Trabajo Final de Máster: Investigación de la Ciberseguridad aplicada a los Sistemas de Control Industrial con énfasis en el sector energético

Autor: Julián Andrés García Arias

Diciembre 2017
Máster Universitario Seguridad de las Tecnologías de la Información y las Comunicaciones (MISTIC)
Universidad Oberta de Catalunya

Directores: Dr. Víctor García Font
Dra. Ángela María García Valdés

Resumen Ejecutivo

El acceso a Internet provoca un aumento de la productividad de las naciones, del ingreso y del empleo, así como también es un motivador de crecimiento. Sin embargo, estas oportunidades conllevan ciertos riesgos debido a que las tecnologías digitales aún no están lo suficientemente maduras, ocasionando que la delincuencia pueda aprovecharse de los riesgos. La ciberseguridad aplicada a los sistemas de control industrial ha venido tomando mayor y más relevancia en los últimos años, al punto que ciertos sectores e industria en donde se utilizan estos sistemas son catalogados infraestructuras críticas. Las estrategias de ciberseguridad que vienen desarrollando los países, definen objetivos que abordan cuestiones sobre la protección a la sociedad frente a las amenazas cibernéticas y el fomento a la prosperidad económica y social en un contexto en donde las principales actividades se basan en el uso de las tecnologías de la información y de la comunicación.

Este trabajo final consiste en la investigación de la ciberseguridad aplicada a los sistemas de control industrial, mediante un estudio de la seguridad cibernética en plantas industriales que tienen sistemas tipo SCADA. También se analizará cómo explotar estos sistemas y de qué manera mitigar y prevenir sus vulnerabilidades. En la investigación se cubrirán aspectos tales como el propósito de los sistemas de control industrial y por qué es importante la ciberseguridad en estos sistemas, los tipos generales de vulnerabilidades, cómo se pueden explotar y qué impacto tienen en las instalaciones industriales, la seguridad operativa y su importancia, y de qué forma es posible mitigar el impacto de este tipo de adversidades.

Abstract

Internet access causes an increase in the productivity of nations, income and employment, as well as being a motivator for growth. However, these opportunities carry on certain risks because digital technologies aren’t yet mature enough, causing crime to take advantage of risks. The cybersecurity applied to the industrial control systems has been taking more importance in the last years, to the point that some sectors of the industry where this type of systems are used are being cataloged critical infrastructures. The cybersecurity strategies that are being developed in some countries define objectives that address issues of protecting society against cyber threats and promoting economic and social prosperity in a context where the main activities are based in the use of information and communication technologies.

This final work consists in the investigation of cybersecurity applied to industrial control systems, through a study of cyber security in industrial plants that have SCADA systems. It will also analyze how to exploit these systems and how to mitigate and prevent their vulnerabilities. The research will cover aspects such as the purpose of industrial control systems and why cybersecurity is important in these systems, the general types of vulnerabilities, how can be exploited and what impact they have on industrial facilities, operational safety and its importance, how it is possible to mitigate the impact of this type of adversity and the legal and commercial actions that are being carried out.

Tabla de Contenido

Introducción

Contexto y justificación

El control de procesos ha venido evolucionando y actualmente es indispensable para controlar los procesos industriales en diferentes sectores, por ejemplo, en las plantas de energía, en las refinerías de petróleo y gas, y en otros procesos, por ejemplo, el aeroespacial, el control de tráfico aéreo, ferroviario, terrestre, el control de producción automotriz, en las plantas químicas, entre otros. El control de procesos siempre ha sido un área de ingenieros de operación y de otros sistemas empresariales, donde cada vez se adquieren mayores niveles de tecnologías de la información y de la comunicación.

En la medida que avanza el tiempo se observa una mayor integración entre los dominios de las tecnologías de la operación (TO) y de la información y comunicación (TIC), debido al uso creciente de las tecnologías, la demanda de nuevos servicios y el acceso a la información en línea, lo que requiere de mayor interconectividad entre todos los sistemas de los mundos TO y TIC. En ese sentido, los sistemas de control de procesos en las TO han venido heredando los riesgos y las vulnerabilidades del mundo TIC, los cuales son conocidos y llevan un recorrido considerable en investigación, análisis y desarrollo, pero que, a diferencia del mundo en las TO en los sistemas de control de procesos el impacto por la materialización de riesgos podría ser catastrófico para la sociedad.

En el Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas, elaborado por la Organización de Estados Americanos OEA en conjunto con la firma de seguridad informática Trend Micro, se destaca lo siguiente:

- Las tendencias del año 2014 destacan el uso de malware para comprometer los sistemas de control de supervisión y de adquisición de datos (SCADA) y otros dispositivos conectados. Esta tendencia se manifestó de dos maneras: malware que se hace pasar por aplicaciones SCADA válidas, y malware que se utiliza para analizar e identificar protocolos SCADA específicos.
- Un reporte del Equipo de Respuesta a Emergencias Cibernética de los Sistemas de Control Industrial (ICS-CERT) de Estados Unidos señala que los sistemas de control industrial fueron blanco de los ataques cibernéticos por lo menos 245 veces en un periodo de 12 meses, de octubre de 2013 a septiembre de 2014. Cerca de 32% de las industrias fueron del sector energético. El ICS-CERT reveló que 55% de los incidentes investigados mostraron señales de que se habían utilizado amenazas persistentes avanzadas para violar los sistemas.
- La mayoría de las regiones en las que se aplicó la encuesta indicaron que su equipo de SCI/SCADA estaba siendo atacado, lo que revela una gran cantidad de actividad por parte de los creadores de amenazas. Si bien muchos de estos ataques podrían ser para reunir inteligencia sobre sus objetivos, se puede prever que más regiones reportarán esto en el futuro conforme sus infraestructuras críticas se vuelvan más conectadas o mejoren su capacidad de identificar la presencia de un ataque.

- Los tipos de ataques cibernéticos más utilizados: Phishing (71%), Vulnerabilidades sin parches (50%), Denegación del servicio (42%), Inyección de SQL (32%), Cross-site scripting (21%), Ataques originados por hacktivistas (21%), Amenazas persistentes avanzadas (18%).
- Actualmente el Phishing es la primera amenaza que se utiliza en los ataques dirigidos y podría ser un indicador del estado real de las actividades relacionadas con los ataques dirigidos. Esto también indicaría que los intentos iniciales de los atacantes es penetrar en una organización para tratar de moverse lateralmente a otros sistemas, como a los elementos de los sistemas SCADA.
- Respecto al nivel de administración que supervisa la ciberseguridad organizacional, en general, los departamentos de TI se encargan de supervisar la ciberseguridad con un 47%, respecto a los departamentos de seguridad de la información con un 27%.

Objetivos

Explicar el propósito de los SCI, investigar la importancia de la ciberseguridad aplicada en estos sistemas, establecer relaciones entre los mundos de las Tecnologías de la Información y la Comunicación TIC y de las Tecnologías de la Operación TO, analizar la situación actual y el estado del arte, investigar los tipos generales de vulnerabilidades, cómo se pueden explotar y el impacto que tienen en las instalaciones industriales, explicar la seguridad operativa y su importancia en los SCI, proponer recomendaciones y explicar cómo es posible mitigar el impacto de este tipo de adversidades.

Utilizar a manera de ejemplo un caso que resulte de interés y explicar desde el punto de vista de la seguridad operacional lo que ocurrió mal, las vulnerabilidades de los sistemas y las acciones del atacante.

Metodología

La metodología a seguir durante el desarrollo del TFM no varía respecto a las actividades planteadas por la dirección del proyecto. La modalidad del trabajo será de tipo investigativo / descriptivo, con lo cual, la primera actividad consiste en recopilar toda la información necesaria y una vez se esté documentado al respecto, se procederá con el desarrollo de las tareas a realizar para alcanzar los objetivos. Considerando los avances que se obtengan durante el desarrollo del trabajo, es posible realizar entregas parciales para revisar los avances, obtener retroalimentación por parte de los directores del proyecto y resolución de inquietudes. Una vez culminados los anteriores, se desarrollará la memoria final, se entregará y preparará el video de presentación del TFM y la defensa.

Planificación

El esquema de trabajo para el desarrollo del trabajo final de máster, se dividirá en las siguientes actividades:

- Definiciones. Significado y dimensiones de seguridad de la información, concepto de ciberseguridad.

- Propósito de los sistemas de control industrial y la importancia de la ciberseguridad en estos sistemas.
- Infraestructuras críticas.
- Tecnologías de la Información y Tecnologías de la Operación. Normas, estándares y buenas prácticas.
- Tipos generales de vulnerabilidades, cómo se pueden explotar y que impacto tienen en las instalaciones industriales.
- Explicar la seguridad operativa y qué importancia tiene en los sistemas de control industrial.
- Explicar cómo es posible mitigar el impacto de este tipo de adversidades en los Sistemas de Control Industrial.
- Utilizar un ataque como ejemplo, describir las acciones del atacante y explicar lo que ocurrió mal desde el punto de vista de la seguridad operacional y las vulnerabilidades de los sistemas.
- Preparación de entregables y memoria final.
- Preparación de video presentación del proyecto.

¿Qué son los Sistemas de Control Industrial?

Los Sistemas de Control Industrial (SCI), tienen una historia bastante amplia. Hoy día es muy común encontrarse con literatura, discusiones y diversa información acerca de los controles industriales y su inherente relación con la ciberseguridad; sin embargo, es un fenómeno relativamente reciente.

La Sociedad Internacional de Automatización (ISA), a través del comité para desarrollo de estándares ISA99, reúne a expertos en ciberseguridad industrial para desarrollar estándares de automatización industrial y seguridad de los sistemas de control. Los estándares ISA99, además de ser utilizados por la Comisión Electrotécnica Internacional (IEC) para la producción de los estándares IEC 62443, definen que los SCI son una colección de personal, hardware y software que pueden afectar o influir en la operación segura, la seguridad y la confiabilidad de los procesos industriales. El estándar ISA-62443-3-3, define que los SCI son una colección de personal, hardware, software y políticas involucradas en la operación del proceso industrial y que pueden afectar o influenciar su operación segura y confiable.

El Instituto Nacional de Estándares y Tecnología (NIST) del departamento de Comercio del gobierno norteamericano, establece que un SCI es un término general que abarca varios tipos de sistemas de control, incluidos sistemas de supervisión y adquisición de datos (SCADA), sistemas de control distribuido y otras configuraciones de sistemas de control como controladores lógicos programables (PLC) que a menudo se encuentran en los sectores industriales y en las infraestructuras críticas. Un SCI consiste en combinaciones de componentes de control (p.ej., eléctricos, mecánicos, hidráulicos, neumáticos) que actúan conjuntamente para lograr un objetivo industrial (p.ej., fabricación, transporte de materia o energía).

Propósito

Responder la pregunta acerca del propósito de un Sistema de Control Industrial se podría abordar desde distintas ópticas, por ejemplo, desde un punto de vista económico, un SCI tiene como propósito maximizar la rentabilidad de una planta, mediante la combinación de equipos de control, mano de obra, ingeniería, procesos, materiales, entre otros; por lo tanto, en ese sentido, un SCI tiene como propósito maximizar la producción, optimizar el rendimiento y mejorar la efectividad de una planta industrial, facilitando que la operación sea en óptimas condiciones y minimizando los costos.

Desde el punto de vista de la teoría de control, los SCI tienen cuatro grandes funciones:

- Medir: obtener valores de los sensores y leerlos como entrada para procesarlos o proporcionarlos como salida.
- Comparar: evaluar el valor medido para procesar valores de diseño
- Computar: calcular el error actual, el error histórico y el error futuro
- Corregir: acciones iniciadas por el operador o ajustes automáticos del proceso

Estas cuatro grandes funciones se realizan mediante cinco elementos clave:

- Sensores: dispositivos capaces de medir varias propiedades físicas
- Transductores: convierten la señal no eléctrica en un valor eléctrico
- Transmisores: dispositivos que convierten las medidas de un sensor y envían la señal
- Controladores: proporcionan la lógica y las entradas/salidas (I/O) para el proceso
- Elementos de control final: actuadores que físicamente cambian un proceso

Los SCI comenzaron dando a los humanos una forma de aplicar acciones en el tiempo (reemplazo de las acciones manuales ejecutadas por los operadores) y han venido evolucionado a través de la investigación, la innovación y la tecnología para poder detectar y actuar en ciclos de tiempo mucho más pequeños (milisegundos).

Componentes

Los componentes más comunes en un Sistema de Control Industrial, así como la relación entre estos componentes son los elementos que se describen a continuación:

Instrumentos de campo

Los instrumentos de campo son los encargados de guiar el proceso, y se pueden diferenciar entre los que ingresan datos para el siguiente nivel (por ejemplo, un sensor que detecta si una válvula se encuentra en cierto nivel de presión) y los instrumentos de campo que reciben datos y actúan (por ejemplo, un motor que opera una compuerta que permite la expulsión de gases).

Controladores Lógicos Programables (PLC)

Los controladores lógicos programables son dispositivos de estado basados en computadoras que controlan los equipos y procesos industriales. Estos dispositivos se encargan de controlar los instrumentos de campo, mediante un software, que contiene una lógica de programación para un propósito específico. Los PLC están en capacidad de interpretar los datos de los instrumentos de campo y también pueden actuar sobre ellos. Por ejemplo, si un instrumento de campo detecta que una válvula ha alcanzado cierto nivel de presión por una determinada acumulación de gases, el PLC puede procesar y entender esa información, y luego comunicarla a otros instrumentos de campo para emitir alertas, abrir o cerrar compuertas para liberar presión, entre otros.

Unidad de Terminal Remota (RTU)

Una unidad de terminal remota es un sistema de control autónomo para procesos lógicos simples. Estos dispositivos son un tipo de PLC, pero más robusto y están diseñados para comunicarse con la sala de control (a través de redes de comunicación Ethernet, Wi-Fi, redes celulares 2G, 3G, GPRS, radio enlaces, etc.) en donde está el operador observando a través de una HMI.

Interface Hombre Máquina (HMI)

La interface hombre máquina tiene como funcionalidad la interacción entre una persona y un PLC/RTU. Así como los PLC/RTU, un HMI se compone de software y hardware que permite a los operadores monitorear el estado de un proceso y actuar sobre ello modificando la configuración

o anulando manualmente las operaciones de control automático en caso de una emergencia. Los sistemas HMI están en capacidad de mostrar información, como también de mostrar y procesar información del operador. Los sistemas HMI más recientes, dependiendo de su configuración, pueden ser accesibles remotamente a través de redes LAN, WAN, Internet, entre otros.

Todos los componentes descritos con anterioridad pueden estar, o no, conectados entre sí. Uno o múltiples sensores pueden estar conectados a un PLC y a su vez, se pueden conectar varios PLC con una RTU. Una RTU se puede conectar a varios sistemas HMI, sin embargo, un sistema HMI también se puede conectar directamente a un PLC.

Importancia de la ciberseguridad en los SCI

La creciente interconectividad y la dependencia de las plataformas y servicios basados en Internet han aumentado considerablemente la exposición al riesgo de los gobiernos, las empresas y los ciudadanos, a toda una gran variedad de actos relacionados con la delincuencia, el espionaje y la seguridad cibernética. De acuerdo con un estudio de la Organización de Estados Americanos OEA, los datos disponibles indican que los incidentes y los ataques cibernéticos, en particular aquellos que se realizan con intenciones criminales, están aumentando en frecuencia y en los niveles de sofisticación. Los gobiernos y las empresas reconocen la necesidad de tener políticas y estrategias nacionales de seguridad cibernética, cultura cibernética, educación, formación y competencias en seguridad, marcos jurídicos, reglamentarios y normatividad, así como también contar con cooperación e intercambio de información.

Los incidentes que han ocurrido en los últimos años han ocasionado que las organizaciones sean más conscientes de la importancia de la ciberseguridad en los SCI. El número de incidentes que han sido reportados al Equipo de Respuesta ante Emergencias Informáticas (CERT), ha aumentado tanto en los últimos años que, a partir del año 2003, el CERT dejó de contar los incidentes ya que los números ascendían a cifras considerables, tanto así que durante el año 2003 se alcanzaron a reportar más de ciento veinte mil incidentes. No solo aumentó el número de ataques, sino que también sus niveles de sofisticación.

Entre las tendencias se destaca el uso de malware para comprometer los sistemas de control de supervisión y adquisición de datos SCADA. El año 2010 marcó un hito en la historia de los ataques cibernéticos, el malware más sofisticado nunca antes reportado, apuntaba a la infraestructura de energía atómica de Irán, según informes de fuentes periodísticas y firmas expertas en seguridad cibernética. El malware conocido con el nombre de “Stuxnet”, tomó el control de máquinas que participaban en la producción de material nuclear y les dio instrucciones para autodestruirse. Fue la primera vez en la historia que se registraba un evento de tal magnitud, espiaba y reprogramaba sistemas industriales SCADA para control y monitorización de procesos.

En el año 2014 ocurrieron dos ataques importantes, uno de ellos en Estados Unidos y el otro en Alemania. De acuerdo con el *New York Times*, la firma de seguridad *CrowdStrike* reportó que el ataque en Estados Unidos fue dirigido a empresas del sector energético, a través de un malware conocido con el nombre de “Havex”, diseñado para penetrar en los sistemas de control industrial SCADA. Una vez que los sistemas estuvieron infectados, el malware envió datos e información

sensible a los delincuentes mediante servidores de comando y control. El ataque reportado en Alemania fue dirigido a una planta de acero. De acuerdo con *BBC News*, la Oficina Federal para la Seguridad de la Información de Alemania BSI reportó que los atacantes comprometieron la red de la planta siderúrgica mediante el envío de correos electrónicos que contenían phishing, lo que provocó que el malware penetrara en los sistemas que controlaban el equipo de la planta SCADA dentro de la red de producción provocando daños físicos.

En el año 2015, la red eléctrica de Ucrania sufrió un ataque cibernético provocando el corte de suministro durante varias horas. El ataque afectó a más de seiscientos mil hogares de la región que era alimentada por la planta eléctrica. El ataque se realizó a través del malware conocido con el nombre de "BlackEnergy". Según la firma experta en seguridad "ESET", la infección se realizó a través de archivos de Microsoft Office con macros maliciosas, enviados a través de correos electrónicos que suplantaban a destinatarios reales. En la incidencia se comprobó que el malware "BlackEnergy" instaló un componente identificado con el nombre "KillDisk" el cual se encargaba de borrar archivos importantes del sistema para impedir su arranque (*Master Boot Record*), así como también funciones específicas para atacar sistemas industriales SCADA. Fue la primera vez en la historia que un ataque cibernético fue capaz de provocar un corte de suministro eléctrico.

Los incidentes que han ocurrido en los últimos años han ocasionado que tanto los gobiernos, como las instituciones y organizaciones sean más conscientes de la necesidad de adoptar medidas para controlar los riesgos en ciberseguridad. En la medida que la industria se viene desarrollando e incrementando sus niveles de transformación, la ciberseguridad ha tomado mayor importancia.

Si nos fijamos en la industria energética, se puede observar que las redes eléctricas, desde la generación y la transmisión hasta la distribución y la comercialización están experimentando altos niveles de transformación en sus arquitecturas y una mayor convergencia entre las tecnologías de la operación TO y las tecnologías de información y la comunicación TIC. En las redes futuras, aparecerán cientos o miles de millones de dispositivos de energía distribuidos, paneles solares, nuevos medidores inteligentes para medición avanzada, nuevos generadores de energía, otros medios de transporte eléctrico, ciudades y edificios inteligentes, nuevos tipos de almacenamiento de energía, así como otros sistemas electrónicos de diversas magnitudes. Todos estos elementos adquirirán nuevas capacidades y soportarán nuevos servicios, lo que llevará a las redes y medios de comunicación a brindar acceso e interconectividad en lugares donde antes no había el acceso, porque no existía o simplemente porque no se concebía. Aparecerán nuevas formas de generar y consumir energía, y se utilizará de forma más flexible y en ese mismo sentido aparecerán nuevas vulnerabilidades y riesgos cibernéticos.

Vulnerabilidades en los Sistemas de Control Industrial

En las décadas anteriores al año 2000, los entornos de producción industrial eran relativamente más pequeños que los SCI actuales y eran responsables de una pequeña parte de las cadenas de producción, las comunicaciones dentro de las zonas de producción eran aisladas y se usaban para el intercambio de datos simple, por ejemplo, entre las mismas HMI's, RTU's y PLC's. Por lo tanto, la comunicación entre la zona de producción y las redes corporativas no era posible. Para la comunicación entre las zonas de operación TO, los protocolos que típicamente se utilizaban eran propietarios y las comunicaciones entre sistemas TO y TIC era muy difícil de encontrar (porque los protocolos de TO eran patentados y no compatibles con los de TIC. Algunos ejemplos de estos protocolos: Modbus, DNP3, Profibus, entre otros). La comunicación en las zonas de operación estaba centrada en la transmisión de datos en tiempo real, lo que significa que la baja latencia del sistema de entrada y salida eran cruciales. La mayoría de los componentes del sistema eran hardware y firmware propietarios y en la capa de red la mayoría de los dispositivos usaban enlaces en serie para la comunicación punto a punto.

En la medida que las capacidades de computación aumentaron y la globalización del internet fue creciendo, otras necesidades fueron apareciendo como la de interconectar las redes de operación y de TIC para proporcionar nuevos servicios a los usuarios. Esto fue creando otras necesidades, como la de estandarizar los protocolos de comunicación y el hardware utilizado. La comunicación entre redes comenzó a estandarizarse con el uso de TCP/IP. Los componentes de hardware también tuvieron procesos de estandarización hacia arquitecturas basadas en Windows. La interconexión entre las zonas de operación y las redes corporativas fue posible, por ejemplo, los accesos a las HMI a través de las redes corporativas para controlarlas de manera remota. Así mismo, también fueron apareciendo nuevos riesgos.

Según las cifras publicadas por algunos equipos de atención y respuesta de incidentes (CERT), la información sobre vulnerabilidades en los sistemas de control industrial SCI se remonta desde finales de los años 90. Desde ese entonces el número de vulnerabilidades reveladas año tras año muestran un aumento considerable en la aparición de vulnerabilidades. En los últimos siete años, el índice ha aumentado de 19 reportadas en el año 2010, a 187 en el 2016.

De acuerdo con la guía para seguridad en sistemas de control industrial desarrollada por NIST (SP800-82), las vulnerabilidades típicamente presentes en los SCI pueden agruparse según en dónde existan, por ejemplo: en la política y los procedimientos de cada organización, o en la insuficiencia de los mecanismos de seguridad implementados en cada uno de los componentes del SCI (hardware, firmware y software). De acuerdo con esta definición, los principales grupos de vulnerabilidades son:

- Políticas y procedimientos
- Diseño y arquitectura
- Configuración y mantenimiento
- Físicos

- Desarrollo de software
- Redes y comunicaciones

Grupos y tipos generales de vulnerabilidades

Si bien es cierto que cada SCI tiene sus particularidades, por lo general tiene un subconjunto de los grupos identificados con anterioridad, pero también puede contener otras vulnerabilidades adicionales y condiciones únicas para cada SCI. Algunas vulnerabilidades y condiciones podrán ser mitigadas, otras solo podrán ser aceptadas y controladas mediante contramedidas, pero lo cierto es que siempre darán lugar a algún riesgo residual.

Políticas y procedimientos. A menudo las vulnerabilidades se introducen en los SCI debido a políticas incompletas, inapropiadas o inexistentes, así como a la ausencia de guías de implementación y aplicación. Una adecuada política y procedimientos de seguridad son la piedra angular de cualquier programa de seguridad. Así, la política de seguridad ayuda a la reducción de vulnerabilidades mediante la definición de lineamientos y cumplimiento de conductas adecuadas. Tanto la política como los procedimientos son mecanismos para informar al personal y las partes interesadas, sobre las decisiones en los comportamientos que se deben adoptar. Así, la política y procedimientos son una forma educativa de reducir las vulnerabilidades. Algunos tipos generales de vulnerabilidades son:

- Ausencia o inadecuada política de seguridad para el SCI.
- Ausencia de un programa de concientización y entrenamiento en seguridad.
- Falta de mecanismos administrativos para la aplicación de la política.
- Inadecuada revisión de la efectividad de los controles de seguridad del SCI.
- Ausencia de un plan de contingencia para el SCI.
- Ausencia o inadecuados procedimientos (gestión de configuración, control de acceso, autenticación, atención y respuesta de incidentes, entre otros.).

Vulnerabilidades del sistema. Los controles de seguridad deben identificar claramente los sistemas a los que se aplican. Los sistemas varían ampliamente en tamaño, alcance y capacidad y las vulnerabilidades de cada sistema pueden ocurrir en sus componentes. Las fuentes de vulnerabilidades pueden incluir fallas en el diseño, en el desarrollo, en las configuraciones incorrectas, en el mantenimiento deficiente, administración deficiente y en las conexiones con otros sistemas y redes. Típicamente las vulnerabilidades potenciales que se encuentran dentro de los SCI están categorizadas de la siguiente manera:

- **Diseño y arquitectura**. Principales vulnerabilidades:
    - Incorporación inadecuada de seguridad a la arquitectura y el diseño: Al incorporar seguridad en la arquitectura del SCI, el diseño debe incluir el presupuesto y el cronograma. Las arquitecturas deben abordar la identificación y autorización de los usuarios, los mecanismos de control de acceso, las topologías de red y los mecanismos de configuración e integridad del sistema.

- Evolución de la arquitectura: El entorno de la infraestructura de red dentro del SCI a menudo es desarrollado y actualizado en función de los requisitos comerciales y operativos, sin considerar los posibles impactos de seguridad de los cambios. Con el tiempo, las brechas de seguridad pueden ser inadvertidas, las cuales pueden representar puertas traseras en los SCI.
- Perímetro de seguridad: Sin un perímetro de seguridad definido en el SCI, no es posible garantizar que los controles de seguridad se implementen y configuren correctamente, lo que puede conducir al acceso no autorizado y otros problemas.
- Redes de control utilizadas en tráfico que no es control: El tráfico de control y de no control tiene diferentes requisitos, tal como la confiabilidad, por lo que tener ambos tipos de tráfico en una sola red dificulta la correcta configuración de la red para cumplir con los requisitos del tráfico de control. El tráfico que no es de control podría consumir recursos que afectan las necesidades de tráfico de control, lo que causaría interrupciones en las funciones del SCI.
- Servicios de la red de control que están fuera de la red de control: Cuando las redes de control utilizan servicios TIC (p.ej. DNS, DHCP) que a menudo se implementan en redes TIC, ocasiona que la red del SCI dependa de la red TIC que puede no tener los requisitos de confiabilidad y disponibilidad necesarios para el SCI.
- Recolección de eventos de datos históricos inadecuada: Sin una recopilación de datos adecuada y precisa, sería casi imposible determinar qué causó un incidente de seguridad. Los incidentes pueden pasar desapercibidos y provocar daños y/o interrupciones adicionales. Se necesita una supervisión de seguridad que permita identificar problemas con los controles de seguridad.

- **Configuración y mantenimiento**. Principales vulnerabilidades:
  - Hardware, firmware y software sin una gestión de configuración: La organización no sabe qué tiene, qué versiones tiene, dónde están o cuál es el estado de sus parches, lo que da como resultado una postura de defensa incoherente e ineficaz. Se debe implementar un proceso para controlar las modificaciones al hardware, firmware, software y documentación para garantizar que el SCI está protegido contra modificaciones no autorizadas antes, durante y después que el sistema sea implementado. La falta de estos procedimientos puede conducir a exposiciones y riesgos de seguridad.
  - Parches de seguridad aún sin desarrollar o sin aplicar: Debido al acoplamiento entre el software de los SCI, los cambios deben someterse a pruebas de regresión integrales y que requieren mucho tiempo. El tiempo para las pruebas y posterior distribución de actualizaciones proporciona largas ventanas de vulnerabilidad. Los sistemas operativos y aplicaciones desactualizados pueden tener vulnerabilidades que podrían explotarse. El soporte de parches de seguridad puede que ni siquiera esté disponible para el SCI debido que se usan sistemas operativos obsoletos.
  - Pruebas inadecuadas de cambios de seguridad: Las modificaciones en el hardware, firmware y software sin pruebas de seguridad, pueden comprometer el normal

funcionamiento del SCI. Los sistemas operativos de producción nunca se deben usar para pruebas. Las pruebas den coordinarse con proveedores e integradores.

- Controles de acceso remoto deficientes: Las capacidades de acceso remoto al SCI deben controlarse adecuadamente para evitar accesos no autorizados.
- Configuraciones inadecuadas: Los sistemas configurados incorrectamente pueden dejar puertos y protocolos innecesarios abiertos, estas funciones innecesarias pueden contener vulnerabilidades que aumentan el riesgo general para el sistema. Las configuraciones por defecto exponen vulnerabilidades y servicios explotables.
- Datos desprotegidos en dispositivos portables: Si los datos confidenciales (p.ej., contraseñas) son almacenados en medios portables sin cifrado y estos se pierden, la seguridad del sistema podría comprometerse.
- Uso y protección de contraseñas no cumplen con la política: Se deben seguir las políticas y procedimientos de contraseñas. Las violaciones de la política y procedimientos de contraseñas pueden aumentar las vulnerabilidades de los SCI.
- Controles de acceso inadecuados: Los controles de acceso deben coincidir con la forma en que la organización asigna responsabilidades y privilegios al personal. Los controles de acceso mal especificados dan como resultado que los usuarios del SCI tengan demasiados o pocos privilegios.
- Desactualización o falta de protección contra malware: La instalación de software malicioso o malware es un tipo de ataque común. El software de protección contra malware, p.ej., software antivirus, debe estar instalado y mantenerse actualizado. El software de protección de malware desactualizado deja al sistema abierto a nuevas amenazas de malware.
- Denegación de servicio (DoS): El software de los SCI podría ser vulnerable a este tipo de ataques, lo que impediría el acceso autorizado a un recurso del sistema o retrasaría las operaciones normales y las funciones del sistema.
- Ausencia de software para detección/prevención de intrusiones: Los incidentes pueden provocar la pérdida de disponibilidad e integridad del sistema; la captura, modificación y eliminación de datos. El software para detección/prevención de intrusos (IDS/IPS) puede detectar o prevenir varios tipos de ataques (p.ej., DoS, inyección de código, etc.) y también identificar los equipos atacados y las fuentes de ataque.

- **Físicos**. Principales vulnerabilidades:
  - Personal no autorizado con acceso físico a los equipos: El acceso físico a los equipos de los SCI debe ser restringido solo al personal necesario, teniendo en cuenta los requisitos de seguridad, entre ellos el apagado de emergencia o reinicios. El acceso no autorizado a los equipos del SCI puede conducir a cualquiera de los siguientes:
    - Hurto físico de datos y hardware
    - Daño físico o destrucción de datos y hardware

        - Cambios no autorizados en el entorno operativo
        - Desconexión de enlaces de datos físicos
        - Interceptación indetectable de datos
    - Falta de energía de respaldo: Sin energía de respaldo para los activos críticos, una pérdida general de energía dejaría por fuera al SCI y podría crear una situación insegura. La pérdida de energización también podría ocasionar configuraciones inseguras.
    - Ausencia de control ambiental: La pérdida de control ambiental (temperaturas, humedad) podría ocasionar daños al equipo, tales como sobrecalentamiento de los procesadores.
    - Puertos físicos no asegurados: Los puertos no asegurados podrían permitir la conexión no autorizada de medios extraíbles (p.ej., USB, registradores de teclado, etc.).
- **Desarrollo de software**. Principales vulnerabilidades:
    - Validación incorrecta de datos: El software del SCI puede no validar correctamente las entradas del usuario o los datos recibidos para garantizar su validez. Los datos no válidos pueden dar lugar a vulnerabilidades, incluidas el desbordamiento de búfer, la inyección de código, entre otros.
    - Autenticación, privilegios y control de acceso inadecuados: El acceso no autorizado al software de configuración podría ocasionar la capacidad de dañar un dispositivo o de modificarlo inadvertidamente.
- **Redes y comunicaciones**. Principales vulnerabilidades:
    - Controles de flujo de datos no empleados: Los controles de flujo de datos son necesarios para restringir qué información está permitida entre los sistemas. Estos controles pueden evitar la filtración de información y operaciones ilegales.
    - Ausencia de cortafuegos o fallos de configuración: La falta de firewalls o fallos en la configuración podría permitir el paso de datos innecesarios entre las redes, lo que ocasiona que los ataques y el malware se propaguen.
    - Protocolos de comunicación sin cifrado: Los atacantes que pueden monitorear la actividad de la red del SCI pueden usar un analizador de protocolos para leer los datos transferidos por protocolos inseguros, tales como telnet, FTP, HTTP, NFS, entre otros. El uso de estos protocolos facilita que los atacantes realicen ataques contra el SCI y manipulen la actividad de la red.
    - Autenticación de usuarios, datos o dispositivos deficiente o inexistente: Muchos protocolos de los SCI no tienen autenticación en ningún nivel. Sin autenticación, existe la posibilidad de reproducir, modificar o falsificar datos o dispositivos como sensores e identidades de usuario.

- Protocolos de los SCI inseguros: Estos protocolos a menudo tienen pocas o ninguna capacidad de seguridad, como la autenticación y el cifrado, para proteger los datos contra el acceso no autorizado o la manipulación. La implementación incorrecta de los protocolos puede generar vulnerabilidades adicionales.
- Falta de verificación de integridad en las comunicaciones: No hay controles de integridad en la mayoría de los protocolos de control industrial. Los atacantes podrían manipular las comunicaciones sin ser detectados.
- Incorrecta autenticación entre clientes inalámbricos y puntos de acceso: Sin una correcta autenticación entre los clientes inalámbricos y los puntos de acceso no se puede garantizar que los clientes se conecten a puntos de acceso válidos, lo que ocasiona suplantación y revelación de información confidencial.
- Incorrecta protección de datos entre clientes inalámbricos y puntos de acceso: Los datos confidenciales entre los clientes inalámbricos y los puntos de acceso deben protegerse mediante cifrado para garantizar que los atacantes no puedan obtener acceso no autorizado a los datos transmitidos.

¿Cómo se pueden explotar?

Según índices reportados para los años 2015/2016, los principales tipos de vulnerabilidades fueron:

- **Desbordamiento de buffer**: Son ocasionadas por errores de programación, donde el software, al escribir datos en un búfer sobrepasa el límite y sobrescribe las ubicaciones de memoria. Esto ocasiona posibles daños en los datos, el bloqueo del programa o causar la ejecución de código malicioso. Estos defectos de seguridad se descubrieron en diferentes componentes, incluidos los sistemas SCADA, HMI y otros. Algunas de las vulnerabilidades de este tipo tienen la puntuación más alta en el CVSS (Sistema Común de Calificación de Vulnerabilidades), que corresponde al impacto máximo (acceso con nivel de privilegios altos), lo cual podría ser realizado por un atacante remoto no autenticado.
- **Transmisión de información sensible en texto claro**. Estas vulnerabilidades permiten a un atacante detectar datos confidenciales en un canal de comunicación porque los datos son transmitidos en texto claro.
- **Ejecución de código remoto**. Son vulnerabilidades que permiten la ejecución remota de código arbitrario en un sistema de destino.
- **Denegación de servicio**. Este tipo de ataque se lleva a cabo, típicamente, remotamente. En caso de un ataque exitoso, el software o hardware atacado deja de responder a las solicitudes legítimas dejando por fuera el servicio y/o la funcionalidad proveída.
- **Inyección de código**. Son vulnerabilidades que permiten realizar inyecciones de código, tales como SQL, XML, entre otros. Las vulnerabilidades de este tipo al ser explotadas permiten extraer/leer datos en sistemas de destino sin autorización.
- **Manipulación de archivos**. Estas vulnerabilidades permiten realizar diferentes tipos de operaciones sobre los archivos que son objeto del ataque (crear, eliminar, mover, cambiar propiedades) de forma remota.

- **Manipulación de cuentas de usuario**. Estas vulnerabilidades permiten atacar los datos de los usuarios legítimos (crear un nuevo usuario, eliminar o bloquear un usuario existente o cambiar sus propiedades y permisos).

Impacto en las instalaciones industriales

La explotación de una vulnerabilidad en los SCI podría tener diversas consecuencias, ya que a diferencia de los ataques informáticos convencionales que producen daños "no físicos", los ataques dirigidos a los SCI pueden afectar no sólo a los datos corporativos, sino también producir daños "físicos" significativos. Algunos ejemplos de impacto son los de seguridad física y el entorno, los de tipo sociales, los económicos, entre otros.

- Impactos en la seguridad física y el entorno: Son los impactos más críticos, ya que pueden suponer pérdidas y lesiones humanas, daños físicos y al medio ambiente.
- Impactos sociales: Afectan la imagen corporativa y la pérdida de confianza. Puede conllevar a la pérdida de clientes, de la competitividad y afectan la estabilidad.
- Impactos económicos: Por lo general estos son consecuencia de alguno de los anteriores, ya que, al haber daños físicos o del entorno, o al haber impactos sociales, ocurren pérdidas económicas que afectan el funcionamiento de la organización.

Una vez vistos algunos de los impactos ocasionados por un incidente, un ataque bien organizado podría darnos una idea de que la lista de posibles consecuencias crecería de manera exponencial. En un breve recorrido por los principales incidentes revelados en SCI, encontramos los siguientes:

- Año 2003: La central nuclear de Davis-Besse en Estados Unidos, fue infectada con un gusano conocido como "Slammer", afectando a varios SCI que causaron problemas en el sistema de monitorización de seguridad y lo dejaron bloqueado durante algunas horas.
- Año 2010: El malware conocido como "Stuxnet" se detectó en una central nuclear de Irán. El ataque ocasionó daños físicos y retrasó el programa iraní de enriquecimiento de uranio por al menos dos años.
- Año 2014: El malware conocido con el nombre de "Havex", penetró los SCI de empresas del sector energético en Estados Unidos. El malware envió datos e información sensible a los atacantes mediante servidores de comando y control.
- Año 2014: La red de una planta siderúrgica en Alemania fue comprometida luego que un ataque de phishing provocara que el malware penetrara en los SCI dentro de la red de producción, lo que ocasionó daños físicos.
- Año 2015: La red eléctrica de Ucrania sufrió un ataque que ocasionó el corte de suministro eléctrico durante varias horas. El malware conocido como "BlackEnergy" fue incrustado en macros dentro de archivos de Microsoft Office.

Basado en información suministrada por la firma de seguridad F-Secure Labs y de acuerdo con el análisis realizado por el Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de SCI (ICS-CERT), para el caso relacionado con el malware "Havex" que afectó el sector energético de EEUU

en el 2014, se pueden identificar algunos impactos ocasionados por el ataque en las instalaciones industriales. A continuación, algunos de los principales elementos del ataque:

- El principal componente del malware “Havex” es un troyano o software malicioso que se presenta al usuario como un programa aparentemente legítimo, pero que, al ejecutarlo, le brinda al atacante acceso remoto al equipo infectado.
- El atacante implantó el malware en el software de algunos fabricantes de SCI/SCADA, directamente en los repositorios en donde estaba disponible para descarga; en un intento de infectar las computadoras en donde el software fuera instalado. El atacante también utilizó otros vectores de ataque para distribuir el malware, como fue el correo electrónico.
- Los fabricantes vulnerados estaban relacionados con el desarrollo de aplicaciones y dispositivos para uso en SCI. Dos de ellos proveedores de software de gestión remota para SCI y el tercero desarrollaba cámaras industriales de alta precisión para SCI y el software relacionado.
- El análisis al código fuente del malware demostró que éste analizaba el comportamiento de las redes de los SCI/SCADA. De manera remota también se instruirá a las computadoras infectadas para que descargaran y ejecutaran otros componentes, por ejemplo, uno de ellos enumeraba la red de área local y buscaba recursos y servidores conectados.

Algunos impactos ocasionados:

- Espionaje industrial incluyendo revelación de infraestructuras críticas.
- Afectación de imagen corporativa y pérdida de confianza.
- Impactos económicos. La cuantificación puede ser compleja de realizar, al menos basado en la información revelada al público, sin embargo, no se puede desconocer que si hubo robo de información y afectación de imagen corporativa, en alguna medida existe impacto económico.

Seguridad Operativa y su importancia en los SCI

La seguridad operativa u operacional ha recibido grandes aportes del sector aeronáutico en el cual, durante sus primeros años de operación, la poca reglamentación, vigilancia, infraestructura y comprensión de los peligros, lo mantuvo expuesto a altos riesgos operativos. En la medida que el sector aeronáutico fue creciendo, las mejoras tecnológicas y las exigencias reglamentarias marcaron el camino a seguir, como factor importante para reducir los riegos de lesiones a las personas o daños a bienes, mediante la implementación de un proceso continuo de identificación de amenazas y gestión del riesgo. En la actualidad las buenas prácticas de seguridad operativa son implementadas en otros sectores tales como el de transporte ferroviario, marítimo, vuelos espaciales tripulados, sector eléctrico entre otros.

La Organización de Aviación Civil Internacional (OACI) en su manual de gestión de la seguridad operacional (SMM), el cual está basado en normas y métodos internacionalmente recomendados (SARPS), define la seguridad operacional dentro del contexto de la aviación, como el estado donde la posibilidad de dañar a las personas o las propiedades se reduce y mantiene al mismo nivel o debajo de un nivel aceptable, y dado que no es posible eliminar completamente los riesgos y peligros, se define que la seguridad es una característica dinámica de los sistemas y por lo tanto los riesgos deben ser identificados y mitigados continuamente.

La gestión de la seguridad operacional constituye un camino para disminuir la ocurrencia de los accidentes e incidentes que causan grandes pérdidas en las compañías, así como el incremento de la confiabilidad en los procesos, equipos y el desarrollo de buenas prácticas que potencializan la eficiencia operacional. Para lograr una adecuada gestión, la seguridad operacional se enfoca en los procesos, los sistemas y las personas, entendiendo que, en este último las vulnerabilidades propias de los seres humanos si no son gestionadas apropiadamente incrementan los riesgos.

Dentro de los planes de gestión de la seguridad operacional, los conceptos del factor humano y la conciencia situacional cobran vital relevancia como disciplinas que propenden la adaptación entre las personas y los sistemas en los que trabajan, la comprensión del comportamiento y el desempeño humano, la gestión del error, la fatiga, la respuesta al cambio, el desarrollo del talento en competencias del saber (hacer + ser), consolidando un perfil integral del personal operacional y la adaptación de una cultura orientada a la seguridad, a la vigilancia y el reporte como un proceso estructurado. Igualmente facilitando la percepción, comprensión del entorno y realidad operativa, para proyectar una situación en un futuro inmediato.

En cuanto a los procesos, su integración bajo el marco de la seguridad operacional contempla los atributos de responsabilidad, autoridad, documentación, indicadores, controles e interfaces. Se desarrollan perfiles y funciones a la luz de la seguridad operacional y los factores humanos, definiendo procesos críticos, incorporación de buenas prácticas que contribuyan a la eficiencia operacional y a generar una cultura segura y confiable e implementando esquemas de rendición y control de la seguridad operacional. Las soluciones tecnológicas por su parte, se conciben como herramientas alineadas a las necesidades operativas, que contribuyen a mejorar las capacidades de análisis y conciencia situacional en un entorno que promueve la seguridad operacional.

Para la implementación y/o sostenibilidad de la seguridad operacional, se deben definir factores claves de éxito como el patrocinio organizacional, la gestión del riesgo, procesos y procedimientos y tecnología, definiendo claramente sus objetivos, indicadores y retos, con herramientas óptimas para la medición, seguimiento y monitoreo, con el fin de verificar el cumplimento de la seguridad operacional.

Sin duda, la seguridad operacional es un concepto importante a considerar en los SCI, ya que marca las pautas para garantizar un estado en el que el riesgo se reduce y se mantiene en niveles aceptables. De acuerdo con los estándares ISA99, se reconoce el hecho de que el personal y su interacción con el hardware y el software pueden influir en la operación segura, la seguridad y la confiabilidad de los procesos. Todo esto sumado a la exposición al riesgo introducida por otros factores tales como la interconectividad, la criticidad de los procesos bajo el control de los SCI, el intercambio de información, las vulnerabilidades de los sistemas, entre otros, el concepto de seguridad operacional se vuelve una necesidad en las organizaciones y es adoptada de manera general como una cultura de prevención, vigilancia y reporte.

Es por ello que, unas de las principales causas de los eventos e incidentes que típicamente ocurren en los procesos que están bajo control industrial y en general en cualquier proceso, sean la violación o la carencia de procedimientos, los errores humanos y la falta de entrenamiento al personal, la ausencia de protocolos claros de comunicación.

¿Cómo mitigar el impacto de este tipo de adversidades en los SCI?

Los marcos de trabajo (*frameworks*), los estándares y las normas de seguridad han sido un tema de interés general que, durante las últimas décadas, gobiernos, instituciones e industria en general les han estado invirtiendo esfuerzos en investigación, desarrollo y constante evolución. En la medida que los gobiernos e instituciones son conscientes de los riesgos a los que se exponen las infraestructuras que tienen relación con los Sistemas de Control Industrial, la adopción de *frameworks* y estándares de seguridad sufre un proceso de transformación, pasando de ser una buena práctica a una exigencia de cumplimiento, normalmente definida por los gobiernos en el marco legislativo y regulatorio. En ese sentido, para mitigar el impacto de las adversidades en los SCI, el camino a seguir incluye la adopción de *frameworks* y estándares que mejor se adapten a las necesidades de cada organización.

Los *frameworks* tienen como objetivo mitigar las amenazas que actualmente se planteen para cada SCI, así como el cubrimiento de las medidas de mitigación que deben implementarse sobre los controles existentes. Existe una amplia variedad de marcos de trabajo y mejores prácticas disponibles en el mercado para controlar los SCI, sin embargo, hay un "sub-conjunto" de los más reconocidos y utilizados a nivel mundial, entre los cuales se encuentran: ISA99, NIST 800-82, NERC CIP, ISO 27019 / 27032.

ISA99

ISA-99 es un conjunto de estándares para la seguridad de los SCI que fue creado por la Sociedad Internacional de Automatización (ISA). Estos estándares ofrecen unos lineamientos para mejorar la seguridad digital de los procesos y los entornos SCI / SCADA. La implementación de los estándares lleva a las organizaciones a un nivel superior para la seguridad de las tecnologías de la operación, los procesos o los entornos de producción.

Los estándares de ciberseguridad para los entornos de SCI desarrollados por ISA, incluyen:

- General - ISA99.00.01 - Seguridad para sistemas de automatización y control industrial: Terminología, conceptos y modelos. Establece el contexto para todos los estándares restantes de la serie al definir un conjunto común de terminologías, conceptos y modelos para la seguridad electrónica en el entorno de los SCI.
- Políticas y procedimientos - ISA99.00.02 - Establecer un programa de seguridad del SCI. Describe los elementos de un sistema de gestión de la seguridad cibernética y proporciona una guía para su aplicación a los SCI.
- Sistema - ISA99.00.03 - Operar un programa de seguridad del SCI. Aborda cómo operar un programa de seguridad luego de su diseño e implementación. Esta parte incluye una guía para definir y aplicar métricas para medir la efectividad del programa.
- Componente - ISA99.00.04 - Requisitos técnicos de seguridad para los SCI. Define las características de los SCI que los diferencian de otros sistemas de tecnologías de la información desde el punto de vista de la seguridad. En función de estas características,

el estándar establece los requisitos de seguridad que son exclusivos de esta clase de sistemas.

Su propósito es suministrar estándares e información relacionada que definan procedimientos para implementar SCI seguros electrónicamente y evaluar el rendimiento de la seguridad electrónica. Está dirigido a los responsables del diseño, la implementación o la administración de los SCI. Tiene como objetivo mejorar la confidencialidad, la integridad y la disponibilidad de los componentes o sistemas utilizados para el control industrial, y proporcionar criterios para la adquisición e implementación de sistemas de control seguros.

NIST 800-82 / NIST 800-53

El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, desarrolló la serie NIST 800-82 que proporciona una descripción general de las topologías de los SCI y sistemas típicos, identifica las amenazas y vulnerabilidades típicas de estos sistemas y proporciona medidas de seguridad para mitigar los riesgos asociados. El documento incluye una descripción general de SCI genéricos y brinda orientación sobre cómo desarrollar un programa de seguridad para los SCI. El documento también muestra un resumen del documento NIST 800-53, el cual describe los controles generales y proporciona una guía de cómo se deben aplicar a los SCI.

Debido a que hay diferentes tipos de SCI con diferentes niveles de riesgo e impacto, el documento proporciona una lista de diversos métodos y técnicas para proteger los SCI. El documento NIST 800-82 no se debe usar simplemente como una lista de verificación para asegurar un sistema específico, sino que se recomienda a las organizaciones que lo usen, realizar una evaluación basada en el riesgo de sus sistemas y que personalicen las pautas y soluciones recomendadas para cumplir con sus requisitos específicos.

La publicación NIST 800-53, sobre controles de seguridad y privacidad para las organizaciones y los sistemas con información federal, contiene una guía para la lucha contra las nuevas amenazas e incorpora nuevos hitos de privacidad en el marco de referencia que utilizan las agencias federales norteamericanas. Sirve para hacer frente a los peligros internos, el riesgo de la cadena de suministro, los dispositivos móviles, la computación en la nube y otros desafíos. Agrega un apéndice de Confidencialidad con pautas de implementación asociada.

NERC CIP

Sobre el marco

El estándar NERC CIP para la protección de infraestructuras críticas, fue creado por la Corporación de Fiabilidad Eléctrica de Norteamérica (NERC). Esta es una organización que define y aplica estándares de confiabilidad para el sistema de energía de Norteamérica, los cuales quedaron definidos de obligatorio cumplimiento para todas las entidades responsables de la fiabilidad de los sistemas eléctricos en ese país y en los demás donde NERC tiene aplicabilidad (Canadá, y una parte de México).

El marco NERC CIP (versión 5) propone un total de 12 estándares (CIP-1 al 12) cuyo propósito es la protección de infraestructuras críticas, mediante la coordinación de los esfuerzos necesarios

para mejorar la seguridad física y cibernética para el sistema de energía norteamericano, en lo que respecta a la confiabilidad del sistema eléctrico. Estos esfuerzos incluyen el desarrollo de normas, la aplicación de cumplimiento, evaluaciones de riesgos y la preparación y difusión de información crítica, así como la sensibilización en temas de interés. El estándar reconoce las diferentes funciones de cada SCI en la operación del sistema eléctrico, para lo cual se basa en cuatro pilares:

- Fiabilidad, para abordar eventos y riesgos identificables.
- Aseguramiento, con el fin de proporcionar seguridad al público, la industria y el gobierno. para el desempeño confiable del sistema de energía.
- Aprendizaje, como forma de promover la mejora continua de las operaciones y adaptarse a las lecciones aprendidas del sistema de potencia.
- Enfoque basado en el riesgo, concentra la atención, los recursos y las acciones en los asuntos prioritarios de la operación del sistema.

ISO27019 / ISO 27032

El estándar ISO 27032: Técnicas de Seguridad - Pautas para la ciberseguridad, proporciona una guía para mejorar el estado de la ciberseguridad, destacando los aspectos únicos de esa actividad y sus dependencias en otros dominios de seguridad, en particular:

- Seguridad de información
- Seguridad de la red
- Seguridad de internet
- Protección de infraestructura de información crítica

Este estándar internacional proporciona una visión general de la Ciberseguridad, una explicación de la relación entre Ciberseguridad y otros tipos de seguridad, una definición de las partes interesadas y la descripción de sus roles, así como una orientación para abordar los problemas comunes de Ciberseguridad y un marco para permitir a los interesados colaborar en la resolución de problemas de Ciberseguridad.

El estándar ISO 27019: Técnicas de seguridad - Controles de seguridad de la información para la industria de servicios energéticos, proporciona una guía basada en el estándar ISO 27002 aplicada a los sistemas de control de procesos utilizados por la industria de energía para controlar y monitorear la producción o generación, transmisión, almacenamiento y distribución de energía eléctrica, gas, petróleo y calor y para el control de los procesos de soporte asociados.

Este estándar también incluye un requisito para adaptar los procesos de evaluación y tratamiento de riesgos descritos en el estándar ISO 27001 a la orientación específica del sector de servicios de energía.

Mitigar el impacto, ¿por dónde empezar?

Un programa de Ciberseguridad industrial consiste en todas las acciones, actividades, tecnologías, metodologías, técnicas y esfuerzos para proveer la seguridad necesaria o deseada. El desafío para mitigar el impacto de los SCI, consiste en que las organizaciones puedan identificar la demanda generada por los riesgos que cada una debe asumir o enfrentar en sus operaciones y plasmarla en un plan, en este caso para mitigar las amenazas a los SCI.

A continuación, se describe de manera general, una propuesta con nueve puntos para mitigar el impacto en los SCI, los cuales deben estar incluidos en un programa de ciberseguridad:

- Políticas. Se deben desarrollar en torno a la continuidad y a la disponibilidad de las operaciones industriales, deben incluir evaluación de riesgos mediante una metodología, clasificación de proveedores, seguridad física, protocolos industriales, criterios para aceptación de pruebas y todas las cuestiones inherentes a los SCI.
- Riesgos. Se relacionan con el mundo físico, por ejemplo, interrupción del servicio, afectación de la salud y la vida, etc. En comparación con el mundo TI, las consecuencias son diferentes, pues en esta última nacen preocupaciones como la pérdida de información y los datos personales, el cumplimiento de regulaciones, la gestión de la infraestructura tecnológica, etc. Un buen programa debe asumir las consecuencias y riesgos propios de los SCI.
- Prioridad. La importancia de la disponibilidad en los SCI adquiere la mayor relevancia, sin dejar de considerar a la integridad y la confidencialidad de la información.
- Tecnología. La criticidad de los SCI no admite detener las operaciones para instalar un nuevo software, no es posible probar un parche en producción ni se aceptan latencias en las respuestas cursadas por determinados canales de comunicaciones. Por lo tanto, las particularidades de los SCI deben ser conocidas, entendidas y difundidas en toda la organización.
- Vulnerabilidades. Las debilidades y pruebas de penetración, muy comunes y habituales en el mundo TI, no son viables en los SCI bajo los mismos criterios. Deben definirse cuestiones metodológicas, de ingeniería, de configuración, conexión, interferencias, puestas a tierra y muchas otras que son puntuales del mundo industrial. Una simple prueba podría ocasionar una denegación de servicio. Esto conlleva que deba haber competencias particulares, trabajo manual y gran conocimiento de los procesos industriales.
- Análisis de Riesgos. El inventario de los riesgos es importante y debe ser actualizado constantemente, a fin de evaluarlo frente al nivel de aceptación fijado por la organización.
- Detección. Las herramientas de detección y prevención no pueden ser intrusivas, puesto que una disminución en los tiempos de proceso o respuesta no son aceptables en los SCI; se necesitan homologaciones, pruebas y aprobaciones por parte de los fabricantes previo a su uso.
- Mitigación. Consiste en la implementación de técnicas, herramientas, metodologías de diseño, configuración, monitoreo de eventos, etc. y toda acción encaminada a reducir los

riesgos a niveles predeterminados por la empresa; así como también garantizar un estado razonable de seguridad en la prestación del servicio.

- Protección. Busca preservar la disponibilidad, la seguridad física y de las personas, los procesos y el servicio.

¿Qué se está haciendo a nivel legal?

El cibercrimen y la guerra cibernética han dado lugar a un gran número de iniciativas legislativas y regulatorias a nivel mundial. En la práctica, el nivel internacional de leyes y reglamentos de ciberseguridad es algo diverso. La diversidad en los sistemas legales y las perspectivas políticas ha llevado a una variación significativa en la definición y lucha contra el cibercrimen y la ciberguerra.

La ciberseguridad en las empresas públicas y privadas, se rige cada vez más por una serie de leyes y reglamentos. Los sistemas de control industrial, dependiendo del país y del sector en donde se encuentren (energía, petróleo, gas, aeronáutico, defensa, etc.), así como del nivel de protección que cada nación exija dependiendo de su apetito de riesgo, se enfrentan cada vez más a una gran cantidad de nuevas reglas de cumplimiento que deben adoptarse e integrarse con los procesos internos y de producción.

Estados Unidos tiene un complejo conjunto de normas y políticas para administrar el desafío de la ciberseguridad. Las iniciativas comenzaron hace varios años, pero en los últimos diez años ese país ha considerado las amenazas cibernéticas como una amenaza estratégica para la nación. En el año 1998, la Casa Blanca creó la Directiva de decisión presidencial 63 (PDD-63), que recomienda a los organismos tomar las medidas necesarias para garantizar la continuidad y la viabilidad de las infraestructuras críticas. La Ley de Política energética del año 2005 facultó a la Comisión Federal Reguladora de Energía (FERC) para que supervisara la fiabilidad de la red de transporte de energía eléctrica y para que aprobara normas de ciberseguridad. La Corporación para la Fiabilidad de la Red Eléctrica Norteamericana (NERC), que fue certificada por la FERC como organización encargada de la fiabilidad de la red eléctrica de ese país, desarrolló normas de protección de infraestructuras críticas, finalmente aprobadas en el 2008, y que constituyen un conjunto de estándares de ciberseguridad, que el gobierno federal estableció de obligatorio cumplimiento para las compañías relacionadas con el sector eléctrico.

Los estándares NERC CIP, diseñados para la Protección de Infraestructuras Criticas del sector eléctrico, no sólo se encuentran en constante revisión y evolución por parte de la NERC, sino que además han servido como modelo de referencia para otros gobiernos, por ejemplo, es el caso de Colombia.

El Consejo Nacional de Política Económica y Social del Gobierno de Colombia estableció la política nacional de seguridad cibernética, mediante documento CONPES 3701, en el año 2011, bajo el auspicio del Ministerio de TIC, el Ministerio de Defensa, el Departamento Nacional de Planeación, entre otros. A raíz de esta iniciativa, el Consejo Nacional de Operación (CNO), del sector eléctrico, expidió en el año 2015 el acuerdo 788 que establece la guía de Ciberseguridad que todos los agentes generadores, transmisores y distribuidores del Sistema Interconectado Nacional (SIN) deben cumplir. Este acuerdo, establece una hoja de ruta para la implementación de la guía, que no es más que un resumen de los estándares NERC CIP, con los ítems aplicables a Colombia.

En el año 2016, el Ministerio de las TIC, el Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia divulgaron la nueva Política Nacional de Seguridad Digital, resaltando que además

de contemplar la defensa y seguridad nacional en el entorno digital, incluidas las infraestructuras críticas cibernéticas nacionales, incluye componentes como la gobernanza, la educación, la regulación, la cooperación internacional y nacional, la investigación y desarrollo, y la innovación.

Con respecto a Europa hay avances en la materia. En el año 2004, el Consejo Europeo solicitó la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas. En respuesta a esa solicitud, ese mismo año la Comisión adoptó la Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, en la que se formularon propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a infraestructuras críticas. En el año 2005, la Comisión adoptó el Libro Verde sobre un Programa Europeo para la protección de infraestructuras críticas, en el que se exponían las posibilidades de actuación para el establecimiento del Programa y de la Red de información sobre alertas en infraestructuras críticas (CIWIN).

En el año 2006, la Comisión Europea aprobó la comunicación sobre el Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC) mediante el cual se estableció un marco legislativo para las actividades de protección de las infraestructuras críticas en la Unión Europea. En el 2007 se adoptaron unas conclusiones sobre el PEPIC, en las que se reiteró que correspondía a los Estados miembros gestionar las disposiciones de protección de las infraestructuras críticas dentro de sus fronteras nacionales. Allí se destacó que la protección de las infraestructuras críticas incumbía a sus propietarios, a quienes las explotaban y a los Estados miembros donde éstas estuvieran situadas. También se incentivó a los Estados miembros a elaborar un programa nacional de protección que incluyera la clasificación de las infraestructuras y una identificación de interdependencias geográficas.

En España se creó el Centro Nacional de Protección de las Infraestructuras Críticas, con el objetivo de custodiar y actualizar el Plan de Seguridad y el Catalogo Nacional de Infraestructuras Críticas. Entre sus funciones se encuentran la de obtener y administrar información sobre infraestructuras críticas, evaluación de amenazas, análisis de riesgos, mecanismos de alerta, y la coordinación con las administraciones locales de España y con los programas de la Unión Europea.

En el año 2007 el Secretario de Estado de Seguridad aprobó el Plan Nacional de Protección de las infraestructuras críticas, en el que se estableció que éstas eran aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción podían tener una repercusión en la salud, la seguridad o el bienestar económico de los ciudadanos o en el funcionamiento de los gobiernos de los Estados miembros. Entre las infraestructuras se mencionaron las centrales de energía, las redes de comunicaciones, el sector de finanzas, sanitario y alimenticio, transporte de aguas, entre otros.

En el año 2008, la Directiva 114 /CE del Consejo estableció un proceso con vistas a incrementar la seguridad de las infraestructuras críticas europeas. Esta Directiva contribuyó a crear un enfoque global en materia de seguridad energética de la Unión Europea.

Caso *STUXNET*

El malware conocido con el nombre de Stuxnet llamó por completo la atención de investigadores, ya que había sido la amenaza más compleja que se había analizado hasta ese momento en la historia de incidentes relacionados a SCI.

Stuxnet es una pieza de malware con muchos componentes y funcionalidades diferentes, que se diseñó principalmente para apuntar a un SCI. Su objetivo final es reprogramar los SCI modificando el código en los PLC para que funcionen de la manera prevista por el atacante y para ocultar esos cambios al operador del equipo. Para lograr este objetivo, los creadores recopilaron una amplia gama de componentes para aumentar sus posibilidades de éxito. Esto incluyó exploits de día cero, rootkits de Windows, rootkits de PLC, técnicas de evasión de sistemas antivirus, inyección de procesos complejos, rutinas de infección de red, actualizaciones punto a punto y una interfaz de comando y control.

Stuxnet es una amenaza que apuntó a un SCI específico (central nuclear de Natanz, en Irán). Su objetivo final fue sabotear la instalación para enriquecimiento de uranio, reprogramando los PLC para que funcionaran de acuerdo con las instrucciones de los atacantes.

Acciones del ataque

El escenario de ataque, de acuerdo con las fuentes consultadas, es sólo una especulación que surge del análisis de las características técnicas del código de Stuxnet.

Los SCI son operados por un ensamblaje especializado, tales como el código en los controladores lógicos programables (PLC). Los PLC a menudo se programan desde computadores con sistemas operativos Windows, que no están conectados a Internet, ni incluso a las redes LAN.

En primer lugar, los atacantes tuvieron que realizar un reconocimiento. Como cada PLC está configurado de una manera única, los atacantes primero requirieron los esquemas del SCI. Estos documentos de diseño, que en principio son información confidencial, debieron haber sido robados por un empleado interno de la planta, o incluso robados a través de algún otro tipo de ataque cibernético. Una vez que los atacantes obtuvieron los documentos de diseño del entorno informático de la planta, ajustaron la versión de Stuxnet. Cada característica de Stuxnet se implementó por una razón específica y con el objetivo final de sabotear el SCI.

Además, sus archivos binarios maliciosos contenían archivos de controladores que debían estar firmados digitalmente para evitar sospechas. Para ello, los atacantes debieron obtener dos certificados digitales de alguien que podría haber ingresado físicamente en las instalaciones de las dos compañías y haberlos robado.

Para infectar su objetivo, Stuxnet debió ser introducido en el entorno de la planta. Esto puede haber ocurrido al infectar a una tercera parte, por ejemplo, un contratista, que tal vez tuvo acceso a la instalación, o un interno. La infección original puede haber sido introducida por una unidad extraíble, de tipo memoria USB.

Una vez que Stuxnet infectó un computador dentro de la planta, comenzó a diseminarse en busca de computadores Windows que se usan para programar los PLC. Dado que la mayoría de estos computadores no están conectados a la red, Stuxnet debió intentar primero extenderse a otros computadores en la red mediante una vulnerabilidad de día cero, a través de unidades extraíbles. La propagación a través de la red LAN probablemente sirvió como el primer paso y la propagación a través de unidades extraíbles como un medio para cubrir el último salto al computador que no estaba conectado a la red industrial, el que se utilizaba para programar los PLC.

Mientras que los atacantes podían controlar Stuxnet con un servidor de comando y control, era poco probable que el computador final que ejecutaba el ataque, tuviera acceso a Internet. Por lo tanto, toda la funcionalidad requerida para sabotear el SCI se incrustó directamente en el archivo ejecutable de Stuxnet. Las actualizaciones de este ejecutable se propagaban a través de la red mediante un método de peer-to-peer establecido por Stuxnet. Cuando Stuxnet finalmente encontró el computador adecuado, entonces modificó el código en el PLC. Estas modificaciones probablemente sabotearon el sistema.

Posteriormente, las víctimas que intentaran verificar el problema no verían ningún código PLC fraudulento, ya que Stuxnet ocultaba sus modificaciones.

Si bien haber utilizado métodos de auto-replicación pudo haber sido necesario para garantizar que encontrarían el computador adecuado, también causó daños colaterales notables al infectar máquinas fuera de la planta objetivo, lo cual pudo haber sido visto como una necesidad para alcanzar efectivamente el objetivo deseado.

Vulnerabilidades de los sistemas

Stuxnet contiene muchas características, entre ellas las más relevantes fueron:

- Capacidad de auto-replicarse a través de unidades extraíbles USB, aprovechando una debilidad de Microsoft Windows que permite ejecución automática. La vulnerabildiad es conocida como: Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability.
- Capacidad de propagarse en una red LAN a través de una vulnerabilidad de ejecución remota de código en el servicio de cola de impresión de Microsoft Windows. La debilidad es conocida como: Microsoft Windows Print Spooler Service Remote Code Execution Vulnerability.
- Capacidad de propagarse a través del servicio SMB de Microsoft Windows, explotando una debilidad de ejecución remota de código RPC. La debilidad es conocida como: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability.
- Copia y se ejecuta en computadoras remotas a través de recursos compartidos de red. Esta vulnerabilidad podría estar presente a nivel del diseño de la red de control y de la red LAN, así como también en la ausencia de controles de seguridad para monitorear, detectar e impedir la ejecución no autorizada de archivos ejecutables.

- Copia y se ejecuta en equipos remotos que ejecutan un servidor de base de datos del aplicativo WinCC. Al igual que el caso anterior, esta vulnerabilidad podría estar presente a nivel del diseño de la red de control y de la red LAN, así como también en la ausencia de controles de seguridad para monitorear, detectar e impedir la ejecución no autorizada de archivos ejecutables.
- Se actualiza a sí mismo a través de un mecanismo de peer-to-peer dentro de una LAN. La debilidad en el diseño de las redes LAN y de control sigue siendo evidente, ya que los mecanismos de peer-to-peer deberían estar restringidos a nivel de plantillas de seguridad, que normalmente son definidas y configuradas en los distintos computadores, y cualquier cambio o modificación debería ser monitoreado y alertado.
- Aprovecha un total de cuatro vulnerabilidades de Microsoft no parcheadas, dos de las cuales son de auto-replicación y las otras dos para escalar privilegios.
- Contacta con un servidor de comando y control que permite al atacante descargar y ejecutar código remoto. Se sigue presentado la vulnerabilidad en la ausencia de controles de seguridad, tales como el monitoreo de conexiones entrantes/salientes hacia Internet. Un monitoreo adecuado de las conexiones entrantes/salientes, permite identificar y alertas conexiones hacia servidores de comando y control.
- Contiene un rootkit de Windows que oculta sus binarios.
- Intenta evadir los productos de seguridad. Existe ausencia de implantación de un modelo de seguridad por capas, también conocido como defensa en profundidad, según el cual la seguridad se implementa por capas y en diferentes niveles, en que cada uno tiene unas funciones particulares en detección, monitoreo y notificación, prevención, recuperación, entre otros.
- Toma toda la información de un SCI específico y modifica el código en los PLC de Siemens para sabotear el sistema. Esta vulnerabilidad a pesar que logró mediante una debilidad en dos productos de terceros (fabricante de PLC), existe otra debilidad que se puede identificar, como es el caso de la validación de autenticidad de un producto antes de instalarlo. Una adecuada verificación de la integridad de un firmware o instalador debe ser corroborado antes de confiarle, validando el resumen (hash) de cada producto.
- Oculta el código modificado en PLC, esencialmente el rootkit para PLC.

Desde el punto de visto de la seguridad operacional, ¿qué ocurrió mal?

Stuxnet representa el primero de muchos hitos en la historia de códigos maliciosos: es el primero en explotar cuatro vulnerabilidades de día cero, comprometer dos certificados digitales de fabricantes de PCL, e inyectar código en sistemas de control industrial y esconder el código del operador del SCI.

Stuxnet es de una complejidad tan grande que requirió recursos significativos para desarrollarse, y pocos atacantes estarían en capacidad de producir una amenaza similar. Las implicaciones del mundo real de Stuxnet están más allá de cualquier amenaza que se haya visto en el pasado.

Sin embargo, también es cierto que mediante la adopción de un marco de seguridad (tal como se describió en los apartados: ¿Cómo mitigar el impacto de este tipo de adversidades en los SCI?, y en la Seguridad Operativa y su importancia en los Sistemas de Control Industrial, de este documento) hubiera sido posible evitar el ataque, o al menos dificultarlo en mayor medida a los atacantes. A continuación, se listan los dos principales elementos que desde el punto de vista de la seguridad operacional facilitaron el éxito del ataque:

- Para lograr una adecuada gestión, la seguridad operacional se enfoca en los procesos, los sistemas y las personas, entendiendo que, en este último las vulnerabilidades propias de los seres humanos si no son gestionadas apropiadamente incrementan los riesgos. La adopción de un marco de ciberseguridad debería abordar los aspectos mencionados, entre ellos la capacitación al personal que opera los SCI, las restricciones y prohibición que deben conocer, por ejemplo las restricciones de conexión de cualquier medio removible en los computadores de la planta, sobre el ingreso de proveedores o contratistas a las redes industriales y las restricciones que éstos deben respetar, como impedirles conectar sus computadores a las redes industriales o conectar memorias USB o medios removibles en los computadores de la planta.
- Para la sostenibilidad de la seguridad operacional, se deben definir factores claves de éxito entre ellos la gestión del riesgo, procesos y procedimientos y tecnología, con herramientas óptimas para la medición, seguimiento y monitoreo, con el fin de verificar el cumplimento de la seguridad operacional. Está claro que, mediante unos procesos bien definidos, probados, actualizados, monitoreados, y basados en marcos de trabajo, estándares y buenas prácticas, las posibilidades de intrusión e infección por malware disminuirían drásticamente. Por ejemplo, un proceso bien definido para monitorear cualquier actividad sospechosa, por ejemplo, la conexión de computadores internos, bien sean de la red industrial o de la red corporativa, hacia servidores externos, por ejemplo, de comando y control, debería generar una alerta de seguridad. Cualquier ingreso/conexión de un medio removible no autorizado en un computador, debería ser rechazado ya sea por políticas de configuración de los computadores, o ser monitoreados o controlados por una función de seguridad. Cualquier modificación sobre las rutinas de un PLC, deberían ser realizadas a través de cuentas que tienen contraseñas únicas y no deberían existir contraseñas por defecto; de igual forma, la modificación de un PLC debería ser monitoreado y cualquier cambio no autorizado debería monitoreado y alertado.

Conclusiones

Los SCI son una combinación de diferentes sistemas de procesos industriales en tiempo real, que consta de diferentes componentes interconectados que tienen su propia tarea específica en el proceso. La infraestructura de un SCI a menudo es muy compleja, puesto que SCI podría tener miles de unidades y por lo general, consta de sistemas heredados que son muy antiguos. Como resultado, se tiene que un SCI es difícil de controlar considerando que los sistemas demandan alta disponibilidad.

Al comparar las Tecnologías de la información y las comunicaciones TIC con las Tecnologías de la operación TO, una diferencia muy importante es el impacto que puede ocasionar un incidente de seguridad en un SCI. Por ejemplo, comprometer la seguridad de una red empresarial (TIC) podría tener consecuencias financieras, la privacidad del cliente podría verse comprometida, afectar la imagen corporativa, y así sucesivamente. Cuando se produce un incidente de seguridad en un SCI, la magnitud del impacto cambia, los bienes físicos podrían ser destruidos, las personas heridas o incluso fallecidas, y además gran parte de las consecuencias de las TIC también aplicarían en TO.

No existe una fórmula que permita garantizar la seguridad de todos los activos críticos de un SCI, ni tampoco normas ni componentes tecnológicos que garanticen que todo estará bien y que no habrá problemas en el futuro; se deben considerar factores como la importancia que se le da a la ciberseguridad en la organización, al apoyo y el compromiso de la alta dirección, a los recursos asignados y la importancia del lugar que ocupa la ciberseguridad industrial en la agenda.

La adopción de buenas prácticas, normas y estándares constituyen una hoja de ruta de gran valor, pero los desafíos a la hora de aplicarlas son la transformación del “qué hacer” al “cómo hacerlo”, se deben interpretar las necesidades de la organización, conseguir el apoyo gerencial, obtener los recursos, gestionar los riesgos, diseñar métricas para tomar decisiones y demostrar el retorno de las inversiones en ciberseguridad industrial.

El desarrollo y la adopción de tecnologías, las amenazas y los estándares crece a ritmos diferentes, para proteger los sistemas de control industrial, no es suficiente seguir los estándares y buenas prácticas, éstos deben utilizarse como referencia, adoptando y adaptando sus contenidos, pero siempre se debe ir más allá de los mismos.

APÉNDICE A – Glosario de Siglas y Acrónimos

Activo: Algo de valor tangible o intangible que vale la pena proteger. Algunos ejemplos son las personas, la información, la infraestructura, las finanzas, la reputación, entre otros.

Amenaza: cualquier cosa que sea capaz de actuar contra un activo de una manera que pueda resultar en daño. De manera amplia se puede definir como una posible causa de un incidente no deseado.

APT: *Advanced Persistent Threat*. Una amenaza persistente avanzada, es un conjunto de procesos informáticos sigilosos y continuos de piratería informática, dirigido a una entidad específica.

BSI: *Federal Office for Information Security*. Oficina Federal para la Seguridad de la Información de Alemania.

CE: Consejo Europeo.

CIWIN: *Critical Infrastructure Warning Information Network*. Red de información sobre alertas en infraestructuras críticas en Europa.

CNO: Consejo Nacional de Operación, del sector eléctrico en Colombia.

CONPES: Consejo Nacional de Política Económica y Social de Colombia.

Cross-site scripting: Es un tipo de vulnerabilidad informática típica de las aplicaciones web, que permite al atacante inyectar código JavaScript u otro lenguaje similar en la página web vulnerable.

CVSS: *Common Vulnerability Score System*. Sistema común de calificación de vulnerabilidades.

DoS: *Denial of Service*. La denegación de servicio es un ataque a un sistema que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Exploit: Palabra inglesa que significa explotar o aprovechar. En el ámbito de la informática es una secuencia de comandos o acciones, que se utiliza con el fin de aprovechar una debilidad de seguridad de un sistema de información.

FERC: *Federal Energy Regulatory Commission*. Comisión Federal Reguladora de Energía, en Estados Unidos.

FTP: *File Transfer Protocol*. Protocolo para transferencia de datos.

Hacktivista: Pirata informático con motivaciones políticas. Por lo general apunta a individuos u organizaciones específicos para lograr diversos fines ideológicos.

Havex: Malware que afecta sistemas de control industrial/SCADA.

HTTP: *Hypertext Transfer Protocol*. Protocolo de transferencia de hipertextos, que se utiliza en la mayor cantidad de direcciones de internet.

IDS / IPS: *Intrusion Detection System / Intrusion Prevention System*. Los sistemas para detección y prevención de intrusos, son funcionalidades provistas a nivel de software y/o hardware, que ejercen el control de acceso en una red para proteger la red y los sistemas contra ataques.

Inyección de código: Es un método que consiste en ingresar código en una aplicación para realizar operaciones no autorizadas la aplicación.

ISA: *International Society of Automation*. La Sociedad Internacional de Automatización es una asociación que establece estándares para mejorar la gestión y la seguridad de los sistemas de automatización y control utilizados en la industria y las infraestructuras críticas.

ISO: *International Organization for Standardization*. Esta organización promueve el desarrollo y la implementación de normas a nivel internacional, tanto de fabricación como de servicios.

Malware: Es la abreviatura de *Malicious software* o software malicioso. Engloba a todo tipo de programas o códigos informáticos maliciosos cuya función es dañar un sistema o causarle un mal funcionamiento.

NERC: *North American Electric Reliability Corporation*. Corporación para la Fiabilidad de la Red Eléctrica Norteamericana.

NFS: *Network File System*. El sistema de archivos de red, es un protocolo de nivel de aplicación utilizado para sistemas de archivos distribuido en un entorno de red de área local.

Peer-to-peer: Es un tipo de arquitectura que permite la comunicación entre aplicaciones para compartir información entre computadores sin la necesidad de un servidor central que facilite la comunicación.

PEPIC: Programa Europeo para la Protección de Infraestructuras Críticas.

Phishing: Es un término utilizado para referirse a un método de suplantación de identidad para estafar y obtener información confidencial de forma fraudulenta.

Plantilla de seguridad: Proceso para asegurar un sistema mediante la reducción de sus posibles vulnerabilidades.

PDD: *Presidential Decision Directive*. Directiva de decisión presidencial.

Riesgo: La combinación de la probabilidad de un evento y su consecuencia.

Riesgo residual: después de haber establecido salvaguardas, siempre existirá un riesgo residual. Se puede definir como el riesgo restante después de haber implementado controles.

Riesgo inherente: el nivel de riesgo o la exposición al riesgo sin tener en cuenta las medidas que se hayan tomado o que se podrían tomar.

Rootkit: Programa que oculta la presencia de malware en el sistema en donde esté instalado, y puede esconder su presencia interceptando y modificando las funciones a bajo nivel. También sirve para esconder los procesos y archivos que el intruso esté ejcutando.

SIN: Sistema Interconectado Nacional, en Colombia.

SCADA: *Supervisory Control and Data Acquisition*. Este tipo de sistemas permiten controlar y supervisar los procesos industriales a distancia.

Servidor de comando y control: Es un computador que da órdenes remotamente a dispositivos infectados con malware y que recibe información de esos dispositivos de manera remota.

SQL: *Structured Query Language*. El lenguaje de consulta estructurada SQL es un lenguaje que da acceso a un sistema de gestión de bases de datos relacionales que permite especificar diversos tipos de operaciones en ellos.

Stuxnet: Es un malware diseñado para los sistemas de control industrial.

Telnet: *Telecommunication Network*. Es un protocolo de red que permite acceder a otra máquina para manejarla remotamente como si se estuviera en ella.

TIC: Tecnologías de la información y las comunicaciones.

Troyanización: Implantación de un troyano dentro de una pieza de software.

Troyano: Programa malicioso que realiza acciones no autorizadas por el usuario. Algunas de las acciones que pueden realizar son la eliminación, bloqueo, modificación y copia de datos, así como la interrupción del rendimiento de un computador o una red de computadores.

Vulnerabilidad de día cero: Vulnerabilidad que aún no ha sido identificada por el fabricante.

APÉNDICE B – Bibliografía y Referencias documentales

Advisory (ICSA-14-178-01) "*ICS Focused Malware Havex*" 2014, disponible en https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01

Alert (ICS-ALERT-14-176-02A) "*ICS Focused Malware (Update A)*" 2014, disponible en https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A

BBC News "*Hack attack causes 'massive damage' at steel works*" 2014, disponible en http://www.bbc.com/news/technology-30575104

Centro Nacional de Integración de Ciberseguridad y Comunicaciones NCCIC, Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial ICS-CERT "*Industrial Control Systems Assessment Summary Report*" 2015, disponible en https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

Computer Emergency Response Team (CERT), division of the Software Engineering Institute (SEI), Carnegie Mellon University "CERT Annual Reports 1994-2003", disposnible en https://www.cert.org/historical/annual_rpts/

Departamento de Defensa de los Estados Unidos, "*Remarks on the Department of Defense Cyber Strategy*" 2011, disponible en http://archive.defense.gov/speeches/speech.aspx?speechid=1593

Directiva 2008/114/CE "*sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección*" 2008, disponible en https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

Documento Conpes 3701 "Lineamientos de Política para Ciberseguridad y Ciberdefensa" 2011, disponible en http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Documento Conpes 3854 "Política Nacional de Seguridad Digital" 2016, disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf

Ellison R./ Alberts C./ Creel R./ Dorofee A./ Woody C. "*Software Supply Chain Risk Management: From Products to Systems of Systems*" 2010, disponible en https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9377

Equipo de Respuesta a Emergencias Cibernéticas de Sistemas de Control Industrial ICS-CERT "Overview of Cyber Vulnerabilities", disponible en https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

Federal Energy Regulatory Commission, "*Cyber & Grid Security*" 2005, disponible en http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp

Hentunen D. / Tikkanen A. “Havex Hunts For ICS/SCADA Systems” 2014, disponible en https://www.f-secure.com/weblog/archives/00002718.html

Homeland Security Digital Library, “*Presidential Decision Directive 63: Protecting America's Critical Infrastructures*” 1998, disponible en https://www.hsdl.org/?abstract&did=3544

Homeland Security Digital Library, “*The Comprehensive National Cybersecurity Initiative*” 2010, disponible en https://www.hsdl.org/?abstract&did=28609

Informe "*Seguridad Cibernética e Infraestructura Crítica en las Américas*" 2015, disponible en http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-120/15

Infosec Island “*South Houston's Water Supply Network Hacked*” 2011, disponible en http://www.infosecisland.com/blogview/18244-South-Houstons-Water-Supply-Network-Hacked.html

ISA 62443-1-1 “*Security for industrial automation and control systems*” 2017, disponible en http://isa99.isa.org/Public/Series/Documents/ISA-62443-1-1-Public.pdf

ISA 62443-3-3 “*Security for industrial automation and control systems*” 2013, disponible en http://isa99.isa.org/Public/Series/Documents/ISA-62443-3-3-Public.pdf

ISO 27019 “*Information technology - Security techniques - Information security controls for the energy utility industry*” 2017, disponible en https://www.iso.org/standard/68091.html

ISO 27032 “*Information technology - Security techniques - Guidelines for cybersecurity*” 2012, disponible en https://www.iso.org/standard/44375.html

Kaspersky Lab ICS-CERT “Threat Landscape for Industrial Automation Systems in the second half of 2016” 2016, disponible en https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

Kon M. “¿Qué hay de cierto, aciertos y desaciertos cuando se habla de convergencia IT/OT?” 2016, disponible en http://wisecourses.com/wp-content/present/ConvergenciaITOT/index.html

Lipovsky R./ Cherepanov A., “El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania” 2016, disponible en https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

Marinos L./ Belmonte A./ Rekleitis E. “*ENISA Threat Landscape 2015*” 2016, disponible en https://www.enisa.europa.eu/publications/etl2015

McGraw, G. "*Software [In]security: How to p0wn a Control System with Stuxnet.*" 2010, disponible en http://www.informit.com/articles/article.aspx?p=1636983

National Institute of Standards and Technology, "*NIST Identifies Five Smart Grid Standards*" 2010, disponible en http://www.nist.gov/public_affairs/releases/smartgrid_100710.cfm

North American Electric Reliability Corporation, "*Critical Infrastructure Protection Committee (CIPC)*" , disponible en http://www.nerc.com/comm/cipc/pages/default.aspx

Perlroth N. "*Russian Hackers Targeting Oil and Gas Companies*" 2014, disponible en https://www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html

Stouffer K./ Pillitteri V./ Lightman S./ Abrams M./ Hahn A. "*NIST Special Publication 800-82 Rev 2*" disponible en http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

White House, Office of the Press Secretary, "*Executive Order -- Improving Critical Infrastructure Cybersecurity*" 2013, disponible en https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Zetter K., "*How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*" 2011, disponible en https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/