque fue ingresar al sistema por la puerta trasera principal o backdoor principal, para que se pudieran instalar los demás componentes, se presume que el vector de ataque utilizado fue el phishing utilizando correo electrónico que permitiera engañar al personal de operación de la subestación eléctrica. Con esta interpretación y por los módulos que tiene Industroyer no se ve la posibilidad que el malware se propague por la red.

6.1.4 Descripción de los Módulos de Industroyer. Industroyer es modular, en este malware se encuentran los siguientes módulos.

6.1.4.1 Puerta trasera Principal. Se considera el módulo principal de Industroyer, su función es instalar y controlar las demás herramientas necesarias para el ataque y establecer la comunicación vía HTTPS con los servidores de comando y control C&C para posteriormente recibir órdenes de los autores del ataque. En las muestras tomadas se encontró que la puerta trasera principal tenía asignada un proxy específico de la red local del sistema y unas líneas de código de programación que le iban a permitir estar activo o disponible después de transcurridas dos horas de la instalación de los módulos necesarios.

También los autores de Industroyer tuvieron en cuenta que el mejor horario para conectar el malware con los C&C sería en horas nocturnas preferiblemente cuando el horario laboral de operación hubiese terminado.

Figura 1. Módulos de Industroyer



Fuente: Los autores

6.1.4.2 Puerta trasera adicional. La puerta trasera adicional, es una muestra de que los autores del malware conocen el sistema y saben cómo atacarlo, la puerta trasera adicional la instalaron una vez se escalaron privilegios de administrador con la puerta trasera principal y mediante el uso de herramientas adicionales. Su función es retomar el control del sistema atacado cuando la puerta trasera principal ha sido dada de baja o se ha desactivado.

El malware troyanizó la versión original del block de notas del sistema operativo Windows insertando código malicioso que se ejecuta y hace su función de comunicación con C&C diferentes a los de la puerta trasera principal cada vez que la aplicación se inicia. Para que los usuarios del block de notas no notaran la ejecución de código malicioso, el malware dejo intacto la funcionalidad del block de notas solo que le adicionó una función especial.

Figura 2. Block de Notas Troyanizado

BLOCK DE NOTAS ORIGINAL

```
.text:01004AD5     lea     eax, [ebp+var_50]
.text:01004AD8     push    eax
.text:01004AD9     lea     eax, [ebp+h]
.text:01004ADC     push    eax
.text:01004ADD     push    0B0h
.text:01004AE2     push    hWnd
.text:01004AE8     mov     stru_100A680.lStructSize, 58h
.text:01004AF2     mov     stru_100A680.hwndOwner, edx
.text:01004AF8     mov     stru_100A680.nMaxFile, 104h
.text:01004B02     mov     stru_100A500.lStructSize, 28h
.text:01004B0C     mov     stru_100A500.hwndOwner, edx
.text:01004B12     call    esi ; SendMessageW
.text:01004B14     push    [ebp+var_50]
.text:01004B17     push    [ebp+h]
.text:01004B1A     push    0B1h
.text:01004B1F     push    hWnd
.text:01004B25     call    esi ; SendMessageW
.text:01004B27     push    ebx
.text:01004B28     push    ebx
.text:01004B29     push    0B7h
.text:01004B2E     push    hWnd
.text:01004B34     call    esi ; SendMessageW
.text:01004B36     push    ebx
.text:01004B37     call    ds:GetKeyboardLayout
.text:01004B3D     and     ax, 3FFh
.text:01004B41     cmp     ax, 11h
.text:01004B45     jnz     short loc_1004B58
.text:01004B47     push    1
.text:01004B49     push    1
.text:01004B4B     push    0D8h
.text:01004B50     push    hWnd
.text:01004B56     call    esi ; SendMessageW
```

BLOCK DE NOTAS TROYANIZADO

```
.text:01004AD5     lea     eax, [ebp+var_50]
.text:01004AD8     push    eax
.text:01004AD9     lea     eax, [ebp+h]
.text:01004ADC     push    eax
.text:01004ADD     push    0B0h
.text:01004AE2     push    hWnd
.text:01004AE8     mov     stru_100A680.lStructSize, 58h
.text:01004AF2     mov     stru_100A680.hwndOwner, edx
.text:01004AF8     mov     stru_100A680.nMaxFile, 104h
.text:01004B02     mov     stru_100A500.lStructSize, 28h
.text:01004B0C     mov     stru_100A500.hwndOwner, edx
.text:01004B12     call    esi ; SendMessageW
.text:01004B14     pusha
.text:01004B15     pushf
.text:01004B16     neg     ebx
.text:01004B18     shr     eax, 1
.text:01004B1B     dec     ebx
.text:01004B1C     mov     eax, 17B200AFh
.text:01004B21     mov     edi, 71CFC28h
.text:01004B26     or      edi, dword_10095C7
.text:01004B2C     xor     esi, 1C779E91h
.text:01004B32     xor     eax, eax
.text:01004B34     dec     edi
.text:01004B35     rol     esi, 5
.text:01004B38     and     esi, edi
.text:01004B3A     and     esi, edi
.text:01004B3C     rol     edx, 6
.text:01004B3F     neg     eax
.text:01004B41     xor     esi, eax
.text:01004B43     neg     ebx
.text:01004B45     shr     ebx, 5
.text:01004B48     mov     ecx, 5E9542h
```

Fuente: CHEREPANOV, Anton. Win32/industroyer a new threat for industrial control systems.

6.1.4.3 Módulo de carga. Es un ejecutable, lanza en un tiempo establecido un DLL que ataca el protocolo que se esté utilizando en el sistema de control y cuenta dos horas para lanzar el módulo Wipe. Como estrategia del ataque el malware modificó la prioridad en que se ejecutan estos dos sub procesos en “THREAD_PRIORITY_HIGHEST” y con esto garantizó recurso de maquina al momento de ejecutarse.

El módulo Wipe una vez lanzado, borra todas las claves de registro del sistema, borra los archivos de configuración del disco duro, y borra las unidades de red que haya podido mapear. En las muestras tomadas del malware los investigadores encontraron que este módulo estaba especialmente configurado para borrar archivos propios del IED ABB que son gestionados con la herramienta de software PCM 600. Esta herramienta de configuración PCM600 exporta archivos de las siguientes extensiones utilizadas en la configuración IEC 61850 del proyecto:

.pcmp: Corresponde al archivo del árbol de proyecto con las carpetas de los IED utilizados.
.pcmi: Corresponde al archivo de configuración de la comunicación.
.scd: Corresponde al archivo de descripción de configuración de la subestación.

.cid: Corresponde al archivo de la descripción de configuración del IED en particular.
.cin: Corresponde al archivo que utiliza MicroScada en la configuración.

También el malware estaba configurado para sobre escribir los archivos de Windows con el propósito de dejarlo fuera de uso.

6.1.4.4 Módulo de ataque para el protocolo IEC 60870-5-101. También conocido como Payload 101 o carga útil 101. El protocolo IEC 60870-5-101 se utiliza en los controles de las subestaciones eléctricas para permitir la comunicación entre un sistema Scada maestro y la terminal remota RTU que hoy en día vienen siendo remplazadas por los convertidores de protocolo o Gateway en los SAS actuales. A través de este protocolo se envía la posición de equipos o Scada de la subestación y se reciben comandos de cierre y apertura dirigidos a los equipos de maniobra en el patio de conexiones. La medida de las variables eléctricas procesadas en la subestación también se envía por este protocolo.

El Payload 101 es un archivo de nombre IEC 101.DLL que implementa el protocolo, desplaza el puerto serial utilizado COM1 o COM2 y los otros puertos los deja abiertos para impedir que sean utilizados, se comunica con la RTU, SAS o con cualquier otro dispositivo que tenga el protocolo implementado. Para ejecutar los comandos sobre los equipos de maniobra analiza el archivo .ini del SAS o API de RTU y de este archivo extrae las direcciones IEC para materializar el comando. Para los comandos dobles el Payload 101 implementa toda la secuencia del protocolo, es decir primero realiza la selección del dispositivo y una vez confirmada la selección modifica el bit del comando.

6.1.4.5 Módulo de ataque para el protocolo IEC 60870-5-104. También conocido como Payload 104 o carga útil 104. El protocolo IEC 60870-5-104 es una extensión del 101. Este protocolo utiliza la red TCP / IP para establecer comunicación con los equipos de la red, lo que lo hace flexible y configurable.

Así como en el payload anterior el ataque se realiza interpretando el archivo de configuración “Estación “cuya ruta de ubicación se extrajo previamente en el módulo de carga. El archivo de estación puede tener configuradas una o varias IP a las cuales el archivo 104.DLL del ataque intentara comunicarse y finalizar el proceso de comunicación D2MultiCommService.exe para desplazarlo y montar una comunicación ficticia. Esta comunicación ficticia envía paquetes a la dirección ASDU de cada equipo e intenta modificar las entradas y salidas de los equipos de proceso.

Módulo de ataque pare el protocolo IEC 61850. Este protocolo es uno de los más implementados en las subestaciones eléctricas y centrales de generación, con él se realiza el control del bus de proceso por la facilidad que tiene de comunicar varios fabricantes de IED´s como Siemens, ABB, Sel, Toshiba, etc.

El payload 61850.exe busca en el archivo de configuración las direcciones IP de los IED´s de la red, en caso de no obtenerlas porque el archivo no existe, entonces este componente enumera todos los adaptadores de red conectados para determinar sus máscaras de subred TCP / IP. El payload 61850 luego enumera todas las direcciones IP posibles para cada una de estas máscaras de subred y se conecta al puerto 102 en cada una de esas direcciones.

Una vez que el payload 61850 se conecta a un host de destino, envía un paquete de solicitud de conexión.

Si el dispositivo de destino responde adecuadamente, luego envía un paquete InitiateRequest utilizando la mensajería MMS. Si se recibe la respuesta esperada, continúa, enviando una solicitud getNameList de MMS.

El payload 61850 analiza los datos recibidos en respuesta a estas solicitudes, buscando variables que contengan los nodos lógicos y sus atributos CSWI, CF, ST, Pos y stVal • CSW, CO, Pos, Oper.

Ubicados los nodos lógicos que relacionan interruptores y seccionadores intentara cambiar el valor sTval de SBO y XCBR, el primero lo selecciona y el segundo lo opera para cambiar la posición.

6.1.4.6 Notpetya – Industroyer Telebots – Apt. Tras la aparición del falso ransomware Not petya o Discoder C después de WannaCry, el 27 de junio de 2017 se produjeron daños en una parte significativa del sector financiero mundial pues se causó borrado de discos duros. Los investigadores han encontrado que esta variante de ransomware tiene similitudes con la puerta trasera utilizada en industroyer. Las tareas de investigación se han venido complementando desde antes del año 2015 y con los sucesos ocurridos con BlackEnergy se ha podido establecer, aunque no se afirma por completo que los ataques a las infraestructuras críticas del sector eléctrico en Ucrania y otras partes del mundo tienen el modelo y las herramientas del grupo de ciber delincuentes APT o también conocido como Sandworm. Esta corriente de investigación se ha venido desviando ya que aparentemente APT 28 ha dejado de actuar para convertirse en TeleBots actual autor de los ataques con NotPetya.

Las similitudes de código utilizadas, las infraestructuras en servidores de comando y control C&C, las cadenas de ejecución de malware entre otras conjeturas que se venían manejando en la investigación se afirmaron el 13 de abril de 2018 cuando

se descubrió una nueva campaña del grupo TeleBots para desplegar una puerta trasera conocido como Exaramel en el sector comercial, versión mejorada de la puerta trasera principal utilizada en 2016 por Industroyer.

6.1.4.7 El malware Triton, una amenaza grave paras los sistemas industriales de seguridad. En enero de 2018 se conoció el malware diseñado para modificar la programación de los controladores Triconex fabricados por Schneider Electric, que son altamente utilizados en sistemas industriales de seguridad SIS en la industria y en el sector eléctrico en el Medio Oriente, países como Arabia, Emiratos Árabes, Irán y muchos más se podrían ver afectados. Tritón o Trisis o HatMan fue diseñado para provocar un daño físico de grandes magnitudes en la industria, su función principal es evitar que los sistemas industriales de seguridad ejecuten la función programada y a cambio de esto permitan el control del sistema a un tercero ilegal probablemente apoyado por el gobierno ruso. El malware ataca las estaciones con sistema operativo Windows que gestionan el sistema SIS haciéndose pasar por una aplicación legal y una vez dentro inyectan código malicioso para que el sistema de seguridad ignore cualquier situación peligrosa, poniendo en peligro el proceso que se esté llevando a cabo junto con los operarios de la planta.

Los controladores Triconex utilizan el protocolo de comunicación propio del fabricante de nombre TriStation en la implementación de sistemas industriales de seguridad SIS, del cual no se tiene información pública, por lo que los investigadores presumen que los autores del ataque han tomado el protocolo y a través de ingeniería inversa han descubierto las tramas de comunicación o en su defecto han desarrollado un protocolo independiente que les ha permitido realizar el ataque[23].

6.1.4.8 Análisis de ataques al sector eléctrico en Colombia. “Solo existen dos tipos de empresas: aquellas que han sido atacadas, y otras que lo serán en el futuro”, Robert Mueller, Director FBI 2012.

En Colombia los ataques cibernéticos se multiplican día a día, las estadísticas de las compañías aseguradoras indican que los sectores industriales son más propensos a sufrir ataques, el sector energético está en segundo lugar y le siguen las entidades de servicios financieros.

---

[23] Malware Triton vinculado al Instituto de Investigación del Gobierno Ruso. {En línea}. {12 diciembre 2018}. Disponible en: https://www.disoftin.com/2018/10/malware-triton-vinculado-al-instituto.html

Las infraestructuras críticas de Colombia están expuestas a ataques de ciber delincuentes locales e internacionales y en algunos casos a organizaciones trasnacionales organizadas, lo que hace pensar que se deben implementar medidas de seguridad prioritarias. La tarea que se debe enfrentar es muy retadora, no es fácil ubicar a un delincuente cibernético en Colombia y mucho menos en el exterior porque desde cualquier café internet de barriada, o computadora portátil, o Tablet e incluso desde un teléfono móvil se puede atentar contra la infraestructura crítica y de la misma manera eludir la responsabilidad legal. El fácil acceso a la información ilegal, la dificultad de rastreo para los servidores de comando y control ubicados en la red Tor, y el intercambio comercial establecido con monedas virtuales han facilitado que el escenario delincuencial cada día se expanda.

En la séptima cumbre latinoamericana de seguridad realizada en Argentina en el año 2017, se aseguró que américa latina tuvo un aumento del 59% en el número de ciber ataques en 2017 y Colombia se encuentra entre los países más afectados.

A partir de las denuncias realizas en la plataforma del Centro Cibernético de la policía nacional se ha podido caracterizar el delito informático en Colombia de la siguiente forma:

En los últimos tres años el ciber delincuente ha cambiado de victima pasando del ciudadano común a las grandes empresas del sector privado colombiano.

Aparecen nuevas plataformas de correo electrónico para desde ahí lanzar campañas de phishing.

El ciber delincuente se esconde en los servicios en línea del sector gubernamental para distribuir malware.

Vinculación de ciber delincuentes extranjeros en las organizaciones colombianas dedicadas a los ciber ataques en la red.

Uso y presencia de gran número de colombianos en la Deep Web.

Uso de la red de internet para crear grupo de ciber delitos.

Uso de monedas virtuales para legalizar delitos.

6.2 ESTUDIO DEL ESTÁNDAR IE61850 Y ANÁLISIS COMPARATIVO DE ATAQUES REALIZADOS Y SUS CARACTERÍSTICAS (DRAGONFLY, BLACKENERGY, STUXNET, INDUSTROYER 2016)

6.2.1 Los Sistemas industriales y el Estándar IEC61850.

6.2.1.1 Sistemas de Control para Subestaciones Eléctricas

6.2.1.1.1 Subestación eléctrica. Una subestación eléctrica se define como un conjunto de obras complementarias y de equipos conectados lógicamente de tal forma que permitan direccionar, transformar y redistribuir el flujo de energía en un sistema de potencia. Las subestaciones eléctricas están conformadas por equipos de patio, por equipos de protección o relés de protección, por equipos de control y equipos de telecomunicaciones.

6.2.1.1.2 Patio de conexiones de una subestación alta tensión. El patio de conexiones de una subestación eléctrica es un espacio generalmente al aire libre, demarcado y delimitado, donde se encuentran conexionados físicamente los equipos de maniobra o equipos operables como interruptores, seccionadores, pararrayos, transformadores de instrumentación, transformadores de potencia entre otros y las barras de conexión de la subestación.

La conexión de los diferentes equipos de patio, dan pie a las diferentes configuraciones o arreglos que de una u otra forma facilitan el mantenimiento y la operación de los equipos.

6.2.1.2 Tipo de Configuraciones de una subestación eléctrica. Una subestación eléctrica se distingue por el tipo de conexión o arreglo en que estén sus equipos de maniobras (interruptores - seccionadores) en un nivel de tensión determinado. Este arreglo se selecciona en la etapa de concepción y de diseño, con base en los requerimientos de confiabilidad que se necesiten para prestar el servicio. Lo que se busca es que la subestación no interrumpa el suministro o transformación de potencia cuando un equipo de maniobra este en falla o en mantenimiento.
Equipos y dispositivos característicos de una subestación eléctrica

- Seccionador. Dispositivo de maniobra que aísla parte de la subestación para mantenimiento. No tiene la capacidad de interrumpir o establecer corrientes, salvo casos especiales.

- Seccionador o cuchilla de puesta a tierra. Dispositivo que, mediante operación manual, conecta las líneas de trasmisión o los transformadores a la malla de puesta a tierra de la subestación por requerimiento especial o por mantenimiento.

- Interruptor. Dispositivo de maniobra capaz de interrumpir o establecer las corrientes eléctricas del circuito, tanto nominales como de falla o cortocircuito.

- Barraje de la subestación. En una subestación se pueden tener más de una barra y se define como el punto común de conexión de los circuitos del mismo nivel de tensión.

- Bahía. Es el conjunto de equipos de maniobra necesarios para conectar un transformador, un equipo de compensación, una línea de trasmisión a la barra de una subestación. A los equipos de maniobra que se utilizan para seccionar o acoplar las barras de la subestación también se les denomina bahía.

Las configuraciones más conocidas en el sector eléctrico colombiano son:

Configuración barra sencilla: en esta configuración se encuadran dos seccionadores a lado y lado del interruptor y un seccionador de línea con su respetivo seccionador de puesta a tierra. Se considera una configuración muy básica y rígida a la vez. No permite desconexiones con suplencia por lo que es necesario realizar desconexiones totales de la subestación.

- Configuración Barra principal más barra de transferencia. En esta configuración se tiene la ventaja que el interruptor de la bahía se puede remplazar por el interruptor de transferencia, con la limitación que si no se dispone de un dispositivo para transferir los disparos por protecciones de un interruptor a otro no se puede llevar a cabo la transferencia.

- Configuración doble barra. Esta configuración permite separar los circuitos en dos en dos barras, es como si la subestación se convirtiera en dos, aumentando con esto la flexibilidad de la subestación.

- Configuración doble barra más seccionador de transferencia. Esta configuración une dos configuraciones, la de transfería y la doble barra haciéndola muy apetecida porque aumenta la confiabilidad y flexibilidad.

- Configuración doble barra más seccionador de “By pass”. Esta configuración tiene un seccionador que en conjunto con el campo de acople permiten sacar el interruptor principal de la línea sin afectar la transferencia.

- Configuración interruptor y medio. Esta configuración tiene tres interruptores que unen las dos barras de la subestación y utiliza dos de ellos por cada bahía de línea, de esta forma el interruptor del corte central es compartido para cada bahía. Esta configuración es muy flexible y se utiliza cuando en una subestación se manejan más de cuatro bahías que se conectan a las barras.

- Configuración en anillo. En esta configuración se tiene tantos interruptores como circuitos a manejar. Tiene la dificultad que no permite ampliaciones de la subestación fácilmente.

6.2.1.3 Transformadores de instrumentación. Los trasformadores de instrumentación son equipos encargados de aislar y transformar las variables eléctricas (Corriente y Tensión) en valores secundarios, tales que se puedan incorporar a los circuitos de los relés de protección y los IED de control.

Estos dispositivos generalmente acoplados e instalados en el patio de conexiones de la subestación tienen un devanado primario y varios devanados secundarios con un nivel de precisión para permitir un reflejo exacto de la medida de los circuitos conectados.

- Transformador de Corriente CT. El transformador de corriente tiene como función aislar los circuitos de medida y de protección de las altas tensiones del patio de conexiones. El CT adapta la corriente que circula en los circuitos secundarios de la sala de control haciéndola fácilmente manejable. Un ejemplo típico de la función de este transformador en las subestaciones de alta y extra alta tensión es adaptar la corriente nominal de 1000 Amperios en alta a 1 amperio en los circuitos secundarios con el mismo ángulo de fase.

- Transformador de Tensión PT. El transformador de tensión se conecta en paralelo con líneas o barrajes en el patio de conexiones de la subestación para transformar y asilar las tensiones de alta y adaptarlas a los circuitos secundarios de las protecciones y el control. En las subestaciones de alta y extra alta tensión estos transformadores típicamente tienen una relación de transformación de 2000 a 1, así si se tienen 230 kV en alta el dispositivo reducirá la tensión a 115 v en los circuitos secundarios.

6.2.1.4 Tipos de control en una subestación eléctrica. El control de las subestaciones eléctricas desde sus inicios tiene similitud con los sistemas de control industrial, en ellos fácilmente se identifican los niveles característicos de la de la pirámide de control.

- Nivel de Campo

- Nivel de Control de Bahía

- Nivel de Control de subestación

El control de una subestación eléctrica es diseñado para suministrar los métodos y los medios al personal de operación, se convierte en la interface entre los equipos del nivel de campo y el administrador de la red, los sistemas de control de subestación deben contener la lógica de enclavamientos que brinde seguridad en la operación local y en las operaciones remotas sobre los equipos de maniobra, así como también debe contener las diferentes interfaces que le permitan adaptar protocolos de comunicación industriales para la supervisión y control remoto.

En Colombia y en el mundo aún se tienen subestaciones eléctricas con control convencional, esto quiere decir que los enclavamientos del nivel campo se implementan con tecnología de contactos entre los equipos de maniobra y relés repetidores discretos para completar las lógicas requeridas de acuerdo a la configuración de las subestaciones.

Para permitir supervisión y control remoto, los sistemas convencionales de las subestaciones utilizan las unidades terminales remotas “RTU” teniendo así una combinación de lógica discreta y el procesamiento de un dispositivo a base de microprocesadores para llevar la información a sitios remotos utilizando un canal de comunicación industrial IEC 60870-5-101 entre la terminal y una estación maestra donde se tiene un sistema central Scada.

Desde los años 1970 con la aparición del PLC Modicom y otros, los sistemas de control convencional empezaron a cambiar, la gran facilidad para realizar programas lógicos de contactos o lógica blanda o lógica escalera, término acuñado por los ingenieros electricistas de la época, inició una etapa de cambio y renovación. Este paso dado hacia el cambio también trajo consigo el desarrollo de interfaces de comunicación como la famosa interface RS232 y protocolos propios de los fabricantes de los PLC como fueron Modbus, LON, SPA Indactic 3341, DNP3, quizá tímidamente se empezó a cambiar y combinar el procesamiento electrónico con las tecnologías de la información TI en los controles de las subestaciones eléctricas.

IED Intelligent Electronic Devices.

Los dispositivos electrónicos inteligentes aparecieron en el sector eléctrico alrededor del año 2001, cuando el auge de los PLC empieza a disminuir, son utilizados en el sector eléctrico para supervisar y controlar interruptores de

potencia, seccionadores, transformadores, módulos de compensación y muchos más.

Inicialmente los IED´s funcionaron de forma separada en las subestaciones, reciben información de los dispositivos externos (CT, PT. Válvulas) la procesan y en algunos casos la tramitan a un nivel de control superior. Gracias a los esfuerzos de Europa y E.U para crear una norma de aceptación mundial y después del proyecto “Utility Communications Architecture” UCA 2.0 se lanzó en 2004 el estándar IEC 61850 que terminó de desarrollar los IEDs y de paso definió las comunicaciones en las subestaciones eléctricas.

Desde entonces cada fabricante de IED tiene como propósito desarrollar el hardware y el software tal que pueda ofrecer en el mercado un dispositivo que cumple con lo establecido en el estándar. Entre muchos aspectos definidos en el estándar, los IED´s deben suministrar en lenguaje XML eXtensible Markup Language (lenguaje de marcas) un archivo con la descripción y las características principales donde este contenida la estructura de los datos o nodos lógicos para permitir interoperabilidad entre fabricantes.

A continuación, veremos un dispositivo IED de la marca SIEMENS

Figura 3. Dispositivo “IED” de la marca Siemens Siprotec

Fuente:
https://www.siemens.com/press/en/presspicture/?press=/en/presspicture/2017/energymanagement/im2017100003emen.htm

Niveles de operación de un Sistema de Automatización en subestaciones eléctricas

Las subestaciones poseen 4 niveles de control y son operadas desde todos los niveles jerárquicos según los enclavamientos respetivos.

Nivel 0.

Lo constituye el mando que se ejecuta desde los gabinetes de control de los equipos en el patio de conexiones (interruptores, seccionadores y cambiadores de tomas) generalmente para maniobras de mantenimiento y se activa a través de un selector local - 0 – Remoto.

Nivel 1.

Corresponde al mando que se realiza a los equipos de maniobra desde el mímico de la sala de control y/o al comando que se realiza desde los IED´s ubicadas en las casetas de relés.

Nivel 2.

Corresponde al control que se realiza desde la consola de mando ubicada en la sala de control de la subestación. Está formada por dos terminales de computadora (PC) denominadas IHM1 e IHM2 y desde éstas se pueden realizar acciones de control y supervisión a los equipos de maniobra.

Nivel 3.

Corresponde al control y supervisión que se realiza a la subestación desde un sitio remoto. La información desde y para la subestación eléctrica se hace a través de un canal de comunicación utilizando el estándar IEC 60870-5-101 y un equipo gateway que convierte y adapta los diferentes protocolos.

6.2.1.5 El Estándar IEC 61850 para Subestaciones Eléctricas. El estándar IEC 61850 es utilizado en los sistemas de automatización de subestaciones, que implementan la pirámide de control característica de los sistemas industriales (nivel de proceso, nivel de campo, nivel de estación), tiene como característica principal permitir la integración e interoperabilidad de todos los niveles de control en una única red y en un solo protocolo sin necesidad de acudir a los convertidores de protocolo para cada dispositivo. El estándar IEC 61850 está especialmente diseñado para la industria eléctrica.

En el estándar IEC 61850 se virtualizan los dispositivos del patio de conexiones de tal forma que una imagen del mundo analógico se pueda llevar a un modelo de datos dentro del IED.

El estándar IEC 61850 se divide en 10 partes o capítulos:

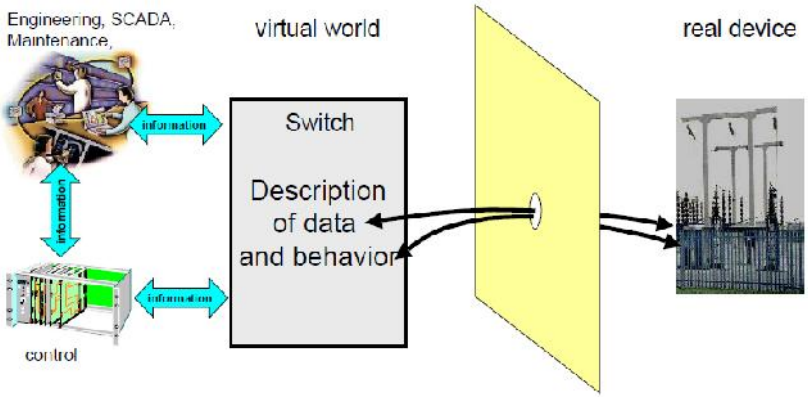
Tabla 1. Capítulos del Estándar IEC 61850

Aspecto	Parte de IEC 61850
Aspectos Generales del sistema	
• Introducción y vista general	1
• Glosario	2
• Requerimientos generales	3
• Gestión de Sistema y Proyectos	4
• Requerimientos en comunicaciones	5
Lenguaje de configuración para IED's	6
Datos y modelos de servicio	
• Introducción	7-1
• Modelo de datos - Funciones	7-2
• Modelo de datos - Atributos	7-3
• Modelo de servicios, Modelo de datos	7-4
Mapeo de la red de comunicaciones	
• Comunicación en las subestaciones	8-1
• Valores de muestreo	9-1, 9-2
Pruebas de conformidad	10

Fuente. Los Autores

Las señales de los dispositivos reales del patio de conexiones en una subestación eléctrica son virtualizadas en el estándar 61850 para permitir interoperabilidad.

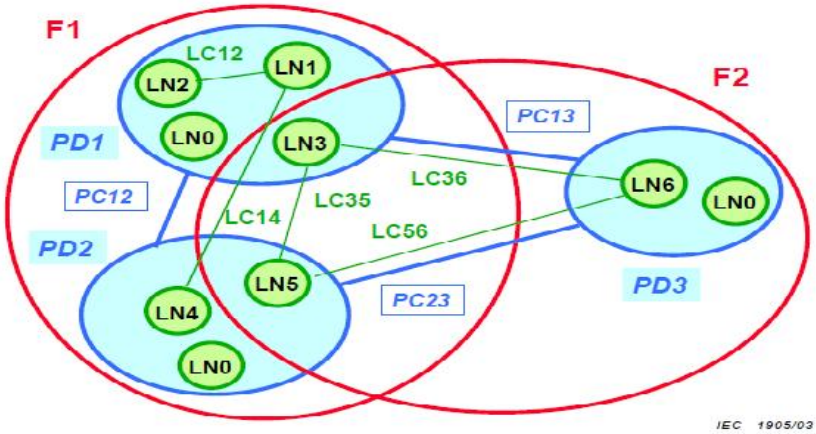
Figura 4. Virtualización



Fuente: INTERNATIONAL STANDARD. IEC 61850-7-1. Communication networks and systems in substations – Part 7-1: Basic communication structure for substation and feeder equipment – Principles and models. Edición 1.0 03-2007

Cuando en un sistema de automatización se implementa el estándar IEC 61850, los IED's que hacen parte de la red tienen la facilidad de intercambiar el modelo de datos y los servicios que tiene normalizados (protección, control, medida etc.), entre uno o más, de forma cooperativa; permitiendo que las funciones configuradas en los dispositivos puedan entender la información que les llega a través de la red y completar o realizar otra función de forma común en el sistema, aunque esta función este distribuida físicamente en otro dispositivo. Los nodos lógicos de la red comparten información para formar nuevas funciones.

Figura 5. Intercambio de Información con nodos lógicos



Fuente: INTERNATIONAL STANDARD. IEC 61850-7-5. Communication networks and systems in substations Communication networks and systems in substations – Part 5:

Concepto de modelo de datos en IEC 61850.

Para dar respuesta al manejo individual de los diseños en cada subestación eléctrica y a la posible interpretación de parte de los ingenieros analistas del sistema eléctrico, el estándar define el concepto de datos orientados a funciones y a objetos para permitir reflejar una imagen más general del sistema sin necesidad de conocer la ingeniera de detalle que hay en cada configuración. Los objetos y las funciones en conjunto van a modelar transformadores, interruptores, seccionadores y demás equipos del patio de maniobras con todas sus propiedades, lo cual nos indica que marcas de fabricantes y detalles particulares no van a ser relevantes para la parametrización y con esto el estándar garantiza interoperabilidad.

En la práctica esto indica que si por condición de falla en una subestación eléctrica se tiene que cambiar un interruptor de marca ABB por uno de marca Siemens el cambio debe ser transparente sin necesidad de realizar ningún ajuste en la lógica ni en los enclavamientos gracias a la virtualización en el IED del mundo real.

Nodo Lógico

Los equipos de maniobra de la subestación eléctrica, los equipos de protección, o los dispositivos auxiliares utilizados en la subestación se modelan con nodos lógicos LN que contienen atributos y son considerados como la entidad más pequeña de una función, el estándar IEC 61850 define 92 LN. Los nodos lógicos tienen como función intercambiar información entre los IED´s o dispositivos físicos en los cuales se implementan las funciones.

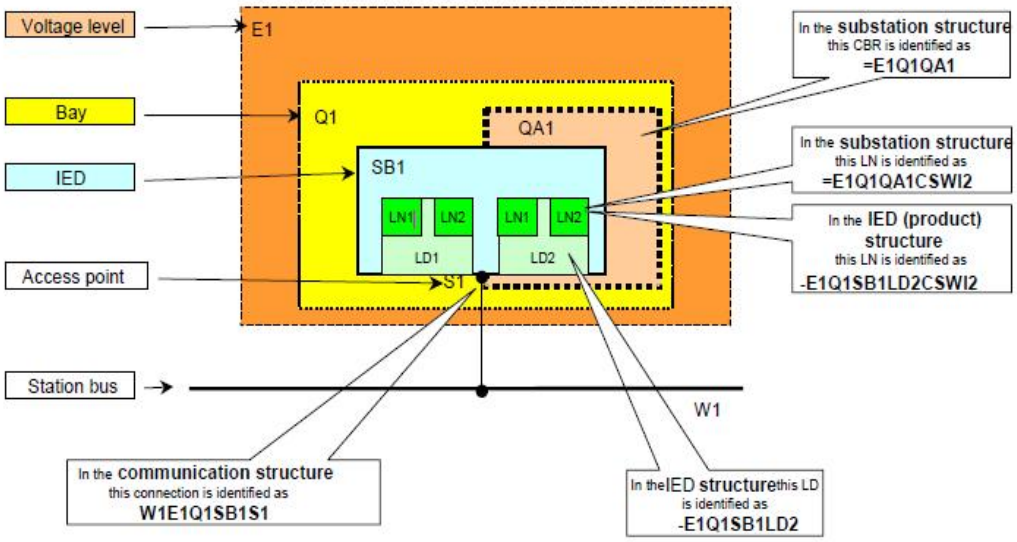
La descripción de un nodo lógico junto con su atributo seria la siguiente para un interruptor No 1 ubicado en la subestación eléctrica de nombre “proyecto”.

Tabla 2. Ejemplo de la estructura de un nodo lógico

PROY/Q0CSWI1.Pos. ctlVal

Fuente. Los Autores

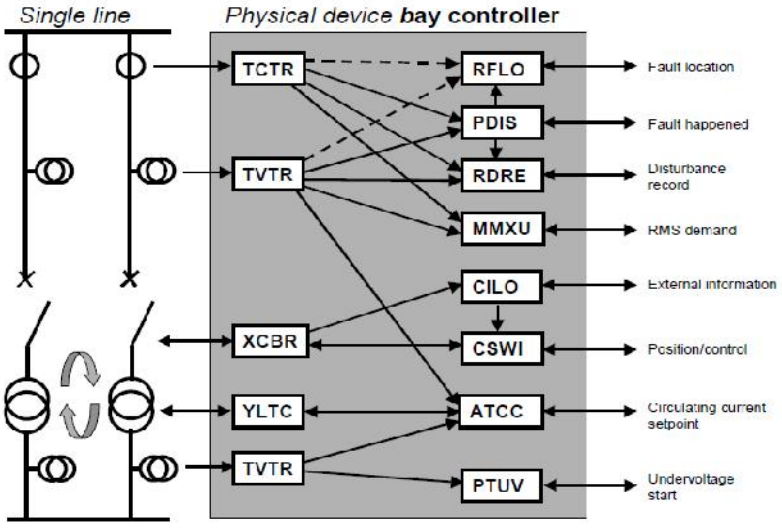
Figura 6. Nodo Lógico



Fuente: INTERNATIONAL STANDARD. IEC 61850-6. Communication networks and systems for power utility automation –Part 6: Configuration description language for communication in electrical substations related to IEDs Edición 2.0 12-2009

La combinación de diversos nodos lógicos da origen a los dispositivos lógicos.

Figura 7. Nodo lógico, Dispositivo lógico



Fuente: INTERNATIONAL ESTÁNDAR. IEC 61850-5. Communication networks and systems for power utility automation –Part 5: Communication requirements for functions and device models Edition 2.0 01-2013

Tabla 3. Nodos Lógicos del estándar IEC 61850

Cantidad	Descripción
3	Nodos Lógicos del sistema
28	Nodos Lógicos de funciones de protección
10	Nodos Lógicos de funciones relacionadas con protecciones
5	Nodos Lógicos de control supervisión
3	Nodos Lógicos de referencia genérica
4	Nodos Lógicos de interfaces y almacenamiento
4	Nodos Lógicos de control automático
8	Nodos Lógicos de medidores y medición
4	Nodos Lógicos de sensores y monitoreo
2	Nodos lógicos de dispositivos de conmutación
2	Nodos Lógicos de transformadores de medida
4	Nodos Lógicos de transformadores de potencia
15	Nodos lógicos de otros equipamientos del sistema de potencia

Fuente: Los Autores

6.2.1.6 Mapeo. Una vez definidos los modelos en términos de funciones y servicios, el estándar mapea o direcciona estos servicios en los protocolos de comunicación definidos en el modelo OSI, así como también define las estructuras de los mensajes que se originan en una subestación eléctrica y que son de diferente naturaleza.

Los mensajes sin prioridad los maneja con el protocolo MMS Manufacturing Message Specifications (comunicación maquina a máquina) y los mensajes urgentes o con alta prioridad de tiempo GOOSE los maneja con las definiciones el tipo Ethernet.

6.2.1.7 Configuración. El estándar IEC 61850 define un lenguaje de configuración SCL a nivel de subestación eléctrica, está escrito como se mencionó anteriormente en XML.

EL SCL describe la configuración y los parámetros del IED en términos de comunicaciones para permitir el intercambio de este archivo ente las distintas herramientas de diseño de ingeniería sin depender de las herramientas de gestión de la casa fabricante.

Así como el archivo SCL existen otros archivos definidos en el estándar, que se pueden considerar una particularidad del archivo de configuración de la subestación[24].

Archivo SSD. Describe las especificaciones de la subestación

Archivo ICD. Define las características del IED, en este archivo se encuentra la estructura de los datos y los nodos lógicos configurados en el IED.

Archivo SCD. Descripción de la configuración de la subestación. Presenta le estructura del proyecto con todos los IED's, la configuración y la descripción de la subestación.

Archivo CID. Descripción de la configuración del dispositivo.

6.2.1.8 Implementación del estándar IEC61850 en subestaciones eléctricas. En este capítulo se indica de manera conceptual como implementar un sistema de automatización SAS, integrando hardware y aplicativos computacionales configurados de tal forma que puedan cumplir con la arquitectura básica de un sistema para subestaciones.

La parte fundamental de la implementación está compuesta por un estándar industrial con tecnología Microsoft que ofrece una interface común de comunicación entre diferente aplicativa computacional "OPC". (OLE para Control de Procesos).

OPC es una solución abierta y flexible que entrara a solucionar la problemática de los drivers en el control de las subestaciones Prácticamente todos los grandes fabricantes de sistemas de control (Siemens, ABB, Areva, etc), e instrumentación y de procesos han incluido OPC en sus productos.

6.2.1.9 Identificación de grupos funcionales en la implementación. Servidor IEC 61850. Se definen como servidores del estándar IEC 61850 a los relés de protección, el equipo de medida, los controladores de diámetro y/o de bahía que conforman el bus de proceso, en general todos los "IED's" de la red.

[24] INTERNATIONAL ESTÁNDAR IEC 61850. Primera edición. Año 2002

Estos dispositivos están formados por nodos físicos y nodos lógicos, compuestos por atributos que publicaran el valor del dato, el cambio de estampa de tiempo y la calidad de la señal (d, t, q).

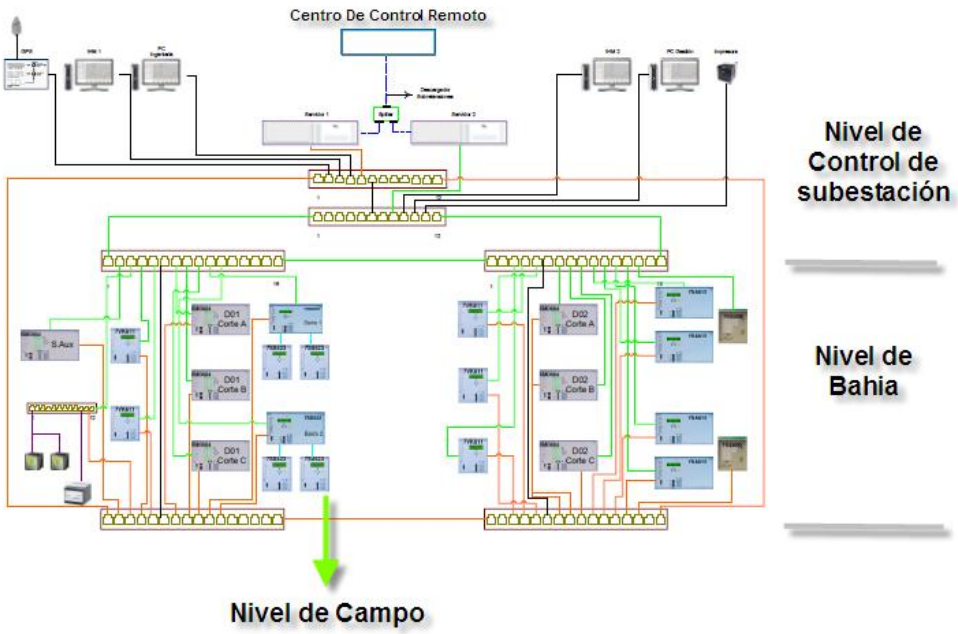
Cliente IEC 61850: Se define el cliente del estándar como la interface capaz de interactuar y tener acceso a los nodos lógicos de IEC 61850 y cualquier aplicación de Windows preferiblemente OPC.

En la implementación propuesta el cliente IEC61850 debe tener la posibilidad de ser la interfaz con los nodos lógicos del bus de proceso y adicionalmente debe tener las capacidades de servidor para suministrar los datos a una interface de comunicación industrial como es el OPC.

Puerta de enlace: Se define la puerta de enlace o “Gateway”, como un dispositivo conversor de protocolos (este dispositivo generalmente se implementa en un PC) que traduce la información del protocolo de red al protocolo usado en la red de destino.

El Gateway debe traducir la información contenida en los nodos lógicos de estándar IEC 61850 al estándar IEC 608050-5-101. El IEC 608050-5-101 es el protocolo utilizado para comunicar dos extremos remotos. (Traduce atributos de IEC 61850 en direcciones IEC utilizando enmascaramiento).

Figura 8. Arquitectura de un SAS



Fuente: Los autores

6.2.1.10 Generalidades relevantes en Sistemas de Control Industrial. Los avances tecnológicos tradicionalmente antes de la primara revolución industrial estaban basados en mecanismos impulsados por agua o por vapor, cada vez se lograba un adelanto o una nueva invención la sociedad celebraba el logro con gran entusiasmo.

En 1870 se inventó la primera banda transportadora y el impacto en la industria se dio a conocer por todo el mundo, pero fue en 1969 con la aparición del primer PLC Modicom 084 que las cosas cambiaron en el control industrial, aparece la tercera revolución industrial y con ella el uso de la electrónica y la tecnología de la información TI, que le dieron una velocidad característica a los inventos y a la evolución de la tecnología hasta el punto de convertir los cambios casi en vertiginosos.

Estos cambios nos han hecho pasar de lo estacionario a lo móvil e inteligente en nuestras vidas cotidianas y en el control industrial se ha pasado de los avances rápidos y seguros a avances extraordinarios y vertiginosos que son de interés de propios y extraños, entre ellos los ciber delincuentes de red para los cuales los sistemas de control industrial se han convertido en todo un laboratorio de pruebas en donde desean explotar y conocer el límite de las tecnologías utilizadas.

La seguridad en las redes interconectadas pertenecientes a la tecnología de la Información TI, trata cada día de cerrar brechas vulnerables aplicando métodos de autenticación, autorización, de cifrado, manejo de los errores, eliminación de log, entre otros, sin embargo, en el control industrial donde la interconexión a través de redes de comunicaciones es un tema innovador no se han aplicado las contramedidas con la misma rigurosidad que en el sector comercial de las tecnologías de la información.

En los sistemas de control industrial que hacen parte de infraestructuras críticas como en las refinerías, en las centrales nucleares, centrales eléctricas, subestaciones eléctricas, centros de control remotos, etc. se aplican tecnologías propias de la operación “Operational Technology TO”.

6.2.1.11 Tecnología Operativa TO “Operational Technology”. La tecnología operativa es todo el hardware y software necesario en un control industrial para detectar cambios en el sistema y permitir control sobre los dispositivos físicos como las válvulas, los sensores, los interruptores de potencia los seccionadores, con una característica particular de no estar conectadas a la red de internet.

Las tecnologías operativas TO se encuentran en entornos tales como las Unidades terminales Remotas RTU, los sistemas industriales de control SIC, los sistemas de control –supervisión y adquisición de datos SCADA, los sistemas de

control coordinado implementados con PLC propios de refinerías centrales nucleares, centrales y subestaciones eléctricas por lo que generalmente se les considera parte de las infraestructuras críticas de las naciones.

Las válvulas los sensores y en general la mayoría de los dispositivos físicos utilizados en control industrial se están convirtiendo en inteligentes, estas tecnologías combinadas con las redes inalámbricas en pleno desarrollo brindan un entorno muy favorable para que ingenieros y administradores realicen gestión a los equipos desde sitios remotos. A medida que esto sucede y los sistemas TO abren sus horizontes y se conectan a la red se enfrentan con los problemas de seguridad informática, los problemas de autenticación y problemas de control de acceso entre otros, que los van a hacer cada día más vulnerables con el gran impacto que cualquier espionaje, ataque o sabotaje afecta directamente las infraestructuras críticas.

6.2.1.12 Integración IT/OT. Es fácil resaltar las ventajas que trae la unión o integración de las tecnologías TI y TO en los sistemas de control industrial entre ellas podemos citar la reducción de costos en la implementación, la flexibilidad y la gestión en línea, la incorporación de adelantos tecnológicos, el aumento de velocidad en el procesamiento de los datos, la portabilidad de sistemas.

Estas ventajas que están a la orden del día van a influir en la mente de los diseñadores, administradores e ingenieros de control industrial para realizar integración de tecnologías e integración de diferentes redes, dejando como resultado implementaciones de control y supervisión inseguras.

Con análisis básicos de seguridad informática y por la propia necesidad de tener sistemas de operación más accesibles, el ingeniero de control conecta sus sistemas a Routers comerciales que además de tener contraseñas por defecto, publicas e inseguras que no se modifican al realizar la conexión, carecen de los mínimos análisis de vulnerabilidades y en algunos casos no se tiene en cuenta las actualizaciones disponibles de seguridad.

6.2.2 Análisis Comparativo de Ataques realizados y sus características (DragonFly, BlackEnergy, Stuxnet, Industroyer 2016).

A continuación, se presenta un análisis comparativo de los ataques informáticos que se han efectuado a las infraestructuras críticas, se realiza destacando sus impactos físicos, económicos y sociales con el fin de conocer de qué manera podemos ser afectados o impactados considerablemente en mayor o menor proporción por un ciberataque o ataque informático para la prevención y/o mitigación de estos.

Tabla 4. Cuadro comparativo de ataques realizados y sus características (DragonFly, BlackEnergy, Stuxnet, Industroyer 2016

INCIDENTE	IMPACTO FÍSICO	IMPACTO ECONÓMICO	IMPACTO SOCIAL	LECCIONES APRENDIDAS
Stuxned Origen U.S.A. e Israel Tipo: ataque	se afectó los parámetros de los PLC S7 que manejaban los rotores de las centrifugas de uranio	Pérdidas económicas	Incremento de la consciencia de la seguridad en entornos de SCI	Implementar mayor reserva en documentación de los procesos
DragonFly Origen Rusia Ciberespionaje sabotaje	Afectación directa de PLC	Pérdida de Información	Incremento de la consciencia en la existencia del Ciberespionaje	Desconfianza
BlackEnergy Tipo: Espionaje / Ataque	Fallas en el suministro de la electricidad	Pérdidas económicas y Reputación	Incremento de la consciencia por ataques masivos en el sector eléctrico	Identificación del poderío del malware que ataca subestaciones eléctricas
Industroyer Tipo: Ataque	Afectación directa de IED´s / Fallas en el suministro de la electricidad	Pérdidas económicas y Reputación	Preocupación mundial por nuevos ataques	Presunta fuga de información y consciencia de que los atacantes están bien preparados
Triton Tipo: Ataque	Afectación directa de controladores del sistema de seguridad industrial. Se puso en peligro la vida de las personas	Pérdidas económicas	Identificación de diferentes y diversos actores de ataque	Realizar discusiones públicas acerca de las tecnologías de SIS e integrar a los fabricantes con las empresas, para que compartan buenas prácticas y eviten intrusiones en sus ambientes

Fuente: Los autores

7. RESULTADOS E IMPACTOS ESPERADOS

Sensibilización.

Los ataques cibernéticos a la infraestructura crítica pueden desestabilizar los gobiernos y en caso de materializarse pueden generar “efecto dominó” en toda la población en general, generando pérdidas catastróficas y comprometiendo el bienestar y la vida de pueblos.

Los ataques en el ciberespacio a gran escala que se publicaron al inicio del año 2017, entre los cuales podemos recordar a WannaCry entre otros, indican que esta realidad, si no se toman las precauciones respectivas, en cualquier momento estará en nuestros ordenadores personales modificando nuestras formas de vida. Los ciberataques junto con los fenómenos meteorológicos se están convirtiendo en los mayores riesgos que enfrenta nuestra sociedad actual. La manera en que las amenazas cibernéticas evolucionan y cambian su forma de ataque, dan cuenta que todos los sistemas conectados en red se han vuelto sensiblemente atractivos para las diferentes comunidades del ciberespionaje y ciberataque, las infraestructuras críticas del sector eléctrico colombiano no se escapan a esta realidad para la cual el enfoque y la mitigación de este riesgo se debe cambiar, si bien es cierto, debe haber continuidad en los análisis técnicos de los diferentes malwares que atacan, se debe llevar la problemática existente a un contexto político donde gobernantes y el sector privado aborden el tema de forma integral, con equipos de trabajo multidisciplinario y si la situación lo amerita extender las experiencias en un ámbito internacional.

La unión de sinergias entre los diferentes grupos interdisciplinarios en busca de mitigar el riesgo de ataques cibernéticos a las infraestructuras críticas debe dar como resultado el análisis y la determinación de las siguientes situaciones.

- Asignar presupuesto para inversión técnica y recurso humano. La ciberseguridad en general no debe estar en cabeza de una sola persona, hacerse rodear de expertos en ciberseguridad aumentara los niveles de seguridad, combinado esto con capacitación periódica a todo el personal.

- Delimitar responsabilidades. En el sector eléctrico colombiano existe el liderazgo del Consejo Nacional de Operación el cual muestra el norte a los diferentes agentes y clientes conectados en el Sistema de Trasmisión Nacional en cuanto a los temas requeridos de ciberseguridad los cuales deben ser acatados a su cabalidad. En el acuerdo CNO 788 se presentan las pautas y los procedimientos a seguir.

- Tener presente un enfoque general de la ciberseguridad en todo el sector eléctrico. Todos los puntos de vista a la hora de mitigar y llevar a cabo análisis de incidentes de ataques cibernéticos son válidos, se debe considerar los aspectos técnicos, económicos, legales, organizacionales y gubernamentales. Cada agente conectado al sistema debe tener claro su rol y su responsabilidad a la hora de actuar identificando tareas estratégicas y canales de comunicación eficaces.

- Participar y fomentar grupos de ayuda mutua en el sector eléctrico. La documentación de los diferentes incidentes de amenazas cibernéticas en cada uno de los agentes y la comunicación oportuna para los grupos de ayuda mutua fortalecerá las alianzas en todos los grupos empresariales, así como el gobierno.

8. RECOMENDACIONES

Estas recomendaciones están dirigidas a estudiantes, ingenieros, profesionales de TIC-TO, directores gerentes y en general a toda la comunidad que interactúa con las infraestructuras críticas del sector colombiano. Muy claramente lo expresó el Director del FBI Robert Mueller en el año 2012 cuando se refirió a las infraestructuras críticas. ¡Hay algunas que ha sido atacadas y las otras serán atacadas en el futuro!

Los sistemas de control industrial que conforman en muchos casos las infraestructuras críticas requieren especial atención. Los antecedentes relacionados con ataques a estos sistemas indican que además del interés formal de administradores y diseñadores del sector eléctrico por su implementación y desarrollo, existe otra comunidad interesada en conocerlos atacarlos y tomar el control.

Los ataques se han sucedido en muchas partes del mundo y han sido dirigidos especialmente desde los países que tienen o han tenido conflictos políticos, lo que de cierta forma aclara la intensión del ataque, pero no podemos olvidar nuevas corrientes de ataques, espionaje, interés, sabotaje, facilidad de medios, libre información entre muchas otras que pueden llevar a materializar las intenciones de mentes maliciosas en sistemas de control de subestaciones eléctricas.

Con una visión general y gracias a todos los temas aquí expuestos, los autores de este trabajo recomiendan un cambio en los diseños y desarrollo de los sistemas de automatización de subestaciones eléctricas, vistos desde la seguridad física, perimetral, de diseño e implementación, y quizás lo que es más importante emprender un cambio de formación y educación en las personas para evitar que sean los eslabones más frágiles de la cadena.

A continuación, se muestran diez recomendaciones para el análisis y discusión del lector.

1. Medir y cuantificar la exposición al riesgo que pueden tener los sistemas de control en infraestructuras críticas.
2. Establecer una cultura en seguridad informática permanente y con seguimiento.
3. Los gerentes deben tener claro que no solamente se debe invertir en tecnología, deben tener claro que las personas se han convertido en foco de ataques y por tanto en muchos escenarios se hacen vulnerables.
4. Consolidar equipos de trabajo que pueda hacer frente a los vectores de ataque dirigidos contra las infraestructuras críticas, disponer de personas

con dedicación cien por ciento comprometidas y permanentemente actualizadas.

5. Impartir formación en seguridad informática para profesionales del sector eléctrico, estableciendo de manera clara los conceptos sobre ciberseguridad en entornos industriales.
6. Establecer claramente que los programas de ciberseguridad deben estar totalmente conectados con las estrategias de las compañías.
7. Las auditorías que se realicen al sector de infraestructuras críticas deben tener enfoque de ciberseguridad.
8. La alta dirección debe apoyar y demostrar convencimiento de las políticas que controlan los riesgos informáticos.
9. Se debe crear conciencia en que se debe implementar una cultura de ciberseguridad activa en los diferentes centros de control regionales y el nacional e incluso en cada subestación para fortalecer la capacidad de Detección, Respuesta y Recuperación ante un ataque.
10. En cuanto a la tecnología a implementar se debe garantizar que los diseños de control y supervisión de una subestación eléctrica deben contar con la integración de las tecnologías TI y la tecnología Operativa TO. Las implementaciones con algunos años de uso que no cuenten con los requerimientos de ciberseguridad para garantizar la disponibilidad, integridad y confiabilidad deben ser sacadas de servicio lo más pronto posible.

Es notable que las recomendaciones anteriores van a reflejar un panorama más seguro para las infraestructuras críticas del sector eléctrico en Colombia, no obstante, se debe tener presente la aparición de nuevas tecnologías disruptivas como son las que traerá el internet de todo e industria 4.0, que terminaran por afirmar que el mundo cambió y que próximamente estaremos viviendo en un mundo nuevo con estrategias de nuevos ataques. El sector eléctrico se prepara para estos cambios y desde la perspectiva de ciberseguridad para subestaciones eléctricas digitales se recomienda la aplicación estricta de los estándares IEC 62351 orientado a la ciberseguridad de los equipos de supervisión y control incluidos los protocolos de la serie IEC 60870-5 para los cuales incluye nuevas estrategias de autenticación y aplicación de firmas digitales para evitar ataques de hombre en el medio. Para completar la seguridad en entornos digitales el estándar IEC62443 ha llegado para aumentar los niveles de seguridad del perímetro. La aplicación de estos estándares en conjunto ¡no debe hacerse esperar!

9. CONCLUSIONES

- Para los autores de este trabajo es muy importante que el lector comprenda la importancia de los sistemas de infraestructura crítica y conozca el soporte que estos sistemas brindan al desarrollo de una nación. En Colombia gran parte de la infraestructura eléctrica distribuida a lo largo y ancho del país es catalogada como infraestructura crítica, tal como lo define el Concejo Nacional de Operación CNO en el anexo de su guía de ciberseguridad. Por lo tanto, un ataque informático a la infraestructura crítica del sector eléctrico tendría consecuencias devastadoras y de incalculable valor.

- El mundo reseña noticias de ciberataques a las infraestructuras críticas en países como Estados Unidos, Irán, China, Corea, entre otros, que de acuerdo a los resultados concretos de estos ataques y con un análisis mediático se han tratado como simples teorías de ciberataques o ciberguerra. El 17 de diciembre de 2016 en Ucrania, se produce un ciberataque contra las subestaciones eléctricas con resultados devastadores para los usuarios y el sector eléctrico de Ucrania donde los atacantes explotaron los protocolos de comunicaciones utilizados en la subestación y generaron denegación de servicio en los dispositivos de control Siemens Siprotec aprovechando la vulnerabilidad CVE-2015-5374 ampliamente documentada. Este panorama evidente de las infraestructuras críticas no tiene por qué alarmarnos, pero si es de vital importancia recoger y capitalizar lecciones aprendidas a lo largo de estos años para poder adaptar las infraestructuras críticas a las necesidades de seguridad actual.

- En Colombia se han sucedido un gran número de actos mal intencionados contra las infraestructuras críticas, entre ellos; los oleoductos, estaciones petroleras, infraestructuras de telecomunicaciones, torres de trasmisión de energía, subestaciones eléctricas entre otras de pleno conocimiento de la sociedad, por parte de grupos al margen de la ley, entre ellos el extinto grupo de las FARC, el ELN, el EPL y algunas disidencias que en ocasiones llevan al país a situaciones de desastre y emergencia.

- Fuentes oficiales del sector eléctrico colombiano no se han pronunciado oficialmente para denunciar ciberataques a sus sistemas de control en sus subestaciones eléctricas. En el Foro de Riesgos 2018 “RIMS” celebrado en la ciudad de México, Sandra María Ríos representante de “XM” empresa encargada del control y despacho de energía, dio a conocer las políticas de seguridad nacional e infraestructura, partiendo de un contexto global, haciendo énfasis en los principales ataques sucedidos a nivel mundial, para finalmente sociabilizar los marcos adoptados por el sector eléctrico colombiano para combatir o minimizar los ciberataques, El concejo nacional de Operación del

sistema eléctrico colombiano "CNO" contiene la guía de ciberseguridad para realizar la gestión.

- Desde el nacimiento de la Unidad de Planeación Minero Energética – UPME ocurrido en los años 1992 en Colombia, el sector eléctrico ha jalonado el diseño y la construcción de subestaciones eléctricas basadas en la pirámide de control para adecuar diferentes arquitecturas de operación y control. Los proyectos de UPME01 revolucionaron la forma y los procesos de construir subestaciones eléctricas en la mente de los ingenieros, para beneficio del sector que desde entonces crece con muy buenas expectativas tecnológicas. UPME01, UPME02, construyen subestaciones en alta y ultra alta tensión, topológicamente cerraron el anillo en 500 kilo voltios entre la costa atlántica y las grandes generadoras ubicadas en Antioquia y el oriente colombiano. Nuevos equipos de potencia, nuevos seccionadores de corte central y pantógrafos, fibra óptica mono y multimodo en salas de operación, computadores de propósito específico, dispositivos electrónicos inteligentes "IED´s", marcas reconocidas ABB, Siemens, entre otros, referencias típicas como REL 670, 7SJ, 6MD, etc., y con ellas vulnerabilidades a la orden del día, que intentan ser controladas por ingenieros administradores de las TIC o en su defecto ingenieros con principios básicos de TO.

- Por la necesidad de la interoperabilidad de los IED´s de diferentes fabricantes la popularidad de la aplicación del estándar IEC 61850 en las subestaciones eléctricas aumenta en cada proyecto, la combinación y el uso de protocolos de comunicación industrial cada vez es más frecuente y se hace tan común en cada proyecto identificar el protocolo IEC 61850 traducido a IEC 60870-5-101 mediante una aplicación OPC. Todo el panorama anterior es muy parecido por no decir casi igual al ofrecido en 2016 a los atacantes en Ucrania, cuando a través de puertas traseras ingresaron a los sistemas de control y cargaron e instalaron su carga útil "Payload" para afectar los protocolos y rápidamente desplazar los comandos legítimos de los interruptores de potencia por comando manejados desde servidores de C&C por los atacantes.

- De acuerdo a los ataques informáticos que se han efectuado a las infraestructuras críticas y al análisis comparativo realizado de los más representativos, destacando sus diferentes impactos físicos, económicos y sociales causados, se considera que serán un gran aporte como lecciones aprendidas que contribuirán en el futuro para la prevención y/o mitigación de estos.

BIBLIOGRAFÍA

Acuerdo No CNO 788. Por el cual se aprueba la Guía de Ciberseguridad. {En línea}. {12 diciembre 2018}. Disponible en: file:///C:/USER%20DEL%20D/Users/USUARIO/Downloads/C.N.O%20-%20Acuerdo%20788%20-%202015-10-13%20(3).pdf

AVILA, Fred Y. Grupos avanzados de amenazas persistentes. {En línea}. {10 marzo 2019}. Disponible en: https://securityhacklabs.net/articulo/grupos-avanzados-de-amenazas-persistentes-apt-groups

BOLIVAR. Infraestructuras críticas y sistemas industriales. Auditorias de seguridad y fortificación. Primera edición. Madrid. 0Xword. 2016. Páginas 67; 70

CHEREPANOV, Anton. WIN32/INDUSTROYER A new threat for industrial control system. {En línea}. {12 diciembre 2018}. Disponible en: https://www.welivesecurity.com/wp-ontent/uploads/2017/06/Win32_Industroyer.pdf

CORPORACIÓN COLOMBIANA DIGITAL. Las amenazas informáticas son capaces de controlar los sistemas de energía eléctrica de una nación. {En línea}. {12 diciembre 2018}. Disponible en: https://colombiadigital.net/actualidad/noticias/item/9805-las-amenazas-informaticas-son-capaces-de-controlar-los-sistemas-de-energia-electrica-de-una-nacion.html

CREG Comisión de Regulación de Energía y Gas. {En línea}. {12 diciembre 2018}. Disponible en: http://www.creg.gov.co/

CVE-20011-0611. {En línea}. {12 diciembre 2018}. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0611

CVE-2015-5374. {En línea}. {12 diciembre 2018}. Disponible en: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5374

Disponible en: http://www.scadahackr.com/library/Documents/Case_Studies/Case%20Study%20-%20NIST%20-%20Maroochy.pdf

Disponible en: https://gosint.wordpress.com/2017/08/19/the-farewell-dossier-geopolitical-consequences-on-the-end-of-the-cold-war/

Documento Compes 3701. LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA. {En Línea}. {12 diciembre 2018}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Dragonfly. Espía de la energía. {En línea}. {12 diciembre 2018}. Disponible en: https://www.symantec.com/es/mx/outbreak/?id=dragonfly

DRAGOS. CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations. {En línea}. {12 diciembre 2018}. Disponible en: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

FEDERAL ELECTRIC REGULATORY COMMISSION. FERC. 2018. {En línea}. {12 diciembre 2018}. Disponible en: https://www.ferc.gov/

Grupo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT. {En Línea}. {12 diciembre 2018}. Disponible en: http://www.colcert.gov.co/?q=acerca-de

HERNÁNDEZ, José. Infraestructura Crítica Cibernética. {En línea}. {12 diciembre 2018} Disponible en: http://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

INCIBE. CrashOverride: El malware para SCI ataca de nuevo. {En línea}. {12 diciembre 2018}. Disponible en: https://www.certsi.es/blog/crashoverride-el-malware-sci-ataca-nuevo

INTERNATIONAL ESTÁNDAR IEC 61850. Primera edición. Año 2002

JIMENEZ, José. Los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años. {En línea}. {12 diciembre 2018}. Disponible en: https://politica.elpais.com/politica/2017/05/24/actualidad/1495619175_136537.html

LEY 142 DE 1994 {En línea}. {12 diciembre 2018} Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html

Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia. {En línea}. {12 diciembre 2018}.

Malware Triton vinculado al Instituto de Investigación del Gobierno Ruso. {En línea}. {12 diciembre 2018}. Disponible en: https://www.disoftin.com/2018/10/malware-triton-vinculado-al-instituto.html

PREZ, David. La verdadera historia detrás del virus informático que provocó un apagón en Ucrania. {En línea}. {12 diciembre 2018}. Disponible en: https://omicrono.elespanol.com/2017/11/virus-informatico-provoco-apagon-en-ucrania/

REALPE. Milena LA CIBERDEFENSA EN COLOMBIA {En línea}. {12 diciembre 2018} Disponible en: https://www.cci-es.org/documents/10694/468834/3.+CCOC+PLAN+NACIONAL.pdf/84da120e-3bd6-478c-99c8-1f88c3543355;jsessionid=5E61914D5E08633E7DD315CB4A68FC94?version=1.0

The “FAREWELL DOSSIER”: Geopolitical consequences on the end of the Cold War Posted on August 19, 2017. {En línea}. {12 diciembre 2018}.

UPME Unidad de Planeación Minero Energética {En línea}. {12 diciembre 2018}. Disponible en: http://www1.upme.gov.co/Paginas/default.aspx

ANEXO A. RESUMEN ANALÍTICO ESPECIALIZADO

RESUMEN ANALÍTICO ESPECIALIZADO -RAE	
1. Información General	
Titulo	Ataques informáticos a la infraestructura crítica del sector eléctrico colombiano
Autores	Pedro Julio Mendoza Villamil Álvaro Díaz Ardila
Edición	Por las características del documento, no presenta
Fecha	Diciembre 12 de 2018
Palabras Claves	Infraestructuras Criticas; CON; COMPES 3701; Ataques; Vector de ataque; Payload; Wipe; Stuxnet; DragonFly; BlackEnergy; Indsutroyer; Protocolos; IEC61850; IEC60870-5-101; IEC60870-5-103; IEC60870-5-104; OPC
Descripción	
Monografía para optar al título de Especialistas en Seguridad Informática de la Universidad Nacional Abierta y a Distancia " UNAD" En este documento inicialmente se enmarca el concepto de infraestructura crítica, la regulación existente en Colombia y se detallan los antecedentes que se conocen en cuanto a ciberataques a nivel mundial. Los autores a lo largo del trabajo hacen énfasis en la necesidad de proteger y aumentar los controles de seguridad informática en las subestaciones eléctricas colombianas, que aún tienen implementado viejos protocolos de comunicación en sus sistemas de automatización, así como también se destaca la atención que se debe prestar a los nuevos sistemas de automatización que utilizan el estándar IEC 61850 y dispositivos electrónicos inteligentes de la marca Siemens Siprotec 5, ya que los patrones del malware Industroyer analizado al final del documento, indican que este tipo de implementación y de arquitectura dejan los sistemas con un alto grado de vulnerabilidad. En las referencias bibliográficas de la monografía se encuentran los documentos fuentes consultados para el logro de este trabajo de grado.	
Fuentes	
35 Referencias bibliográficas.	

Acuerdo No 788. Concejo Nacional de Operación. (Colombia)

Documento Compes 3701. Lineamientos de política para ciberseguridad y ciberdefensa (Colombia)

FEDERAL ELECTRIC REGULATORY COMMISSION. FERC. 2018. [Citado Octubre de 2018]. Disponible en: https://www.ferc.gov/

BOLÍVAR, Francisco Juan. Infraestructuras críticas y sistemas industriales. Auditorias de seguridad y fortificación. Editorial OxWORD. Primera edición. 2016

CRASHOVERRIDE. Analysis of the Threat to Electric Grid Operations. Dragos Inc./ www.dragos.com. Versión 2.20170613.

WIN32/INDUSTROYER A new theater for Industrial Control System

DragonFly. Attack on Critical Infrastructure Leverages Template Injection. Disponible en: https://blog.talosintelligence.com/2017/07/template-injection.html

CRITICAL INFRASTRUCTURE PROTECTION. THE WHITE HOUSE. WASHINGTON Presidential Decision Directives – PDD. [Citado Octubre de 2018] Disponible en: https://fas.org/irp/offdocs/pdd/pdd-63.htm.

Estándar Internacional. INTERNATIONAL ESTÁNDAR. Segunda edición

CVE-2015 5374 Vulnerabilidad Equipos IED Siemens Siprotec 5 Disponible en:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5374

Seguridad operacional. BAYSHORE Securing Operational Technology in the Energy Industry Disponible en: www.bayshorenetworks.com

Contenidos

Los ataques a la infraestructura crítica del sector eléctrico colombiano aún no han tenido pronunciamiento oficial de parte de las entidades gubernamentales que manejan dichos activos. En el último foro de riesgos 2018 “RIMS” celebrado en México el funcionario encargado para hacer la presentación por parte del sector eléctrico colombiano dio a conocer la política de seguridad nacional colombiana del sector eléctrico contra los ataques del ciberespacio, sin referirse

puntualmente a un ataque en especial. En este trabajo se presenta un enfoque internacional de los ataques que se han registrado a través de la historia Stuxnet, DragonFly, BlackEnergy, Industroyer y que sirve de guía para abordar este riesgo latente en nuestro sistema interconectado nacional “SIN”. Como tema especial tratado en este documento y dada la gran acogida y aceptación dentro de la ingeniería colombiana del estándar IEC 61850 en las arquitecturas de los sistemas de automatización de subestaciones eléctricas, se hizo un estudio detallado del contenido del estándar en sus 10 capítulos y se estructuró una implementación para subestación de alta tensión abordando los conceptos necesarios para su comprensión, adicionalmente todas las ideas aquí presentadas tratan de correlacionar el ataque realizado en Ucrania en el año 2016 con los protocolos de comunicación que se están utilizando en Colombia, entre ellos el OPC y el IEC 61850.

Metodología	Por las características del documento, no presenta

Conclusiones
Para los autores de este trabajo es muy importante que el lector de la importancia a los sistemas de infraestructura crítica y conozca el soporte que estos sistemas brindan al desarrollo de una nación. En Colombia gran parte de la infraestructura electica distribuida a lo largo y ancho del país es catalogada como infraestructura critica, tal como lo define el Concejo Nacional de Operaciones CNO en el anexo de su guía de ciberseguridad. En Colombia se han sucedido un gran número de actos mal intencionados contra los oleoductos, estaciones petroleras, infraestructuras de telecomunicaciones, torres de trasmisión de energía, subestaciones eléctricas entre muchas más de pleno conocimiento de la sociedad, por parte de grupos al margen de la ley, entre ellos el extinto grupo de las FARC, el ELN el EPL y algunas disidencias que en ocasiones llevan al país a situaciones de desastre y emergencia. Paralelo a estos acontecimientos el mundo reseña noticias de ciberataques a las infraestructuras críticas en países como Estados Unidos, Irán, China, Corea, entre otros que de acuerdo a los resultados concretos de estos ataques y con un análisis mediático se han tratado como simples teorías de ciberataques o ciberguerra. El 17 de diciembre de 2016 en Ucrania, se produce un ciberataque contra las subestaciones eléctricas con resultados desbastadores para los usuarios y el sector eléctrico de Ucrania donde los atacantes explotaron los protocolos de comunicaciones utilizados en la subestación y generaron denegación de servicio en los dispositivos de control Siemens Siprotec aprovechando la vulnerabilidad CVE-2015-5374 ampliamente documentada. Este panorama evidente de las infraestructuras críticas no tiene por qué alarmarnos, pero si es de vital importancia recoger y capitalizar lecciones aprendidas a lo largo de estos años para poder adaptar las infraestructuras críticas a las necesidades de seguridad actual. Fuentes oficiales del sector

eléctrico colombiano no se han pronunciado oficialmente para denunciar ciberataques a sus sistemas de control en sus subestaciones eléctricas. En el Foro de Riesgos 2018 “RIMS” celebrado en la ciudad de México 2018, Sandra María Ríos representante de “XM” empresa encargada del control y despacho de energía, dio a conocer las políticas de seguridad nacional e infraestructura, partiendo de un contexto global, haciendo énfasis en los principales ataques sucedidos a nivel mundial, para finalmente sociabilizar los marcos adoptados por el sector eléctrico colombiano para combatir o minimizar los ciberataques. El concejo nacional de Operación del sistema eléctrico colombiano “CNO” contiene la guía de ciberseguridad para realizar la gestión. Desde el nacimiento de la Unidad de Planeación Minero Energética – UPME ocurrido en los años 1992 en Colombia, el sector eléctrico ha jalonado el diseño y la construcción de subestaciones eléctricas basadas en la pirámide de control para adecuar diferentes arquitecturas de operación y control. Los proyectos de UPME01 revolucionaron la forma y los procesos de construir subestaciones eléctricas en la mente de los ingenieros, para beneficio del sector que desde entonces crece con muy buenas expectativas tecnológicas. UPME01, UPME02, construyen subestaciones en alta y ultra alta tensión, topológicamente cerraron el anillo en 500 kilo voltios entre la costa atlántica, las grandes generadoras ubicadas en Antioquia y el oriente colombiano. Nuevos interruptores de potencia, nuevos seccionadores de corte central y pantógrafos, fibra óptica mono y multimodo en salas de operación, computadores de propósito específico, dispositivos electrónicos inteligentes “IED´s”, marcas reconocidas ABB Siemens, referencias típicas como REL 670, 7SJ, 6MD, etc., y con ellas vulnerabilidades a la orden del día, que intentan ser controladas por ingenieros administradores de las TIC o en su defecto ingenieros con principios básicos de TO. Por la necesidad de la interoperabilidad de los IED´s de diferentes fabricantes la popularidad de la aplicación del estándar IEC 61850 en las subestaciones eléctricas aumenta en cada proyecto, la combinación y el uso de protocolos de comunicación industrial cada vez es más frecuente y se hace tan común en cada proyecto identificar el protocolo IEC 61850 traducido a IEC 60870-5-101 mediante una aplicación OPC. Todo muy parecido por no decir casi igual al panorama ofrecido en 2016 a los atacantes en Ucrania, cuando a través de puertas traseras ingresaron a los sistemas de control y cargaron e instalaron su carga útil “Payload” para afectar los protocolos y rápidamente desplazar los comandos legítimos de los interruptores de potencia por comando manejados dese servidores de C&C por los atacantes.	
Autores del RAE	Pedro Julio Mendoza Villamil y Álvaro Díaz Ardila