# Tácticas, Técnicas y Procedimientos para escenarios de ciberataque y ciberdefensa en infraestructura critica basada en procesos de control industrial basados en el protocolo modbus*

Manuel Humberto Santander Peláez *

## Introducción

La industria eléctrica provee el servicio de energía eléctrica a toda la población y a diferentes industrias. Es un sector de infraestructura crítica en casi todos los países y se convierte en uno de los motores fundamentales del funcionamiento de la sociedad y la economía. Los siguientes negocios operan en dicha industria:

- Generación: Su propósito es la producción de energía eléctrica a partir de fuentes primarias. A continuación, se detallan los principales tipos de centrales eléctricas o centrales de generación: Central hidroeléctrica (Embalse, borde de agua, minicentral), Central Térmica (carbón, gas, fuel oil, entre otros), Energía Renovable entre otros). Corresponde a una persona física o jurídica que produce electricidad, que tiene al menos una planta o unidad generadora conectada al Sistema Interconectado Nacional (SIN).

* Esta ponencia es un avance del Proyecto de Investigación "Desarrollo de capacidades en ciberseguridad y Ciberdefensa para el Estado Colombiano", adscrito al grupo de Investigación Masa Crítica de la Escuela Superior de Guerra en su línea de Terrorismo, Nuevos Guerras y Desafíos a la seguridad.

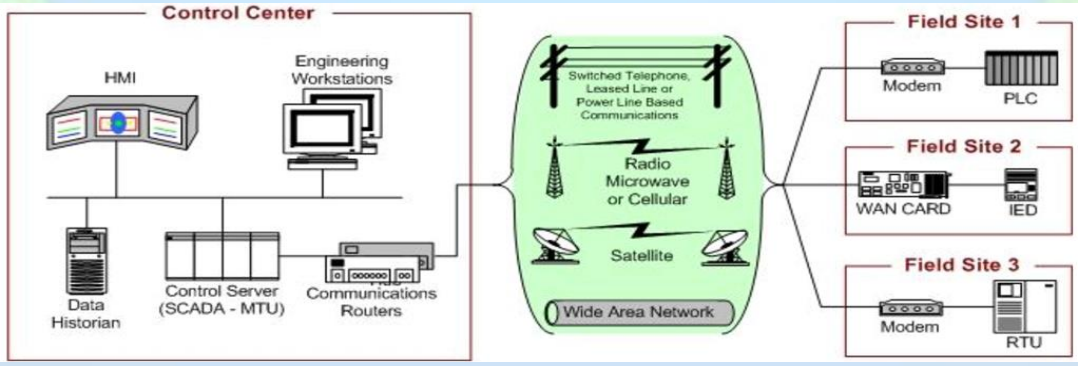
* Estudiante Doctorate of Information Assurance - University of Fairfax, Virginia – Estados Unidos. Magíster en Administración de Negocios de la Universidad de Eafit y Magíster en Ingeniería de Seguridad de la Información de Sans Technology Institute – Maryland, Estados Unidos y Profesional en Ingeniería de Sistemas de la Universidad de Eafit. Arquitecto de Seguridad de la Información, Chief Information Security Officer de la Dirección de Estrategia y Arquitectura de IT de Empresas Públicas de Medellín. Asesor científico del Instituto Tecnológico de Medellín – ITM, Docente e Investigador de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra.

- Transmisión: Su objetivo es transportar energía eléctrica a través del SIN entre los sitios de generación y las subestaciones de distribución, para lo cual se utilizan subestaciones de alto voltaje (230KV o superior) y líneas de transmisión. Este negocio también es responsable de la operación, mantenimiento y expansión de los sistemas de transmisión, ya sean nacionales o regionales. El SIN tiene 723 subestaciones de transmisión y distribución, de las cuales 233 operan a niveles de alta tensión y cuenta con más de 24.000 kilómetros de líneas de transmisión.
- Distribución: Su objetivo es llevar la energía eléctrica de las subestaciones de transmisión a los diferentes centros de consumo, como la vivienda, el comercio y las industrias. Las redes de distribución, que se componen principalmente de postes y transformadores de distribución, se utilizan para suministrar electricidad. Este negocio asegura un servicio confiable y de calidad a la población ya las industrias. También se encarga de la operación, mantenimiento y expansión de los sistemas de distribución.
- Comercialización: Responsable de la compra y venta de electricidad del mercado mayorista y su venta a otras operaciones en ese mercado a los usuarios finales (Comando Conjunto Cibernético de Colombia, 2016)

La industria de la electricidad necesita una tecnología principal para asegurar la coordinación de todos los componentes de la Tecnología de Operación (OT) desde un único centro central y se llama Sistemas de Supervisión y Adquisición de Datos (SCADA).

Los sistemas SCADA se utilizan para controlar los activos dispersos en los que la adquisición centralizada de datos es tan importante como el control (Stouffer, et al., 2015). Estos sistemas son capaces de controlar varias variables en este negocio como garantizar una cantidad específica de electricidad generada, asegurar una cantidad específica de flujo eléctrico en las líneas de transmisión, decidir qué usuario es capaz de utilizar el servicio eléctrico y quién no puede, entre muchos otros. Los sistemas SCADA integran sistemas de adquisición de datos con sistemas de transmisión de datos y software de Human to Machine (HMI) para proporcionar un sistema de supervisión y control centralizado para numerosas entradas y salidas de proceso. Los sistemas SCADA están diseñados para recopilar información de campo, transferirla a un centro informático central y mostrar la información al operador gráficamente o textualmente, permitiendo así al operador monitorear o controlar un sistema completo desde una ubicación central en tiempo casi real. Basado en la sofisticación y configuración del sistema individual, el control de cualquier sistema, operación o tarea individual puede ser automático, o puede ser realizado por comandos del operador.

**Figura 1.** Componentes sistema SCADA (Stouffer, et al., 2015).




**Fuente**: Stouffer (2015).

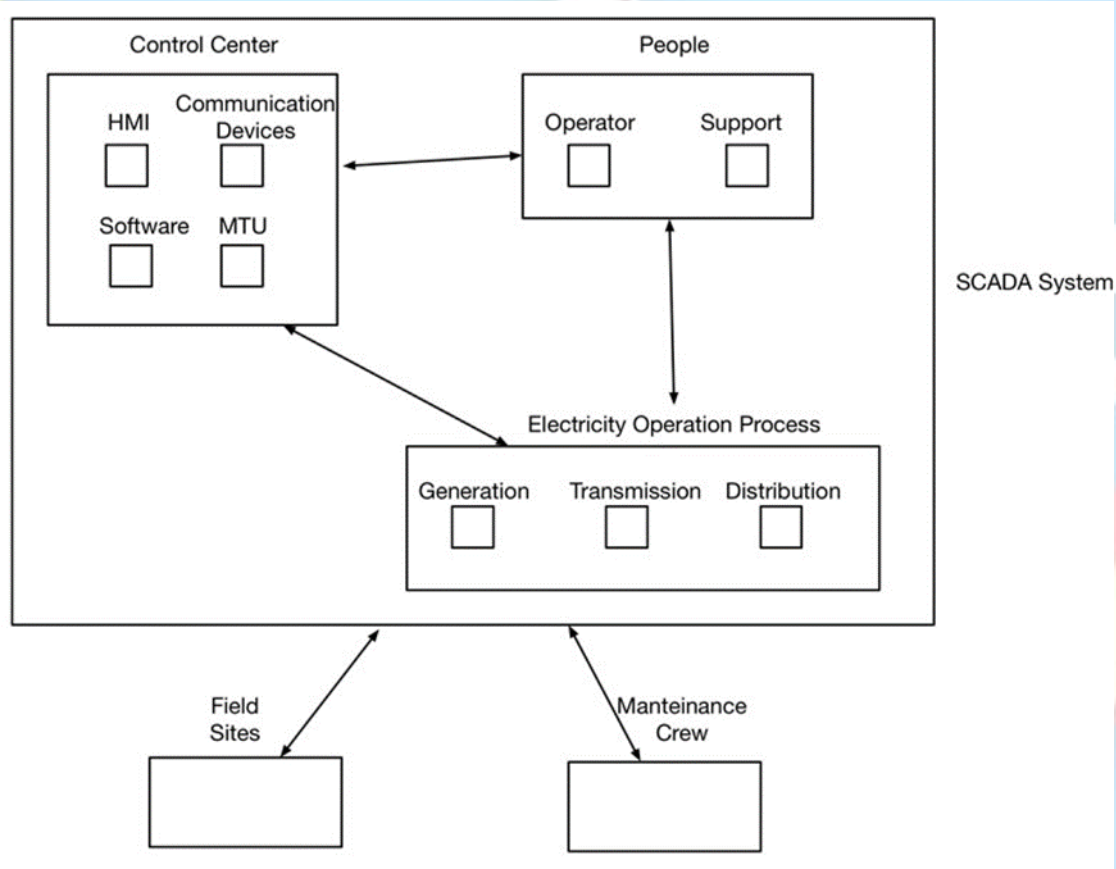
La Figura 1 muestra los componentes y la configuración general de un sistema SCADA (Stouffer, et al., 2015). El centro de control está compuesto por un servidor de control, enrutadores de comunicaciones, una HMI, algunas estaciones de trabajo de ingeniería y el historiador de datos, todos conectados por una LAN. El centro de control realiza las siguientes funciones:

- Recoge y registra la información recogida por todos los elementos de la estación, muestra información al HMI y puede generar acciones a los dispositivos OT basándose en los eventos detectados.
- Realiza alarmas centralizadas, análisis de tendencias y reportes.

Los sitios de campo realizan el control local de los dispositivos OT presentes en las plantas de generación, subestaciones de transmisión y subestaciones de distribución. Los protocolos de comunicación utilizados para operar las estaciones que funcionan a través de comunicaciones en serie y en red son tanto estándar como propietarios.

La Figura 2 muestra los componentes de los límites del sistema SCADA. Los siguientes componentes forman parte del límite del sistema (Stouffer, et al., 2015):

**Figura 2.** Límites del sistema SCADA




- Centro de control, que agrega hardware (HMI), software, dispositivos de comunicación y unidad maestra de terminales (MTU).
- Personas: Hay dos roles: el operador, que los servidores de 8 horas de turno. Tres turnos se sirven todos los días para un total de tres operadores y soporte, que maneja posibles fallos o trabajos de mantenimiento al centro de control.
- Proceso: para este caso, habrá tres procesos: Operación para generación, transmisión y distribución de electricidad.

- Sistemas externos: Existen dos: sitios de campo, que son planes de energía hidroeléctrica y subestaciones de transmisión y distribución y equipos de mantenimiento para operaciones físicas en los sitios de campo.

## Discusión de resultados

### Análisis de riesgos

De acuerdo con los tres propósitos del análisis del impacto de los negocios, declarados por Paul Hopkin (Hopkin, 2014), los riesgos del centro de control pueden afectar a los siguientes objetos:

- Financiero: La compañía de electricidad podría no ser capaz de generar electricidad y pagar compensaciones onerosas debido al incumplimiento del contrato
- Personas: Las partes interesadas podrían morir debido a acciones como la apertura de una represa hidroeléctrica y la correspondiente inundación masiva.
- Reputación: La industria podría buscar otro proveedor de electricidad debido a una reputación degradada de la compañía de electricidad debido a ataques de ciberseguridad.

La figura 1 del centro de control describe todos los recursos que se pueden encontrar en un sistema SCADA y se tomaron como entrada principal para el análisis de riesgo. La Tabla 1 muestra el mapa de los atributos de seguridad de la información que forman parte del análisis y las correspondientes amenazas asociadas (May & Rohde, 2005) (Lathrop et al., 2006).

**Tabla 1.** Mapa entre el atributo y la amenaza de seguridad de la información asociada

| Atributo | Amenaza |
|---|---|
| Confidencialidad | Acceso no autorizado |
| | Reconocimiento de red |
| Integridad | Modificación de la configuración del ciberactivo |
| | Modificación no autorizada del estado del proceso industrial |
| Disponibilidad | Negación del servicio |
| Trazabilidad | Pérdida de registros |
| No repudio | Imposibilidad de la identificación de un ataque |

Después de un análisis detallado, se ha recogido una lista de vulnerabilidades que se materializan en un sistema SCADA. Se utilizó la categoría de riesgo de Hopkin y luego se evaluó el riesgo con una calificación de magnitud y probabilidad. La Tabla 2 muestra los resultados obtenidos para los riesgos de confidencialidad e integridad. La Tabla 3 muestra los resultados obtenidos para los riesgos de disponibilidad, trazabilidad y no repudio.

| Amenaza | Vulnerabilidad | Objeto de impacto | Categoría del riesgo | Impacto | Probabilidad |
|---|---|---|---|---|---|
| Acceso no autorizado | Malware de Amenazas Persistentes Avanzadas (APT) | Financiero, reputación | Peligro | Alto | Alto |
| | Ataque de hombre en el medio | Financiero, reputación | Peligro | Moderado | Medio |
| | Ingeniería Social | Financiero, reputación | Peligro | Moderado | Muy alto |

| | | | | | |
|---|---|---|---|---|---|
| | Falla en los controles de acceso de seguridad física | Financiero, reputación | Control | Moderado | Bajo |
| | Parches de seguridad incompletos | Financiero, reputación | Control | Moderado | Muy alto |
| | Puertos vulnerables habilitados | Financiero, reputación | Peligro | Moderado | Medio |
| Reconocimiento en la red | Configuraciones por defecto | Reputación | Control | Alto | Muy alto |
| | Escalamiento de privilegios | Reputación | Peligro | Moderado | Muy alto |
| | Falla en los controles de acceso de seguridad física | Reputación | Control | Moderado | Bajo |
| Modificación de la configuración del ciberactivo | Falla en los controles de acceso de seguridad física | Financiero, reputación, personas | Control | Moderado | Bajo |
| | Parches de seguridad incompletos | Financiero, reputación, personas | Control | Moderado | Muy alto |
| | Puertos vulnerables habilitados | Financiero, reputación, personas | Peligro | Moderado | Medio |
| | Robo de identidad | Financiero, reputación, personas | Peligro | Moderado | Medio |
| Modificación no autorizada del estado del proceso | Falla en los controles de acceso de seguridad física | Financiero, reputación, personas | Control | Moderado | Bajo |

| | | | | | |
|---|---|---|---|---|---|
| industrial | Parches de seguridad incompletos | Financiero, reputación, personas | Control | Moderado | Muy alto |
| | Puertos vulnerables habilitados | Financiero, reputación, personas | Peligro | Moderado | Medio |
| | Robo de identidad | Financiero, reputación, personas | Peligro | Alto | Muy alto |
| | Requerimientos maliciosos del protocolo | Financiero, reputación, personas | Peligro | Alto | Muy alto |

Tabla 2. Riesgos de confidencialidad e integridad

| **Amenaza** | **Vulnerabilidad** | **Objeto de impacto** | **Categoría del riesgo** | **Impacto** | **Probabilidad** |
|---|---|---|---|---|---|
| Negación del servicio | Falla en los controles de acceso de seguridad física | Financiero, reputación, personas | Control | Moderado | Baja |
| | Parches de seguridad incompletos | Financiero, reputación, personas | Operacional | Moderado | Muy alta |
| Pérdida de registros | Configuraciones por defecto | Financiero | Control | Alto | Muy alto |
| | Falla en los controles de acceso de seguridad física | Financiero | Control | Moderado | Bajo |
| | Parches de seguridad incompletos | Financiero | Control | Moderado | Muy alto |
| | Robo de identidad | Financiero | Peligro | Alto | Muy alto |

| | | | | | |
|---|---|---|---|---|---|
| Imposibilidad de identificación del atacante | Deshabilitación de los controles de no repudio | Reputación | Peligro | Alto | Alto |

Tabla 3. Riesgos de disponibilidad, trazabilidad y no repudio

Después del análisis de riesgos, se encontraron las siguientes diferencias:

- Uso de protocolo inseguro: los protocolos SCADA son muy antiguos. Los primeros fueron diseñados antes de TCP / IP y no consideraron los requisitos de seguridad, ya que fueron utilizados principalmente en entornos serie. Existen nuevos estándares de seguridad como IEC 61850 que imponen fuertes controles de seguridad de la información que se utilizarán en las comunicaciones del centro de control a las estaciones de campo. Sin embargo, todos los dispositivos del sitio de campo deben ser capaces de soportar esas nuevas características y necesitan ser reemplazados completamente primero. Los controles que abordan las vulnerabilidades de protocolo deben estar en su lugar.
- Ausencia de monitoreo de seguridad cibernética: dispositivos como firewalls e IPS se usan comúnmente en entornos de TI para monitorear posibles ataques a activos de seguridad de la información. Sin embargo, el uso de dispositivos IPS y firewall en entornos OT no es común debido a problemas de latencia. Un retraso de 10 ms no es un problema en una transmisión entre dispositivos de TI, pero en una SCADA de energía podría ser la diferencia entre un aumento controlado de electricidad en una línea de transmisión o un apagón masivo con daños a dispositivos activos como interruptores o transformadores.

- Configuración predeterminada para dispositivos de centro de control: el software Early SCADA no consideró el concepto de endurecimiento del sistema operativo o requisitos de seguridad de la información, ya que la disponibilidad y la transmisión rápida son la principal prioridad de cada proceso industrial. Se diseñó teniendo en cuenta tener todos los privilegios de administrador y muchos servicios inseguros del sistema operativo activos. Como resultado, no se puede realizar ningún endurecimiento a los servidores SCADA porque el proceso industrial simplemente no funcionaría.
- Nombre de usuario y contraseña locales para servidores: Los entornos de TI están enlazados a directorios que definen qué usuarios pueden iniciar sesión en el sistema y qué tareas se permiten. En los sistemas SCADA, es realmente extraño encontrar directorios centrales y es por eso que sólo los usuarios del sistema operativo local se utilizan. Los fabricantes recomiendan encarecidamente a las compañías de electricidad que utilicen nombres de usuario genéricos compartidos con todo el equipo de operaciones.
- Sólo la autenticación de contraseña almacenada en sistemas SCADA para sitios de campo: En entornos de TI, la operación de inicio de sesión a dispositivos se realiza con nombre de usuario y contraseña. Para dispositivos OT ubicados en estaciones de campo, el estándar es dos contraseñas: una para operaciones de sólo lectura y otra para operaciones de configuración. Los sistemas SCADA no pueden almacenar de forma segura las dos contraseñas y, por lo tanto, son propensos a ser robados por los atacantes.

- Identidad no unificada para todos los dispositivos: Dado que los nombres de usuario son locales, el equipo de operación tendrá varios usuarios diferentes para cada servidor o equipo ubicado en el centro de control. Esto podría ser utilizado para el robo de identidad o simplemente camuflar cualquier operación maliciosa.
- No se aplica el control de tráfico válido dentro del centro de control y desde / hacia los sitios de campo: El sistema SCADA analizado no implementa actualmente ninguna aplicación de tráfico hacia o desde sitios de campo. El tráfico puede fluir libremente y no hay seguimiento en qué dispositivos se conectan a la red ni el tráfico que comprueba qué comandos se envían a los sitios de campo.

**Ciberinteligencia como solución para anticiparse a los ataques**

Estos riesgos pueden ser aprovechados por los distintos atacantes para ocasionar impactos en el funcionamiento del sistema eléctrico. Por ser una infraestructura crítica, el nivel de continuidad y disponibilidad del servicio debe ser considerablemente alto, pues no es tolerable que porciones de la población o la población en su totalidad no posean fluido eléctrico para la ejecución normal de sus actividades del día a día.

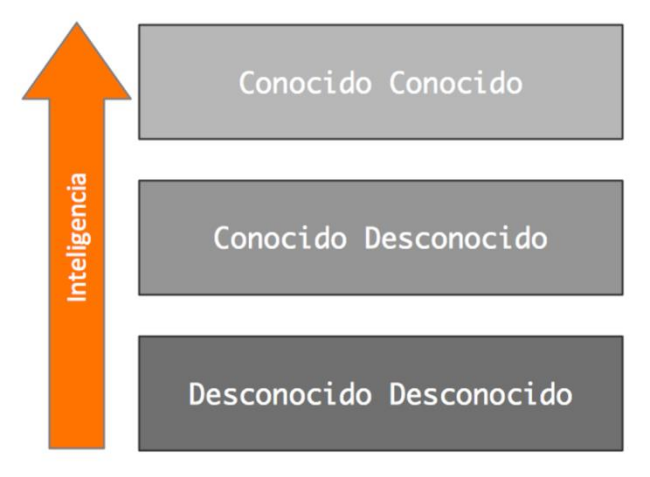
Asegurar la continuidad y la disponibilidad implica la implantación en una entidad de la capacidad de ciberinteligencia y gestión de vulnerabilidades, la cual tiene como propósito establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de la

ciberseguridad de forma proporcional al riesgo y objetivos organizacionales. Para efectos de ciberseguridad, una amenaza se define como cualquier circunstancia o evento con el potencial de afectar adversamente las operaciones organizacionales incluyendo su misión, funciones, imagen, reputación, recursos u otras organizaciones a través de TI, TO o infraestructura de comunicaciones mediante cualquiera de los riesgos revisados en la tabla número 2.

La ciberinteligencia implementa un proceso de cambio de estado de las amenazas o riesgos de ciberseguridad del estado desconocido desconocido a conocido desconocido en donde se hacen visible para la organización y se constata que no habían sido contemplados previamente. Esto permite prepararse y hacerles frente a las amenazas para posteriormente cambiarlos de estado a conocido conocido en donde la amenaza es entendida completamente y mitigada. En la figura 3 puede observarse el diagrama ilustrativo de cambios de estados de las amenazas y riesgos de ciberseguridad en el proceso de ciberinteligencia.

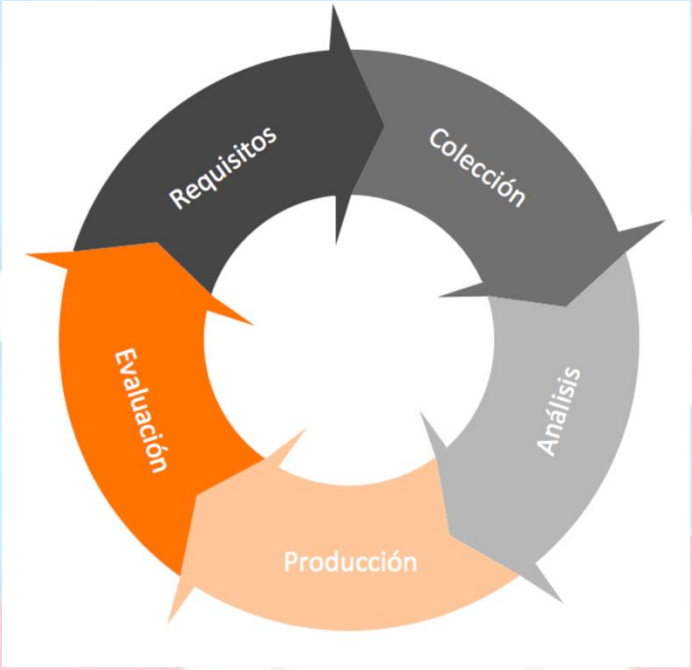
La situación ideal es tener la mayoría de los riesgos en la categoría conocido conocido y continuar trabajando el desarrollo de los riesgos conocido desconocido, propendiendo por siempre tener una vigilancia permanente para minimizar el número de amenazas y riesgos en desconocido desconocido. Este es el reto constante en los campos de la inteligencia tradicional y la inteligencia cibernética.

**Figura 3.** Diagrama cambio de estado de amenazas en el proceso de inteligencia




El proceso de una central de inteligencia tiene diversos componentes con especialidades distintas, lo cual aumenta la probabilidad de encontrar personal capacitado en aspectos específicos del proceso y así facilita el establecimiento de la correspondiente matriz RACI. Las piezas individuales del ciclo pueden ser desarrolladas y revisadas contra el desempeño esperado para descubrir debilidades potenciales. En la figura 4 es posible revisar los distintos componentes del ciclo de vida de la central de inteligencia. A continuación, se revisará cada uno de los componentes de este ciclo propuesto para la infraestructura crítica:

**Figura 4**. Ciclo de vida ciberinteligencia




- Requisitos: Este paso es uno a los que menos importancia se le da en el mercado, pero en realidad es uno de los más importantes, pues determina lo que el negocio espera para iniciar el tratamiento de riesgos no cubiertos. En este paso se define claramente lo que se requiere conocer de los distintos activos de la empresa con base en los distintos canales de información a los que se tiene acceso que pudiera evidenciar la existencia de riesgos no contemplados previamente. Deben ser concretos y con un alcance especifico.
- Colección: Este es el paso que consume el mayor presupuesto y tiempo, después de tener toda la claridad de los requisitos en este paso se recolecta toda la información necesaria para dar una respuesta completa a estos. Esta información puede venir de una gran variedad de fuentes, tales como orígenes de noticias, fuentes pagas de información, foros, sistemas internos y cualquier variedad de recursos. Después de

tener toda esta información se debe hacer un análisis de la misma, es una gran cantidad de información y esto puede consumir mucho tiempo, no es un proceso trivial. Por esto se debe tener claridad en cada una de las dimensiones de la central de inteligencia.

- Análisis: Después de tener toda la información requerida para el caso, se debe hacer un análisis de la misma, esta parte algunas veces puede ser simple, pero en otras oportunidades puede ser una tarea muy compleja. Además de resolver el caso, esta parte es crucial para hacer otro tipo de inteligencia que ayuda a hacer una correlación mayor o generar un nuevo conocimiento para descubrir nuevas amenazas y amenazas ocultas. Siempre debe haber una interconexión entre la colección de datos y el análisis. El análisis debe llevarse a través de muchas fuentes de colección de datos para poder llegar a conclusiones que den con lo que son los requisitos del negocio y poder tomar una decisión más asertiva.
- Producción / Difusión: En esta actividad, el producto como tal de una central de inteligencia es creado y se debe hacer su difusión a sus clientes. El producto varía, dependiendo del tipo de inteligencia y el cliente, el producto puede ser un informe detallado, un informe gerencial, puntos de compromiso o un informe técnico, entre otros tipos de informes.
- Evaluación: Este paso muchas veces no se tiene en cuenta, es en el que se evalúa si el producto resultante cumple realmente con los requerimientos iniciales. Si cumple con todo, este producto puede ser una fuente adicional para la central de inteligencia y vuelve a iniciar el ciclo. Cuando el resultado no va acorde a los requerimientos, en

este paso se hace una evaluación si los requerimientos no fueron realistas, si no se comprendió lo que se deseaba, si se utilizaron fuentes erróneas o si la información si es la correcta pero el análisis no fue el correcto y si el producto final no tuvo una ganancia en inteligencia, o bien evaluar si el producto final identifica acciones ocultas no conocidas.

**Indicadores de compromiso**

Es importante ser muy cuidadoso en el proceso de colección, pues no toda la información que proviene de las fuentes puede brindar datos que sean claves para poder anticipar adecuadamente la amenaza. Por lo anterior, debemos establecer a partir de los riesgos qué información podemos llegar a necesitar para que el proceso de producción brinde la información requerida. Esta información requerida para la generación de productos de inteligencia que provean valor en la anticipación de amenazas se denominan indicadores de compromiso y pueden ser de las siguientes clases, de acuerdo con lo establecido por el modelo pirámide del dolor:

- Valores de hash: SHA1, MD5 u otros hashes similares que corresponden a archivos sospechosos o maliciosos específicos. A menudo se utiliza para proporcionar referencias únicas a muestras específicas de malware o a los archivos involucrados en una intrusión.
- Direcciones IP: Corresponde a direcciones IP que pudieran estar implicados en algún hecho anómalo. Pueden utilizarse también prefijos de red y los correspondientes sistemas autónomos.

- Nombres de Dominio: Corresponde a los Fully Qualified Domain Name (FQDN) que pudieran estar involucrados en hechos anómalos o subdominios con múltiples niveles. Como ejemplo, podemos tener malware.evil.net o i.am.malware.evil.net.
- Artefactos de red: Estos artefactos corresponden a tráfico de red y rastros dejados por las actividades de los atacantes en su red de datos. Técnicamente hablando, cada byte que fluye a través de su red como resultado de la interacción del adversario podría ser un artefacto, pero en la práctica significa realmente aquellas piezas de la actividad que podrían tender a distinguir la actividad maliciosa de la de los usuarios legítimos. Algunos ejemplos típicos pueden ser URL, información de comando y control encapsulada en los protocolos de red, valores distintivos de HTTP User-Agent o SMTP Mailer, etc.
- Artefactos del host: Estos artefactos corresponden a rastros dejados por actividades adversarias en uno o más de sus equipos. Una vez más, nos centramos en cosas que tenderían a distinguir las actividades maliciosas de las legítimas. Pueden ser claves de registro o valores conocidos por ser creados por piezas específicas de malware, archivos o directorios eliminados en ciertos lugares o usando ciertos nombres, nombres o descripciones o servicios maliciosos o casi cualquier otra cosa que sea distintiva.
- Herramientas: Corresponde a software utilizado por el adversario para cumplir su misión. En su mayoría corresponde a software que los atacantes poseen y que no corresponden a comandos que ya pueden estar instalados en el equipo.

Algunas de estas herramientas incluyen utilidades diseñadas para crear documentos maliciosos para spearphishing, backdoors usados para establecer comando y control de los equipos o crackers de contraseña.

- Tácticas, Técnicas y Procedimientos (TTPs): Corresponde al curso de acción que el atacante va escogiendo para la ejecución de su misión, desde el reconocimiento hasta el final de la exfiltración de datos incluyendo cada paso intermedio. Los TTP no son herramientas específicas. Existen varios ejemplos:
    - El spearphishing es un TTP común para establecer una presencia maliciosa al interior de la red y las clasificaciones son "Spearphishing con un archivo PDF trojaned" o "... con un enlace a un archivo .SCR malicioso disfrazado de ZIP"
    - "El vaciado de las credenciales de autenticación en caché y su reutilización en los ataques Pass-the-Hash" sería un TTP. Tenga en cuenta que no estamos hablando de herramientas específicas aquí, ya que hay muchas maneras de armar un PDF o implementar Pass-the-Hash.

**Tácticas, técnicas y procedimientos**

Los módulos SCADA dentro del centro de control son capaces de realizar cualquier tipo de acciones a las estaciones eléctricas. Muchos de esos impactos son conocidos como riesgos no asegurables, ya que las consecuencias financieras son demasiado altas. De acuerdo con el listado de riesgos discutidos en el numeral 2.1, los siguientes impactos podrían materializarse (Zhao & Zhang, 2013):

- Apertura de compuertas en represas hidroeléctricas: Esta acción desencadena un aumento en el caudal permitido por el río utilizado para expulsar el caudal de agua utilizado en el proceso de generación. Esto puede causar inundaciones y avalanchas en extensiones de varios kilómetros, generando pérdidas de vidas humanas, cultivos y desequilibrios en los ecosistemas naturales.
- Daños a los generadores de las principales centrales hidroeléctricas: Si un atacante decide llevar a cabo una acción similar a la llevada a cabo en las centrales nucleares de Irán, es posible dañar los generadores de las plantas más grandes, lo que provocaría una demanda insatisfecha de electricidad en Irán. El país, causando racionamiento prolongado durante meses. Esto tendría un impacto en la competitividad del país a través de paros de producción, pérdida de vidas humanas, daños a las rutas terrestres, destrucción de cultivos agrícolas, entre otros.
- Explosión del transformador de la subestación del transformador: Si un atacante cambia en un tiempo muy corto y con gran desviación la relación de transformación del transformador, causaría una explosión que tendría consecuencias sobre las propiedades circundantes, causando un fallo de servicio. Tienen como consecuencia posible un apagón nacional.

La infraestructura eléctrica nacional funciona bajo el protocolo Modbus. Este protocolo fue creado por Modicon en 1979, el cual plantea las siguientes operaciones básicas, críticas en ciberseguridad:

- Read coils: Permite la lectura de información de las bobinas conectadas al PLC

- Force/write single coil: Permite escritura de información a una única bobina conectada al PLC
- Force/write multiple coil: Permite escritura de información a múltiples bobinas conectada al PLC
- Read input registers: Permite la lectura de información de los registros correspondientes a la medición de dispositivos análogos conectados.
- Write single holding registers: Permite la escritura por set points a un solo registro que gobierna un dispositivo encargado de realizar mediciones de variables.
- Write multiple holding registers: Permite la escritura por set points a múltiples dispositivos que gobiernan múltiples dispositivos encargados de realizar mediciones de variables.

**Tabla 4.** Funciones de operación en modbus

| **Tipo de acceso** | | | **Nombre de función** | **Código de función** |
|---|---|---|---|---|
| Acceso de datos | Bit access | Physical Discrete Inputs | Read Discrete Inputs | 2 |
| | | Internal Bits or Physical Coils | Read Coils | 1 |
| | | | Write Single Coil | 5 |
| | | | Write Multiple Coils | 15 |
| | 16-bit access | Physical Input Registers | Read Input Register | 4 |
| | | Internal | Read Holding Registers | 3 |

| | | | | |
|---|---|---|---|---|
| | | Registers or Physical Output Registers | Write Single Register | 6 |
| | | | Write Multiple Registers | 16 |
| | | | Read/Write Multiple Registers | 23 |
| | | | Mask Write Register | 22 |
| | | | Read FIFO Queue | 24 |
| | File Record Access | | Read File Record | 20 |
| | | | Write File Record | 21 |

La tabla 4. Describe todas las operaciones que implementa modbus.

La interacción a nivel de red no involucra en ninguno de los pasos la realización de autenticación fuerte entre el maestro y esclavo, motivo por el cual el protocolo es sujeto a riesgos de suplantación del HMI, permitiendo la ejecución de tareas en los PLC que pudiera llevar a la materialización de los riesgos descritos al inicio de la presente sección. Esto implica que el rastreo de las distintas direcciones IP que interactúan en la red, especialmente la dirección IP del HMI, pues es fundamental reconocer a tiempo si llega a existir algún tipo de requerimiento hacia los dispositivos de control que provenga desde alguna dirección que no sea conocida en el proceso industrial.

La realización de operaciones técnicas en la infraestructura eléctrica involucra la ejecución de secuencia de tareas a través del envío de solicitudes de ejecución con cualquiera de las funciones de operación descritas en la tabla 4. Para esto, se hace necesario que cada dueño de infraestructura eléctrica realice una línea base en donde se determine de

forma estadística cuál es la cantidad de operaciones por cada código de función que se repiten día a día, con la correspondiente desviación estándar. Una vez se obtenga la información, cualquier desviación más allá de la desviación estándar para las operaciones de lectura y escritura para coils y registros se constituye en una operación anormal del sistema eléctrico, no ejecutada por el operador ubicado en el centro de control central y que debe ser tratado como cualquier incidente de ciberseguridad.

Las TTP identificadas que pudieran materializar los riesgos descritos en la sección 2.1 y los impactos descritos en el numeral 2.4 son los siguientes:

- Escritura de registros múltiples en el controlador de subestación para aumentar la relación de transformación en las centrales de transmisión: Esto implica que deben detectarse al menos un aumento del 10% en la utilización del código de función 23. Pueden darse variantes de modificación en donde se suplante la dirección IP, pero la dirección MAC es distinta al detectado del HMI original oficial del centro de control central.
- Escritura de múltiples bobinas para cambio de la velocidad del regulador de velocidad: Esto implica que debe detectarse al menos un aumento del 15% en la utilización del código de función 15. Pueden darse variantes de modificación en donde se suplante la dirección IP, pero la dirección MAC es distinta al detectado del HMI original oficial del centro de control central.
- Escritura de única bobina para la apertura de circuitos en los IED de las subestaciones de transmisión: Se realiza una suplantación del HMI del centro de control central, pero la dirección MAC es distinta al detectado del HMI original

enviando un paquete con el código de función 5. Es suficiente que una única solicitud llegue al dispositivo para accionar el ataque.

- Escritura de un único registro para la alteración del porcentaje de apertura de compuertas: Se realiza una suplantación del HMI del centro de control central, pero la dirección MAC es distinta al detectado del HMI original con el código de función 6. Es suficiente que una única solicitud llegue al dispositivo para accionar el ataque.

**Conclusiones**

Las tácticas, técnicas y procedimientos que se utilizan en la ejecución de las operaciones militares son extrapolables en su totalidad al mundo cibernético. El problema a resolver es distinguir las operaciones normales de las operaciones maliciosas. A través de la detección de desviaciones mayores a las desviaciones estándar de las muestras detectadas pueden detectarse posibles acciones anormales que pueden ser sujetas de acciones de respuesta a incidentes en ciberseguridad. Estas detecciones de comportamientos están enmarcadas en la fase de colección del proceso de inteligencia y se hace fundamental para anticiparse a la ocurrencia de cualquier hecho anormal que impacte el funcionamiento de la infraestructura que presta el servicio de electricidad.

**Referencias**


Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to industrial control systems (ICS) security*. Gaithersburg, MD: National Institute of Standards and Technology. Recuperado de: http://dx.doi.org/10.6028/NIST.SP.800-82r2

National Institute of Standards and Technology. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems: a security lifecycle approach*. Recuperado de: http://dx.doi.org/10.6028/NIST.SP.800-37r1

National Institute of Standards and Technology. (2004). *Standards for security categorization of federal information and information systems*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory. doi:10.6028/NIST.FIPS.199

Ciprian, B. (2011). SCADA SECURITY IN THE CONTEXT OF CORPORATE NETWORK INTEGRATION. Universitatii Maritime Constanta.Analele, 12(15), 159-164. Retrieved from https://search-proquest-com.ufairfax.idm.oclc.org/docview/912813776?accountid=158316

May, R. P., & Rohde, K. (2005). Cyber assessment methods. Intech, 52(11), 28-31. Retrieved from https://search-proquest-com.ufairfax.idm.oclc.org/docview/208809843?accountid=158316

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. Engineering Management Journal, 25(2), 38-45. Retrieved from https://search-proquest-com.ufairfax.idm.oclc.org/docview/1434438191?accountid=158316

Hadziosmanovic, D., Bolzoni, D., & Hartel, P. H. (2012). A log mining approach for process monitoring in SCADA. International Journal of Information Security, 11(4), 231-251. doi: http://dx.doi.org.ufairfax.idm.oclc.org/10.1007/s10207-012-0163-8

Lathrop, S. D., Gates, C. L., Massie, D. D., & Hill, J. M. D. (2006). Risk assessment of a power plant: Evaluating the security of a supervisory control and data acquisition system. ASHRAE Transactions, 112, 671-679. Retrieved from https://search-proquest-com.ufairfax.idm.oclc.org/docview/192545036?accountid=158316

Zhao, X. L., & Zhang, J. H. (2013). Power system risk assessment software design under impact of disaster conditions. Applied Mechanics and Materials, 441, 204. doi:http://dx.doi.org.ufairfax.idm.oclc.org/10.4028/www.scientific.net/AMM.441.204

Stouffer, K., Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. http://dx.doi.org/10.6028/SINT.SP.800-82r2

Comando Conjunto Cibernético de Colombia. (2016). Sectores estratégicos de la República de Colombia desde la óptica cibernética (1st ed.). Bogotá D.C., CO: Comando General Fuerzas Militares.

Technical Support Working Group. (2005). Securing your SCADA and Industrial Control Systems (1st ed.). Washington, DC: U.S. Department of Homeland Security.

Hopkin, Paul (2014). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page. Kindle Edition.