Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Ciberseguridad en Infraestructuras Críticas Energéticas

Autor:
Erick Santiago Pazmiño Sosa

Tutor de Trabajo Final:
Dr. Juan Pedro Hecht

Año de presentación: 2019
Cohorte: 2018

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Erick Santiago Pazmiño Sosa
DNI: 95817370

Resumen

Este trabajo presenta una descripción del concepto de infraestructuras críticas y su utilidad dentro de la sociedad. Así como los riesgos de ciberseguridad a los que se enfrentan debido a la integración de tecnologías de nueva generación dentro de las mismas.

La integración de los Sistemas de Control Industrial (ICS) y las tecnologías de nueva generación (IIoT) han permitido a las infraestructuras críticas automatizar los procesos robóticos (RPA) mediante el uso de machine intelligence, así como utilizar la automatización cognitiva (CA) y la inteligencia artificial (AI) para la monitorización de seguridad de los sistemas físicos. Sin embargo, esta integración trae consigo una serie de riesgos de ciberseguridad que si no son tomados en cuenta pueden causar desde ligeras pérdidas económicas hasta una catástrofe como sería la pérdida de vidas humanas.

Para el desarrollo de este trabajo se ha recolectado bibliografía de distintas fuentes, la misma ha servido para tomarla como base teórica. Posteriormente, se presenta la conclusión personal que se ha desarrollado teniendo en cuenta lo expuesto a lo largo del presente trabajo.

Palabras claves: ICS – SCADA – riesgos – ciberseguridad – smart – energía – sistemas de control.

Índice de contenidos

Índice de ilustraciones

Antecedentes

Muchos sistemas industriales fueron construidos utilizando dispositivos legacy, así como en algunos casos, se ejecutan protocolos legacy los cuales han evolucionado para funcionar en redes enrutables. Los sistemas de automatización de procesos se construyeron mucho antes de la proliferación de la conectividad de los Sistemas de Control Industrial a Internet, las aplicaciones basadas en la web y los sistemas de información empresarial en tiempo real. La seguridad de la información por lo general no se trataba de manera prioritaria puesto que los sistemas de control estaban separados físicamente sin un sistema común que los uniera a redes vulnerables (corporativas).

Sin embargo, en la década de 1990 muchas organizaciones empezaron a rediseñar sus procesos de negocio y sus necesidades de integración operativa, con lo cual se comenzó a realizar una mayor integración no sólo entre las aplicaciones comunes de un Sistema de Control Industrial sino también con aplicaciones empresariales típicas como los sistemas de planificación de la producción. Por este motivo, en estos momentos la ciberseguridad de las infraestructuras críticas es de vital importancia, tanto para el negocio como para los usuarios de los servicios que estas proveen.

Justificación

Originalmente, las implementaciones de los Sistemas de Control Industrial (ICS) solo eran susceptibles a amenazas locales debido a que sus componentes estaban ubicados en áreas físicamente protegidas, es decir que los componentes no estaban conectados a redes o sistemas corporativos. Sin embargo, la tendencia de integrar los sistemas de control con los sistemas o redes corporativas significan más exposición de los sistemas de control al mundo exterior, por lo tanto, el riesgo se ve incrementado debido a las amenazas externas. En estos momentos donde la integración entre las redes corporativas y las redes industriales están emergiendo se abre un nuevo camino hacia los elementos críticos de un Sistema de Control Industrial, lo cual significa que un atacante que pudiese llegar a encontrar este camino para

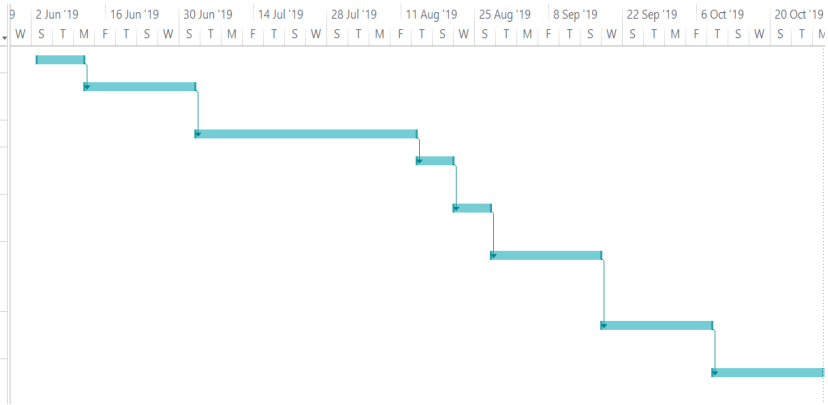
su posterior explotación sería capaz de causar grandes catástrofes. De acuerdo a una investigación realizada en 2010, donde alrededor de 100 instalaciones eléctricas fueron puestas a prueba para comprobar su estado de ciberseguridad demostró que existían más de 38000 advertencias de seguridad y vulnerabilidades. Así mismo, se determinó que el tiempo que pasó entre el descubrimiento público de una vulnerabilidad y el descubrimiento de la misma dentro del Sistema de Control Industrial fue de 331 días. Lo cual demuestra que aún la ciberseguridad no es tomada como una prioridad dentro de las compañías de infraestructura crítica. Una vez mencionado esto, el enfoque de este trabajo es concientizar a los usuarios acerca de la importancia de la ciberseguridad en infraestructuras críticas a la vez que se recomiendan las medidas que se deben tomar a fin de reducir los vectores de ataque que se podrían presentar.

Objetivos y Alcance

- Definir el concepto de Infraestructuras Críticas
- Definir el concepto de Sistemas de Control Industrial
- Definir el concepto de Infraestructuras Críticas Energéticas
- Determinar los estándares de ciberseguridad industrial
- Determinar los estándares de ciberseguridad aplicada a industrias energéticas.
- Recomendar las medidas que permitirán reducir el vector de ataque.

Metodología y plan de actividad

Task Mode	Task Name	Duration
	Recopilación de material	7 days
	Lectura y comprensión de material	15 days
	Síntesis y escritura	30 days
	Descripción de las etapas de un ataque	5 days
	Consecuencias de un ciberataque	5 days
	Evaluación de aplicabilidad de los distintos estándares	15 days
	Recomendación de mejores prácticas	15 days
	Conclusiones y recomendaciones	15 days



Capítulo 1: ¿Qué es una Infraestructura Crítica?

El Departamento de Seguridad de Estados Unidos, define una infraestructura crítica como “conjunto de activos, sistemas y servicios físicos y cibernéticos que son vitales para el país, y su incapacidad o destrucción tendría un impacto debilitante en la seguridad física, económica, salud y seguridad pública” [1]. Algunos tipos de infraestructura crítica son los siguientes:

— Plantas de generación energética.
— Represas
— Servicios de emergencia
— Instalaciones gubernamentales
— Salud pública
— Sistemas de agua y desechos residuales
— Entre otros.

A partir de esto, se puede decir que un ciberataque sobre una infraestructura crítica podría generar un impacto que traería consigo potenciales consecuencias para las personas que utilizan los servicios que estas ofrecen.

Ilustración 1 Ejemplos de Infraestructuras Críticas

Fuente: http://resilens.eu/about-resilience/critical-infrastructures/ [2]

Las infraestructuras críticas se encuentran compuestas por lo general por un entorno OT (Operational Technology). Un entorno OT está compuesto por uno o varios sistemas de control industrial.

¿Qué es un Sistema de Control Industrial?

Un sistema de control industrial abarca una amplia gama de sistemas de automatización que son utilizados para el monitoreo y control de las instalaciones que existen en un ambiente industrial. Así mismo, también puede ser definido como “una parte integral de una infraestructura crítica que permite facilitar las operaciones de distintos tipos de industrias como son: energía, gas, petróleo, agua, transporte, manufactura, petroquímicas, entre otros” [3].

En un sistema de control industrial generalmente pueden existir elementos como: equipamiento de campo ya sean sensores, actuadores, medidores, indicadores y componentes del sistema de control, como controladores lógicos programables (PLC), unidades de terminales remotas (RTU), dispositivos electrónicos inteligentes. (IED), interfaces hombre-máquina (HMI), estaciones de trabajo de ingeniería, servidores de aplicaciones, historiadores de datos y otras consolas.

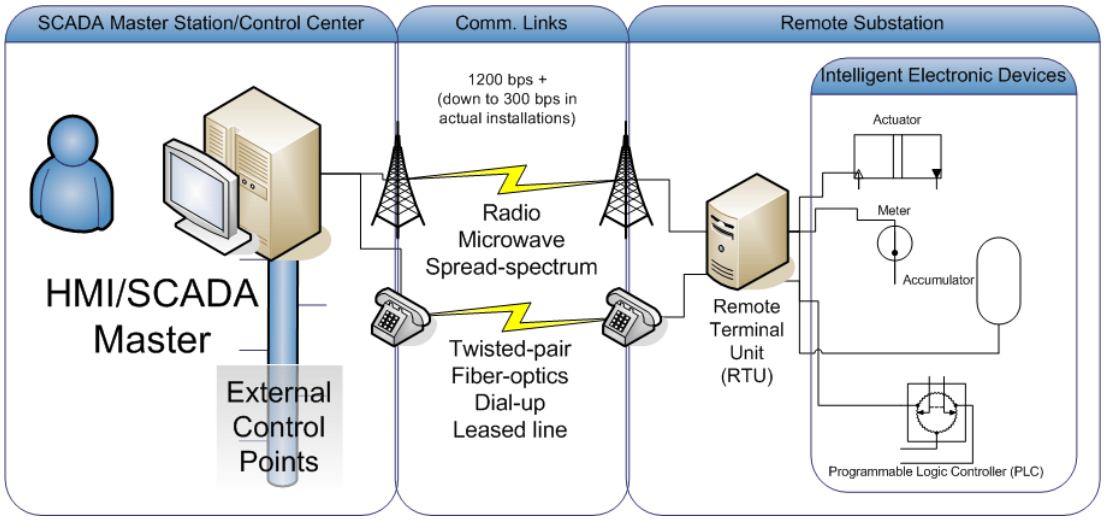


Ilustración 2 Ejemplo de Sistema de Control Industrial

Fuente: https://www.lanner-america.com/blog/5-common-vulnerabilities-industrial-control-systems/ [4]

A continuación, se describirá brevemente la funcionalidad de cada uno de estos componentes:

Componentes de un Sistema de Control Industrial

PLC:

El controlador lógico programable es “una computadora industrial

utilizada para automatizar las funcionalidades dentro de las instalaciones de un entorno industrial. A diferencia de las computadoras utilizadas en el ámbito corporativo, los PLC normalmente están adecuados para ser implementados en un entorno operativo de producción" [5]. Por lo general los PLC, no utilizan un Sistema Operativo que sea comercializado libremente, sin embargo, se basan en programas de aplicación específicos, que permiten al PLC generar acciones de salida en respuesta a entradas específicas. Por ejemplo, una salida que permita bombear motores en respuesta a la variable de un sensor determinada. Los PLC por lo general son utilizados para controlar procesos en tiempo real.

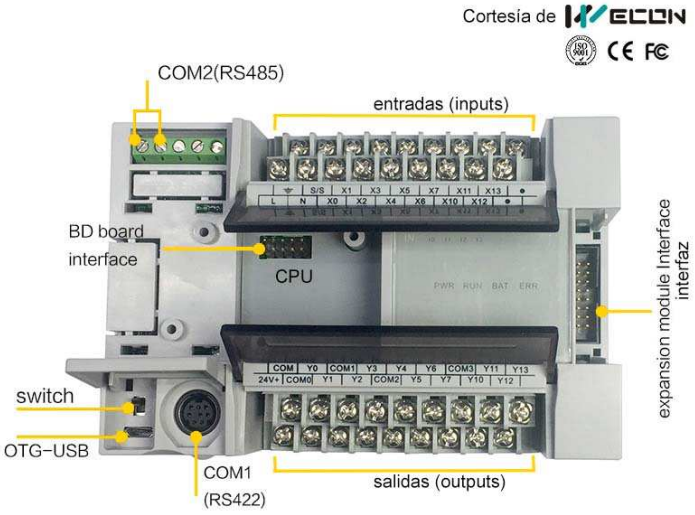


Ilustración 3 Ejemplo de PLC

Fuente: https://intrave.wordpress.com/2015/02/20/para-que-sirve-un-plc/ [6]

RTU:

Por lo general, una Unidad Terminal Remota (RTU), se encuentra implementada en subestaciones de generación de energía eléctrica, ya sea a lo largo de una tubería o en alguna otra ubicación remota. La función principal de las RTU es el monitoreo de los parámetros que son distribuidos a través del campo para su posterior retransmisión a una unidad de terminal maestra (MTU) que por lo general "suele tratarse de una estación de monitoreo central." [5] Generalmente, las RTU poseen la capacidad de enlazar comunicaciones remotas mediante la conexión de radio, datos celulares u otra tecnología de comunicación que alcance un área amplia.

Como se mencionó anteriormente, las RTU se encuentran implementadas a menudo en ubicaciones remotas, a las cuales no se puede suministrar fácilmente electricidad, motivo por el cual esta puede ser suministrada mediante instalaciones locales de generación o almacenamiento de energía solar. Así mismo, las RTU están diseñadas para soportar condiciones ambientales extremas ya que suelen ser colocadas al aire libre. Algunas RTU cuentan con funciones de lógica y control programable, por lo cual en ocasiones una RTU puede ser considerada como un PLC remoto.

Ilustración 4 Ejemplo de RTU

Fuente: https://en.wikipedia.org/wiki/Remote_terminal_unit [7]

Dispositivo Electrónico Inteligente (IED):

Estos dispositivos, al igual que las RTU se encuentran generalmente desplegadas en sectores de servicios eléctricos. Este dispositivo fue "desarrollado para permitir su instalación en áreas que involucran fuentes de energía de alto voltaje ". [5] A medida que se presenta un avance en tecnología, estos dispositivos han evolucionado hasta volverse más sofisticados, por lo tanto, son capaces de realizar más de una tarea dentro del proceso de automatización de un sistema de control.

Ilustración 5 Ejemplo de IED

Fuente: https://www.utilityproducts.com/vehicles-accessories/article/16002728/intelligent-electronic-devices-increase-availability-power-quality-in-power-distribution-networks [8]

HMI:

El HMI por sus siglas en inglés (Human Machine Interface) son dispositivos generalmente utilizados como medio para que un operador pueda interactuar con los PLC, RTU e IED. Es decir, estos dispositivos permiten remplazar los interruptores y otros controles eléctricos que se ejecutaban manualmente, por representaciones gráficas que contienen controles digitales que sirven para que los operadores puedan influir en el proceso operativo. Dentro de las actividades que permiten realizar estos HMI, están los siguientes:

- Iniciar y detener ciclos
- Ajustar parámetros
- Ajustar variables de un proceso de control

En [3] un HMI se define también como “aplicaciones de software que se pueden presentar de dos distintas maneras. La primera, consiste en la ejecución de este software sobre un sistema operativo base (por ejemplo, Windows 7). Así mismo, también se puede presentar como una computadora industrial hardenizada, que contiene un panel táctil local y esta encapsulada para soportar el montaje de este en ambientes industriales”. Cabe destacar, que este HMI funciona como medio de interacción entre el operador y la lógica de uno o más PLC, lo cual permite dar una visualización del proceso. Para lograr esto, la interfaz de usuario se configura para representar gráficamente

el proceso industrial que desea ser controlado, donde se incluya los valores de los sensores de medición y la representación visible de los estados de salida.

Ilustración 6 Ejemplo de HMI

Fuente: https://blog.industrialmegamart.com/things-know-human-machine-interface/ [9]

Estaciones de Trabajo de Supervisión:

Las estaciones de trabajo suelen ser utilizadas con fines de supervisión. Esto lo realizan mediante la recopilación de datos operativos que se generan de los activos que constituyen parte de un sistema de control industrial. La intención de recopilar esta información es para que mediante software se puedan crear métricas de esta información a fin de utilizarla y analizarla con fines de supervisión. Estas estaciones de trabajo se diferencian de los HMI principalmente porque estas generalmente solo son utilizadas en modo lectura, es decir que no cuentan con un elemento que les permita interactuar directamente con el proceso industrial y solo presenta información relevante del proceso. Sin embargo, en casos aislados, estas estaciones pueden ser capaces de cambiar ciertos parámetros que solo pueden ser manipuladas por el jefe del área. Dentro de los parámetros que pueden ser modificados se encuentran los límites de las alarmas, y en casos puntuales, modificar puntos de ajuste del proceso industrial.

Ilustración 7 Ejemplo de Estación de Trabajo de Supervisión

Fuente: http://mumbai.indianrenters.com/pages/workstation.php [10]

Historiadores:

Un historiador de datos es un sistema de software utilizado dentro de las redes industriales para recopilar valores de puntos, eventos de alarma y otra información de los dispositivos y sistemas industriales desplegados en la red industrial, para posteriormente almacenarlo en una base de datos especialmente diseñada.

Ilustración 8 Ejemplo Historiador

Fuente: http://www.iconics-uk.com/solutions/data-historian [11]

Sistema SCADA:

El sistema SCADA (Supervisory Control and Data Acquisition) está diseñado para "realizar monitoreo del sistema de control industrial y el proceso que administra (leer datos y presentarlos a un operador humano y a otras aplicaciones, como historiadores y aplicaciones de control avanzado) y para controlar (definir parámetros y ejecutar instrucciones) equipos industriales." [5]. La arquitectura de estos sistemas varía de acuerdo al proveedor, sin embargo, por lo general todas incluyen las aplicaciones y herramientas necesarias para generar, probar, implementar, monitorear y controlar un proceso automatizado. De acuerdo a [3], los sistema SCADA son "capaces de proporcionar múltiples funcionalidades, es decir, que un inspector de calidad puede usar una estación de trabajo con fines de supervisión (solo lectura), mientras que otro puede para escribir nuevos programas dentro de un controlador, también puede ser utilizado como una interfaz de usuario centralizada para controlar un proceso que requiere más intervención humana".

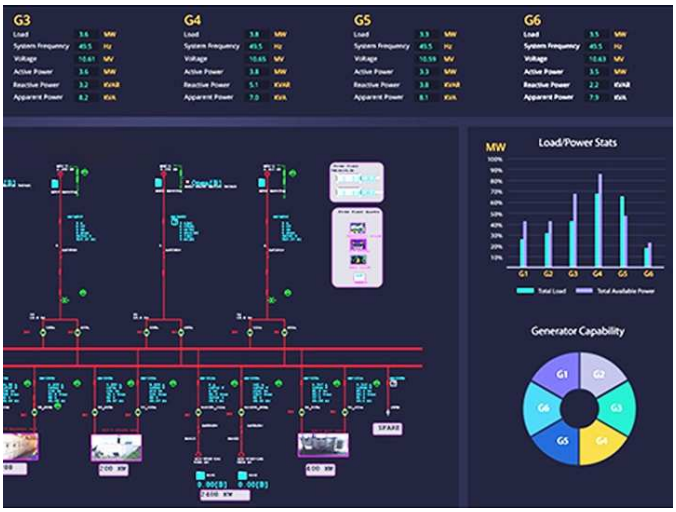


Ilustración 9 Ejemplo SCADA

Fuente: https://etap.com/packages/electrical-scada [12]

En la ilustración 10 se muestra una representación simplificada de un sistema de control industrial, en el cual se encuentran desplegados dispositivos como:

- Estaciones de Ingeniería,
- Servidores SCADA,
- Servidores OPC,
- Switch de comunicaciones,
- HMI (Interfaz Humano-Máquina),
- PLC's (controlador lógico programable),
- Sistema Instrumentado de Seguridad y
- Dispositivos de campo como son válvulas, protecciones, motores, medidores, actuadores, sensores, entre otros.

Todos los dispositivos de la Ilustración 10 funcionan de manera integral a fin de automatizar las tareas del ambiente operativo facilitando la ejecución de estas.

Estas tareas por lo general son controladas mediante una lógica programada en los PLC, los cuales poseen una interfaz gráfica en un HMI esto proporciona al operador visibilidad de valores del equipamiento industrial y la capacidad de realizar cambios sobre los mismos.

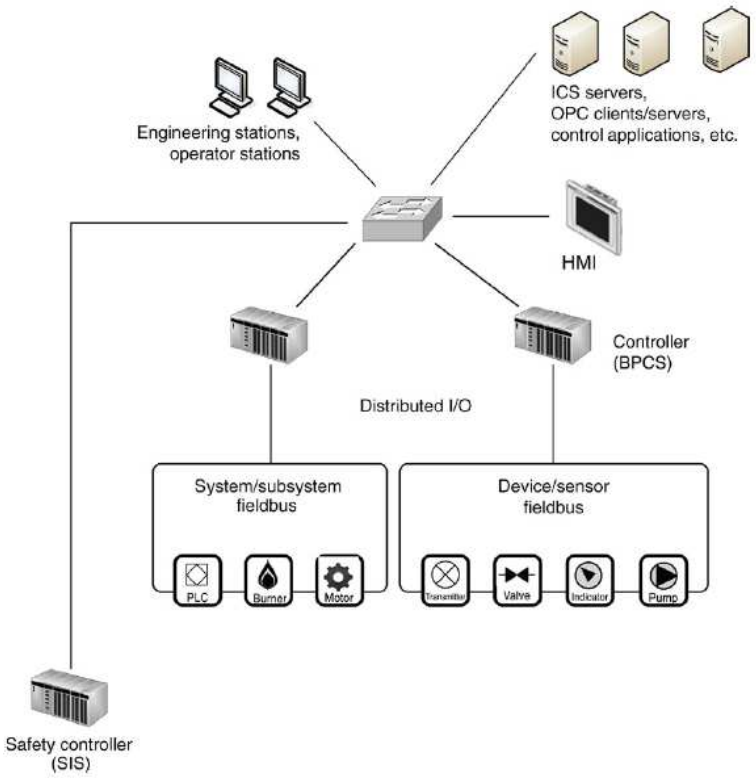


Ilustración 10 Esquema de Arquitectura de un ICS

Fuente: [3, p. 14]

Sistemas de Control en la Industria Energética

Los sistemas de control utilizados en el sector de la energía son también conocidos por varios autores como *"Smart Gris"* [3] el cual forma parte de un proceso de modernización de los sistemas de transmisión, distribución y consumo de energía. El principal objetivo del *Smart Grid* es mejorar los sistemas *legacy* actualmente instalados en estas infraestructuras, a partir de la adición de sistemas de monitoreo, transmisión energética, medición de consumo y automatización. A partir de la utilización de estos sistemas, los involucrados en este proceso se ven beneficiados. Algunos de los beneficiados, se detallan a continuación:

- **Productores de energía:** la innovación de estas infraestructuras, brindan capacidades más precisas de demanda y respuesta para la generación de energía a los productores de energía.
- **Proveedores de energía:** Smart Grid, permite que los proveedores de energía puedan mejorar sustancialmente la gestión de sus procesos

de transmisión, distribución, aislamiento y recuperación de fallas.

- **Consumidores de energía:** Estos nuevos sistemas de control permiten que los usuarios finales tengan una mejor gestión y supervisión de la energía utilizada en sus hogares, oficinas, entre otros.

Sin embargo, en contraste con estos beneficios, la modernización de estos sistemas también trae consigo una serie de consecuencias. Esto debido a que los dispositivos que lo conforman al volverse “inteligentes” se ven expuestos a nuevos riesgos de privacidad ya que se convierten en una fuente de comunicación digital. Estas comunicaciones digitales representan también un riesgo de ciberseguridad para la infraestructura crítica pues al estar automatizados la disponibilidad de las operaciones podría verse afectada en caso de la existencia de un ciberataque.

Como parte de las operaciones de un *Smart Grid* es necesario que varias funcionalidades converjan e interactúen entre sí. Esto quiere decir que, “existen distintos activos de control y protocolos que se encuentra interconectándose, convirtiendo a esta en un nexo de distintas redes industriales” [5].

Dentro de las operaciones de un *Smart Grid,* podemos encontrar varios sistemas interconectados, de los cuales se puede destacar:

- sistemas de información del cliente
- sistemas de respuesta a demanda
- sistemas de facturación
- sistemas de gestión de medidores
- sistemas de gestión de distribución
- sistemas de protección
- sistemas de automatización de subestaciones
- entre otros.

También suele estar interconectado con el sistema de infraestructura de medición avanzada (AMI), el cual a su vez alimenta la distribución local y

la medición. Por este motivo, el AMI se encuentra conectado a una variedad de medidores inteligentes, los cuales proporcionan monitoreo y control a los usuarios finales de la energía.

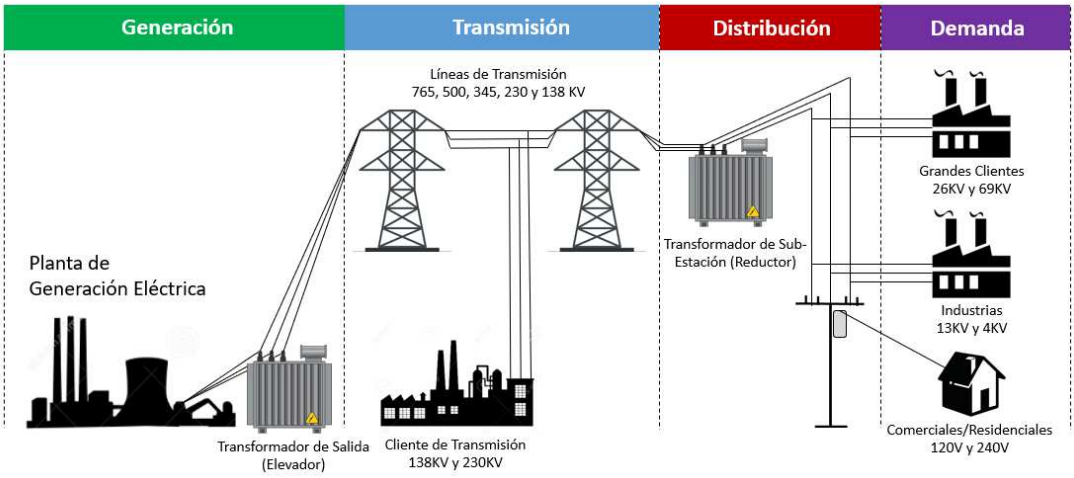


Ilustración 11 Arquitectura de una Infraestructura Crítica Energética

Fuente: Elaboración Propia

Capítulo 2: Ciberataques sobre Infraestructuras Críticas

¿Qué es un Ciberataque?

CheckPoint define un ciberataque como “un asalto lanzado por usuarios mal intencionados que usan una o más computadoras contra una o varias computadoras o redes. El impacto de un ciberataque puede deshabilitar las computadoras, robar datos o usar una computadora infectada como punto de lanzamiento para otros ataques.” [13] En un ambiente industrial un ciberataque tendría un impacto más profundo, puesto que las operaciones pueden ser detenidas e incluso puede llegar a peligrar físicamente la infraestructura.

Estadísticas Generales de Ciberataques Infraestructuras Críticas

De acuerdo a una investigación llevada a cabo por la empresa de seguridad Kaspersky durante un período comprendido entre la primera mitad del 2017 y la primera mitad del 2018 demostró que existen nuevas vulnerabilidades que afectan a distintos componentes de un sistema de control industrial. De la misma forma, se pudo verificar que las infraestructuras críticas ubicadas en la región sureste de Asia es la región más afectada completando un total de 62% de sus dispositivos vulnerados.

Así mismo fue posible evidenciar que en la región Latinoamericana se vieron incrementadas las vulnerabilidades durante el primer semestre del 2018 con un 45% de amenazas detectadas respecto a lo observado en el segundo semestre del 2017 con 38% de amenazas detectadas. [14]

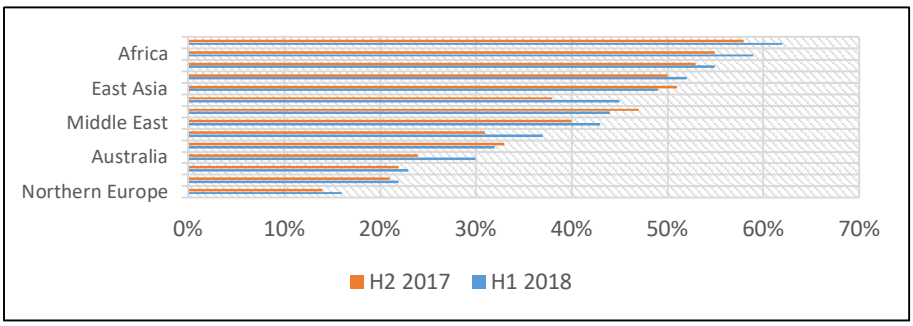


Ilustración 12 Regiones más atacadas durante el período 2017-2018

Fuente: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf [14]

Por otra parte, de esta investigación se pudo demostrar que las principales fuentes de infección que afectan a las computadoras que se encuentran desplegadas en el entorno de una red industrial son internet, medios de almacenamiento extraíble y correo electrónico en este orden respectivamente.

Esto puede ser verificado observando que Internet con un 27.3% es la principal fuente de infección en una computadora, seguidos por un 8.4% que representa la amenaza de dispositivos de almacenamiento extraíble y por último los correos electrónicos con un 3.8% se muestran como una de las principales fuentes de infección. [14]

La investigación, también desveló que los actores maliciosos continúan atacando sitios web legítimos que poseían vulnerabilidades en sus aplicaciones. Los atacantes aprovechan estas vulnerabilidades para alojar malware en estos sitios. [14]

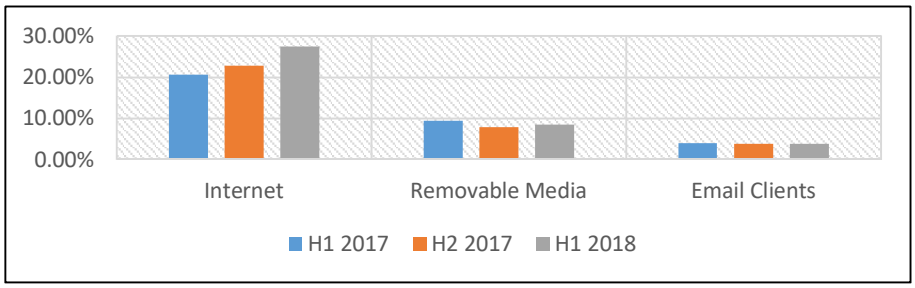


Ilustración 13 Principales fuentes de infección de un ICS

Fuente: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf [14]

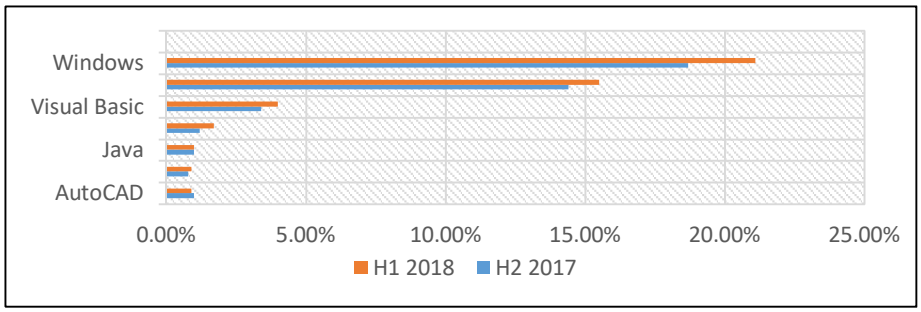


Ilustración 14 Aplicativos más utilizados como métodos de propagación

Fuente: https://ics.kaspersky.com/media/2018-Kaspersky-ICS-Whitepaper.pdf [14]

Ataques más conocidos a Infraestructuras Críticas de Energía

Stuxnet

Stuxnet es una variante de malware que originalmente fue creado para

infiltrarse dentro de instalaciones nucleares en Irán. Sin embargo, con el paso del tiempo ha mutado y se ha dirigido a otras instalaciones industriales de generación de energía. Este malware fue descubierto en el año 2010 y obtuvo gran atención de los medios ya que fue el primero de su tipo que era capaz de destruir equipamiento de hardware. Se cree que Stuxnet “se infiltró dentro de la instalación nuclear mediante dispositivos USB y una vez que fue conectado a una computadora el virus empezó a propagarse a través de la red industrial. Una vez dentro de la red industrial, el virus detectó las estaciones de ingeniería que eran capaces de programar los PLC para actualizar sus códigos. Estos códigos contenían instrucciones que inducen daños al equipo, mientras tanto enviaba paralelamente falsos comentarios al controlador principal a fin de evitar su descubrimiento. Se cree que *Stuxnet* fue capaz de destruir numerosas centrifugadoras en la instalación de enriquecimiento de uranio de *Natanz* en Irán al provocar que estos se quemen.” [15]

BlackEnergy

En diciembre de 2015, la red de energía eléctrica presentó una interrupción cerca de 6 horas de duración, dejando aproximadamente a la mitad de la región *Ivano-Frankivsk* de Ucrania sin energía eléctrica. Según varios informes “este incidente se produjo debido a un ciberataque, que causó que las subestaciones se desconectaran de la red. El malware asociado a este ciberataque es conocido como *BlackEnergy* y en un principio fue diseñado para lanzar ataques de Denegación de Servicios que están diseñados para evitar que un usuario legítimo pueda acceder a un servicio” [16]. Sin embargo, con el pasar del tiempo este malware ha adquirido nuevas capacidades y se cree que aún puede seguir operando.

Vectores de Amenazas sobre Infraestructuras Críticas Energéticas

Las infraestructuras críticas de generación de energía se pueden ver comprometidas, principalmente debido a la interconexión con redes inteligentes. Por ejemplo, una infraestructura de medición avanzada puede verse expuesto a las siguientes amenazas:

- Denegación de servicio: Un atacante puede hacer uso de nodos inteligentes para comunicarse con otros nodos masivamente, con el objetivo de saturar los canales de comunicación y evitar que el sistema funcione según lo diseñado.
- Manipulación de facturas / robo de energía: Un consumidor de energía puede ser capaz de manipular la información de facturación para obtener energía gratuita.
- Acceso no autorizado: Un consumidor puede hacer uso de un medidor inteligente u otro dispositivo conectado a la red, para obtener acceso no autorizado a la red de comunicaciones.
- Interferencia en las telecomunicaciones de servicios públicos: Un usuario no autorizado puede utilizar las interconexiones de este sistema de control a fin de penetrar en el sistema de generación, transmisión y distribución eléctrica.

Estos sistemas de control son un objetivo ideal de ataque, pues su interconexión con medidores accesibles desde el hogar por lo general posee interfaces inalámbricas o infrarrojas pueden permitir un acceso no autorizado.

De la misma forma, este sistema de control al encontrarse interconectado con varios sistemas (comerciales, operativos y de control) causaría que el mismo tenga una superficie de ataque más amplia. Esto debido a que, si alguno de estos sistemas se viera comprometido, se podría saltar al sistema de control objetivo.

Importancia de Segurizar las Redes Industriales

El único método por el cual un sistema de control industrial se puede ver expuesto a ciber-amenazas externas es mediante la interconexión que existe entre las redes industriales y las redes corporativas y recursos empresariales.

Muchos sistemas industriales se construyen utilizando dispositivos *legacy* y los mismos ejecutan protocolos *legacy*, sin embargo, en algunos casos estos protocolos han evolucionado a fin de poder operar en redes enrutables. “Los sistemas de automatización se crearon mucho antes de la

proliferación de la conectividad a internet, las aplicaciones web y sistemas de información empresarial. Sin embargo, en su momento la seguridad de la información no era una prioridad debido a que los sistemas de control tenían una separación física de los sistemas de corporativos" [4]. Pero actualmente esta separación rara vez existe, ya que a principios de la década de 1990 las organizaciones optaron por realizar una integración entre los sistemas de control industrial y las aplicaciones comerciales típicas tales como los sistemas de planificación de producción. A su vez, la necesidad de compartir información en tiempo real estableció un enlace entre la red industrial y corporativa.

En los primeros años que se realizaban estas integraciones, la seguridad de la información no era una prioridad por lo que no existía un aislamiento de red robusto. Sin embargo, con el paso del tiempo las organizaciones empezaron a verificar las diferencias operativas que existían entre las redes corporativas y redes industriales, lo cual motivó la implementación de medidas de seguridad como firewalls para bloquear todo el tráfico de red, a excepción del tráfico que era absolutamente necesario para mejorar la eficiencia de las operaciones comerciales. El principal problema que presenta esto, es que, aunque se encuentre implementada esta medida de seguridad, el aislamiento físico ya no existe, por lo cual existe un camino hacia los sistemas de control industrial y los mismos pueden ser encontrados y explotados por los atacantes.

Durante el año 2010 se realizó una investigación a cargo de la firma de servicios de Ciberseguridad Red Tiger. La misma buscaba indicar el estado de ciberseguridad de las redes industriales en infraestructuras de generación eléctrica de América del Norte mediante la ejecución de pruebas de penetración sobre 100 instalaciones aproximadamente. Esta investigación arrojó cerca de 38000 advertencias de seguridad y vulnerabilidades. Estos resultados demostraron lo que estaba previsto, verificando que el estado de ciberseguridad de estas instalaciones estaba atrasado respecto a otras industrias.

Una vez realizado un análisis a profundidad de esta información, se mostró que el número promedio de días entre el momento en que se desveló

una vulnerabilidad y el momento en que esta fue descubierta en el sistema de control fue de 331 días. Incluso se observaron casos donde la vulnerabilidad tenía más de 1100 días de antigüedad hasta que fue descubierta en el sistema de control. [17]

Estos casos fueron descubiertos en varias instalaciones de generación de energía eléctrica y demuestra que existen vulnerabilidades conocidas con exploits disponibles en internet. Estos exploits pueden ser utilizados por ciber-atacantes utilizando herramientas de código abierto como Metasploit para permitir la entrada de estos a las redes que administran los sistemas de control. La explotación de estas vulnerabilidades puede realizarse de manera sencilla y pueden ser ejecutados por una amplia audiencia.

Estas vulnerabilidades existen en los sistemas de control en gran parte debido a que los mismos son por diseño, difíciles de parchar. Una de las principales complicaciones al momento de parchar es la limitación de acceso a redes externas e internet que existe en las redes industriales, esto dificulta la obtención de los parches necesarios. Así mismo, otra complicación que se puede presentar es que una vez obtenidos los parches se debe esperar hasta que exista una ventana de mantenimiento planificada para aplicarlos, pues la disponibilidad de estos sistemas es primordial. [17]

Capítulo 3: Medidas de Salvaguardas contra Ciberataques

Principales Estándares de Ciberseguridad Industrial

ISA99 / IEC62443

La Sociedad Internacional de Automatización los define como “una serie de estándares con un amplio alcance de uso para entornos ICS / OT / SCADA” [18] , desarrollados por dos grupos:

- ISA99: ANSI/ISA-62443
- IEC TC65/WG10: IEC 62443

Estos estándares cuentan con un alcance internacional y los requisitos de contribución provienen de otros estándares como NERC-CIP, NIST, entre otros. Así mismo, facilita un framework flexible que sirve de base para estándares nacionales. El comité de la ISA99 (Industrial Automation and Control Systems Security) está conformado por más de 500 miembros autorizados para representar a compañías (alrededor del mundo) en sectores industriales, como:

- Procesamiento químico
- Petróleo (refinerías)
- Alimentos y bebidas
- Energía
- Productos farmacéuticos
- Agua

El comité ISA99 se ocupa de establecer estándares que reduzcan el riesgo de que los sistemas de control y equipos de automatización industrial resulten comprometidos (debido a un ataque físico, ciber-ataque o infección de un malware) y origine alguno o todos los siguientes escenarios:

- Poner en peligro la seguridad pública o de los empleados
- Pérdida de confianza pública
- Violación de los requisitos reglamentarios
- Pérdida de información privada o confidencial

- Impacto económico.
- Impacto en la seguridad nacional.

Ilustración 15 Estándar ISA99/IEC62443

Fuente: https://www.isa.org/isa99/ [18]

NIST 800-82

"Es un documento que propone las guías que se deben seguir en función de asegurar los sistemas de control industrial y todos sus componentes asociados, teniendo en cuenta los requisitos necesarios para que el sistema sea capaz de ofrecer rendimiento, confiabilidad y seguridad" [19]. Así mismo, el estándar identificar las amenazas y vulnerabilidades más comunes que afectan a los sistemas de control industrial y provee contramedidas de seguridad que permitan mitigar los riesgos asociados.

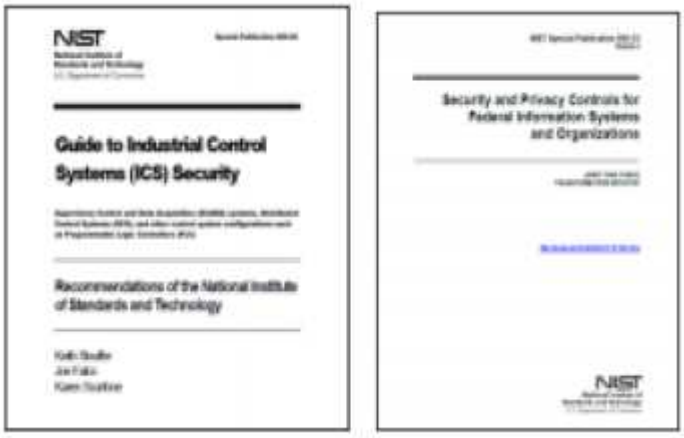


Ilustración 16 Estándar NIST 800-82

Fuente: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final [19]

NERC CIP

"La norma establece un conjunto de estándares de ciberseguridad, que el Gobierno Federal de los Estados Unidos ha definido de cumplimiento

obligatorio para las compañías relacionadas con el sub-sector eléctrico en el territorio norteamericano.” [20]

Dicha norma, en su última versión (publicada), está constituida por ocho (8) estándares establecidos desde versiones anteriores y dos (2) controles nuevos a ser aplicados de manera obligatoria. A continuación, se desglosan cada uno de ellos, con su respectivo título correspondiente:

Controles Obligatorios:

CIP-002-5 – Categorización del Cibersistema BES (Bulk Electric System)*

CIP-003-5 – Control de Gestión de la Seguridad

CIP-004-5 – Personal y Capacitación

CIP-005-5 – Perímetro de Seguridad Electrónica

CIP-006-5 – Seguridad Física de Ciberactivos

CIP-007-5 – Sistema de Gestión de la Seguridad

CIP-008-5 – Plan de Respuesta ante Incidentes de Ciberseguridad

CIP-009-5 – Plan de Recuperación de ciberactivos

Ilustración 17 Estándar NERC CIP v5

Fuente: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx [20]

A continuación, se muestran las principales medidas de ciberseguridad que se deben tomar en función de proteger los sistemas de control industrial antes las amenazas a las que se encuentran expuestos. Estas contramedidas están basadas en las recomendaciones que indican los estándares de ciberseguridad descritos anteriormente.

Programa de Ciberseguridad Industrial

Una de las principales medidas que recomienda la normativa IEC 62443 a fin de segurizar las infraestructuras críticas es desarrollar un gobierno de ciberseguridad industrial. El mismo estará encargado de definir los

lineamientos generales buscando maximizar la disponibilidad y proteger la confidencialidad e integridad de la información que es procesada y almacenad en los sistemas de automatización y control industrial.

Cabe mencionar que a diferencia de los ambientes IT, los entornos industriales tienen como prioridad maximizar la disponibilidad de las operaciones y brindar seguridad a los empleados, de tal forma que la protección de la confidencialidad e integridad de la información no representa la primera prioridad para este tipo de organizaciones.

Los lineamientos para la implementación de un programa de Ciberseguridad Industrial teniendo en cuenta la norma IEC 62443, establece los siguientes parámetros:

- Análisis de Riesgo
    - Entendimiento del negocio
    - Clasificación de riesgos.
- Implementación de un Gobierno de Ciberseguridad Industrial
    - Políticas de seguridad
    - Medidas de seguridad
    - Implementación
- Cumplimiento del programa de Ciberseguridad Industrial
    - Métricas de seguridad
    - Conformidad y plan de mejora [18]

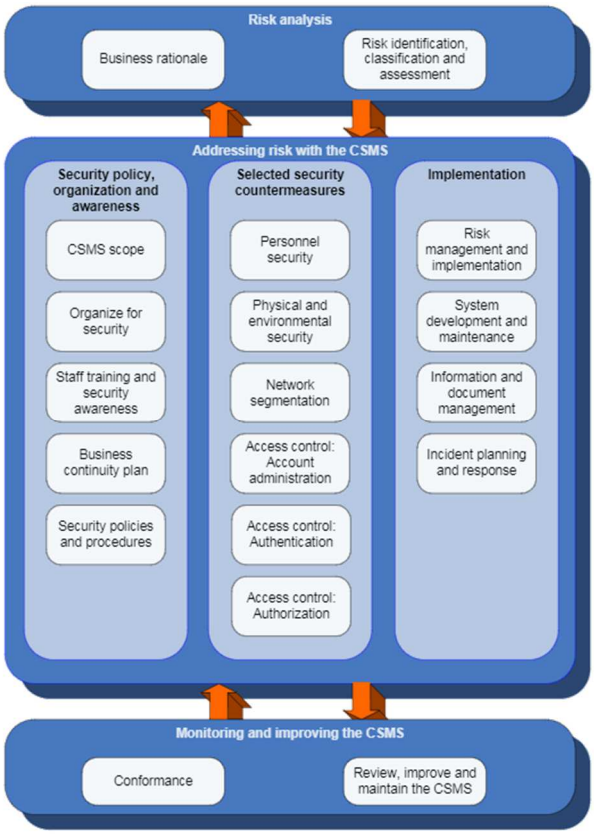


Ilustración 18 Esquema de Implementación de un Programa de Ciberseguridad Industrial

Fuente: IEC 62443-2-1 [18]

Análisis de Riesgo

Durante la etapa de análisis de riesgo se debe tomar en cuenta cuál es la lógica del negocio a alto nivel, que ayude a definir cuál es la dependencia que tiene el negocio con los sistemas de control y automatización industrial. Así mismo, como segunda fase se debe identificar los riesgos cibernéticos asociados a los sistemas de control a los que se enfrenta la organización y evaluar la probabilidad de ocurrencia y gravedad de estos. Para la evaluación de riesgos se deberá tener en cuenta lo siguiente:

- La metodología que utilizar para la evaluación de riesgos.
- Poseer un inventario de activos del sistema de control.
- Ejecutar la evaluación de riesgos a alto nivel para comprender las consecuencias en caso de que la disponibilidad, integridad y confidencialidad del sistema de control se vean comprometidas. [18]

Implementación de un Gobierno de Ciberseguridad Industrial

De acuerdo al gráfico presentado anteriormente, la fase de implementación de un gobierno de ciberseguridad industrial consta de tres etapas:

Política de seguridad, organización y concientización:

En esta etapa se procederá a identificar y evaluar los sistemas, procesos y organizaciones a los que se aplica el Gobierno, así como establecer las entidades responsables de la gestión, realización y evaluación de la ciberseguridad general de los activos del sistema de control. Así mismo, se debe establecer un programa de concientización donde se proporcione a todo el personal la información necesaria para identificar, revisar, en su caso, remediar las vulnerabilidades y amenazas al sistema de control. Por otro lado, también se debe identificar los procedimientos para mantener y/o restablecer las operaciones esenciales mientras se recupera de una interrupción significativa. También se debe establecer una política que contemple la forma en que una organización define la seguridad, opera su programa de seguridad, define y aborda su tolerancia al riesgo, y revisa su programa para realizar mejoras adicionales.

Selección de Contramedidas mitigantes:

En esta etapa se deberán establecer políticas y procedimientos para asegurar que el personal mantenga la seguridad del sistema de control de la organización durante todo el ciclo de vida de su empleo. Así mismo, se debe establecer controles que ayuden a crear un entorno seguro para la protección de los activos del sistema de control. Por otro lado, se deben agrupar y separar los activos clave en distintas zonas con niveles de seguridad para gestionar los riesgos de seguridad. De la misma forma se deben establecer controles que permitan asegurar que sólo las entidades apropiadas tengan cuentas que permitan el acceso y que estas cuentas proporcionen privilegios de acceso apropiados.

Implementación:

Durante esta etapa se pretende reducir el riesgo en los sistemas de control industrial y mantenerlo a un nivel aceptable basado en el nivel de tolerancia al riesgo de la organización. Así como, garantizar que el nivel de

tolerancia al riesgo deseado por la organización se mantenga a medida que evolucionan los activos del sistema de control, mediante el mantenimiento de los sistemas existentes y el desarrollo y adquisición de nuevos sistemas.

Además, se pretende clasificar, gestionar y presentar la información asociada a los sistemas de control y al programa de ciberseguridad industrial en el momento oportuno al personal autorizado. Así mismo, en esta etapa se busca definir cómo la organización detectará y reaccionará ante los incidentes de ciberseguridad.

Contramedidas

Como tercera categoría principal se tiene a la fase de seguimiento y mejora del programa de ciberseguridad industrial, el cual implica tanto asegurar que el programa se esté utilizando, así como como revisar la efectividad de este. Dentro de esta fase, se tiene dos etapas:

Cumplimiento:

Durante esta etapa se verifica que la organización se adhiere a sus políticas establecidas, ejecuta los procedimientos en el momento correcto y elabora los informes apropiados para permitir su revisión en el futuro

Revisar, mantener y mejorar el programa:

Durante esta etapa se establece una supervisión continua del programa de ciberseguridad industrial para comprobar que funciona eficazmente y para gestionar los cambios necesarios a lo largo del tiempo. [18]

Defensa en Profundidad

La organización ICS_CERT, menciona que “todas las organizaciones en las cuales se cuente con un sistema de control industrial deben implementar una estrategia de defensa en profundidad. Esta estrategia define una serie de barreras defensivas de forma escalonada. Es decir que cada nivel que compone el sistema de control industrial posea medidas de seguridad que mitiguen posibles vulnerabilidades o amenazas” [21]. El término Defensa en Profundidad se relaciona con medidas de detección y

protección diseñadas para impedir el progreso de un ciber-atacante mientras brinda una brecha de tiempo a la organización para que pueda responder a la intrusión con objeto de reducir y mitigar las consecuencias de este incidente. Esta estrategia está basada principalmente en un enfoque holístico que le permite proteger todos los activos del sistema de control, teniendo en cuenta sus interconexiones y dependencias utilizando los recursos disponibles con los que cuenta la organización proporcionando de esta manera niveles de protección basado en la exposición del sistema de control a los riesgos de ciberseguridad. Para que esta estrategia sea efectiva dentro del entorno de un sistema de control, la organización responsable debe comprender la relación entre las amenazas y las vulnerabilidades. Por ejemplo, un atacante representa una amenaza para un sistema de control al comprometerlo utilizando vulnerabilidades existentes en sus operaciones, personal y/o tecnología utilizada.

Todas las salvaguardas que proponen las mejores prácticas y estándares ayudan a proteger los activos críticos del sistema de control siempre y cuando estas sean aplicadas a través de distintas capas de defensa. A continuación, se presenta un ejemplo de cuáles son las medidas que se deben adoptar para proteger cada una de las capas que conforman el sistema de control industrial.

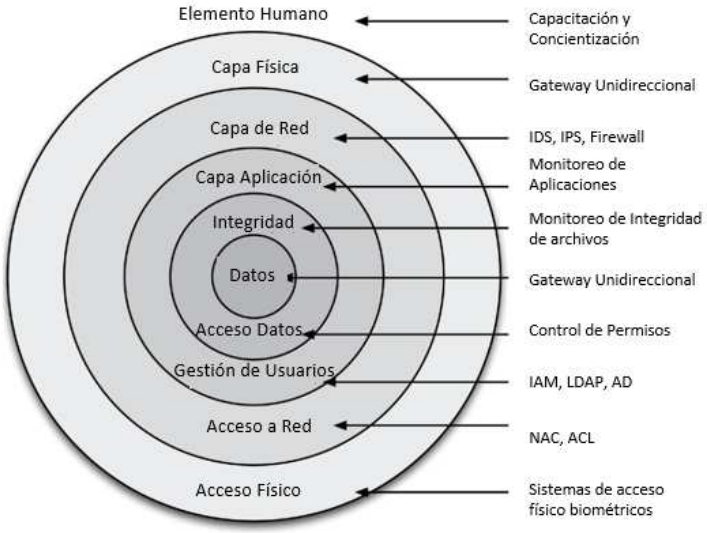


Ilustración 19 Concepto de Defensa en Profundidad

Fuente: Elaboración Propia

En la Ilustración 20, se muestra cuales son los elementos que mínimamente deben ser considerados cuando se esté confeccionando una estrategia de Defensa en Profundidad.

Elementos de una estrategia de Defensa en Profundidad	
Programa de Gestión de Riesgos	• Identificar Amenazas • Caracterizar el riesgo • Inventario de Activos
Arquitectura de Ciberseguridad	• Recomendaciones/Estándares • Políticas • Procedimientos
Seguridad Física	• Control de acceso al centro de control • Control de acceso, barreras
Arquitectura de Red ICS	• Arquitectura común de zonas • DMZ • LAN Virtuales
Perímetro de Seguridad de Red ICS	• Firewalls • Acceso remoto y autenticación • Equipos de Salto
Seguridad del Host	• Gestión de Parches y Vulnerabilidades • Equipos de campo • Máquinas virtuales
Monitoreo de Seguridad	• IDS • Auditoría de logs • Monitoreo de eventos e incidentes
Gestión de Proveedores	• Gestión de la cadena de suministro • Tercerización • Nube
Elemento Humano	• Políticas • Procedimientos • Capacitación y Concientización

Ilustración 20 Elementos de una estrategia de Defensa en Profundidad

Fuente: Elaboración Propia

Programa de Gestión de Riesgos

De acuerdo a distintos autores, la implementación de una estrategia de *Defense-in Depth* "ayuda a mejorar la postura de ciberseguridad de una organización" [21] . Esta estrategia debe comenzar realizando un análisis a profundidad acerca de la comprensión del riesgo corporativo asociado a la ciberseguridad. Este riesgo debe ser gestionado acorde al apetito de riesgo corporativo que esté definido en la organización.

Para que sea posible administrar y mantener la funcionalidad operativa de los sistemas de control acorde al apetito de riesgo definido, los operadores responsables del sistema de control necesitan conocer cuáles son los procedimientos definidos para evaluar e identificar un riesgo de ciberseguridad. De esta forma, una vez que han sido identificadas cuáles son las amenazas a las que está expuesto el negocio, los procesos operativos del sistema de control, la tecnología utilizada dentro del mismo y sus requisitos

técnicos y funcionales, la organización es capaz de incorporar una estrategia de defensa en capas para el monitoreo y protección de la ciberseguridad de la funcionalidad operativa del sistema de control involucrado.

Otro pilar importante para que el despliegue de esta estrategia tenga un resultado eficaz es la voluntad del personal operativo del sistema de control, pues es necesario que estos vean a la seguridad como un facilitador para todas las actividades orientadas al uso de computadores y su capacidad de aplicar medidas de control de seguridad orientada a su tecnología operativa.

Un sistema de control en su mayoría se encuentra desplegado en una infraestructura crítica, por lo cual el análisis de riesgo de estos debe contemplar las posibles consecuencias que provocaría en el mundo real la efectivización de un riesgo. Este análisis debe ser bien comprendido por todas las personas que comprenden cada uno de los niveles de la organización a fin de que estos sean capaces de participar activamente en el proceso de gestión de riesgos.

Para una gestión de riesgos efectiva, se debe considerar el siguiente proceso:

Ilustración 21 Elementos de un programa de gestión de riesgos

Fuente: Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies [21]

Inventario de Activos

El desarrollo de un inventario de activos completo permitiría a la organización tener una comprensión entre todos los interesados con la

infraestructura de soporte (IT/OT). Para este fin la organización deberá identificar los sistemas donde se incluya las operaciones, el equipamiento del proceso, el software, las redes involucradas y el personal a fin del sistema de control y analizar las dependencias para comprender tanto la función del activo en sí como los recursos necesarios para soportar funciones críticas.

Las organizaciones deben combinar diagramas de red, el inventario físico y una comprensión de los flujos de información, a fin de determinar los niveles de protección para cada sistema y los controles que deben implementarse para proteger el sistema sin comprometer ni degradar su rendimiento.

Categorizar la criticidad de los activos

Para determinar la criticidad de un activo, él o los propietarios de este deben realizar una categorización de seguridad en función del impacto potencial (bajo, moderado o alto) que podría generar la ocurrencia de un evento que ponga en peligro la capacidad de la organización para cumplir su misión, proteger sus activos y personal y mantener su operación estable. De esta forma se podrá obtener con más detalle cuáles son los activos a los que se debe prestar especial atención cuando se esté aplicando las medidas de seguridad correspondientes.

Identificar riesgos de seguridad

Para definir cuál es la exposición al riesgo de un sistema de control, es necesario que la organización pueda identificar cuáles son las amenazas potenciales y las vulnerabilidades a las que se encuentra expuesto el sistema de control. Este análisis de riesgo por lo general debería ser realizado por los gerentes y operadores de línea pues estos entienden con mayor profundidad cual sería el impacto en el sistema de control, si este se viera comprometido por una amenaza.

Determinar el impacto potencial

A fin de obtener el impacto potencial, la organización debe estimar la probabilidad de que un atacante realice una amenaza o explote una vulnerabilidad de un activo que forma parte de sistema de control. Para este análisis también se debe tener en cuenta cuales son los medios utilizados

para la explotación de estas amenazas, así como los requisitos para el acceso al activo, configuraciones de seguridad y zona de seguridad de red donde se encuentra el activo (alta o baja).

Identificar y adaptar controles

El gerente del área de seguridad de la información de la organización debe establecer controles de seguridad estándares para los sistemas en función de la criticidad del mismo y tomando en cuenta las recomendaciones del personal operativo y administrativo de los ambientes IT y OT.

Implementar controles de seguridad

La implementación de las medidas de seguridad antes definidas debe ser aplicada en base a la prioridad de los sistemas de control, es decir los sistemas más críticos deberían ser la primera prioridad para aplicar las medidas de reducción y mitigación de riesgos. Las actualizaciones periódicas del sistema también pueden ayudar a la mitigación de riesgos. Sin embargo, se debe tener en cuenta que podrían existir sistemas que por sus propiedades funcionales u operativas no permitan la aplicación de una medida de seguridad. En este caso se debe considerar una variación o excepción de un control. Una variación consiste en aceptar el uso de un control compensatorio que brinde una protección similar o superior al originalmente establecido. Por otro lado, las excepciones del control existen cuando la organización determina que la medida no se aplicará por razones comerciales establecidas, en este caso la organización deberá asegurarse que el personal apropiado revise y acepte el riesgo de no aplicar un control de seguridad. Estas excepciones deben ser revisadas periódicamente a fin de abordarlas de manera oportuna.

Monitorear y ajustar

Debido a que las organizaciones no mantienen estáticos los sistemas de control durante el tiempo y tomando en cuenta que las operaciones y las amenazas evolucionan constantemente, es necesario mantener un programa de monitoreo a lo largo del tiempo para garantizar la protección continua del sistema. A tal fin, los propietarios de los activos deberán evaluar el estado de implementación de los controles periódicamente durante el ciclo de vida de desarrollo del sistema. Estas evaluaciones permitirán tener indicadores que

muestren si los controles están funcionando acorde a lo previsto. De estas evaluaciones también puede surgir la necesidad de aplicar controles adicionales que permitan reducir más el riesgo.

Seguridad Física

Los controles de seguridad física pueden ser activos o pasivos que permitan limitar el acceso físico a cualquier activo de información que se encuentre bajo propiedad del entorno del sistema de control industrial. Estos controles permiten evitar un impacto no deseado, como los siguientes:

- Introducción no autorizada de nuevos sistemas
- Acceso físico no autorizado a ubicaciones sensibles
- Modificación física, manipulación, robo u otra eliminación, o destrucción de sistemas existentes
- Observación visual no autorizada de activos de información confidencial
- Introducción no autorizada de dispositivos para causar manipulación de hardware, escuchas de comunicaciones como dispositivos USB, punto de acceso inalámbrico o dispositivo celular.

Aplicar medidas de seguridad física permitirá reducir el riesgo de pérdidas o daño accidental de los activos de la organización y el entorno asociado. Entre los activos que la seguridad física busca proteger están los siguientes:

- Herramientas y equipos de planta
- Medio ambiente
- Propiedad intelectual (datos de la propiedad, configuraciones del proceso, información del cliente, entre otros.)
- Personal operativo

A fin de proteger el perímetro donde se encuentra la infraestructura energética se puede utilizar cercas, zanjas anti-vehículos, montículos de tierra, muros reforzados, personal de guardia, puertas, entre otros [20].

De la misma forma, si se implementa un sistema de control de acceso

físico, se debe verificar que este sea altamente confiable, es decir que solo otorgue acceso a las personas que puedan confirmar quienes dicen ser. Usualmente las personas deben usar algo que tienen, como tarjetas de acceso; algo que saben, como una clave PIN; o algo que son, como huellas biométricas.

También es recomendable utilizar sistemas de monitoreo de acceso, como son cámaras de video, sensores, entre otros. Estos dispositivos son utilizados para registrar la presencia física de individuos y pueden alertar acerca de un acceso no autorizado.

Arquitecturas de red ICS

La convergencia existente entre los sistemas de control industrial y los componentes del entorno corporativo introduce vulnerabilidades que los propietarios de los activos deben abordar antes que estas vulnerabilidades puedan ser explotadas por actores maliciosos. Los factores importantes que pueden ser aprovechados para comprometer las redes industriales son los siguientes:

- Conexión mediante enlaces inseguros a redes internas y externas.
- Tecnologías utilizadas dentro del ámbito de control que poseen vulnerabilidades conocidas.
- Falta de comprensión de los requisitos a tener en cuenta antes de establecer un enlace entre el dominio corporativo y de control.

El aislamiento existente en tiempos anteriores permitía a las organizaciones tener a sus sistemas de control amenazadas solo por riesgos relacionados a accesos físicos no autorizados a la planta. Sin embargo, interconectar una arquitectura de IT con una red aislada puede presentar distintos conflictos, por lo cual a fin de abordarlos la Sociedad Internacional de Automatización propone una arquitectura integrada entre los ámbitos industriales y corporativos [18]. Esta representación puede ser observada en la siguiente ilustración.

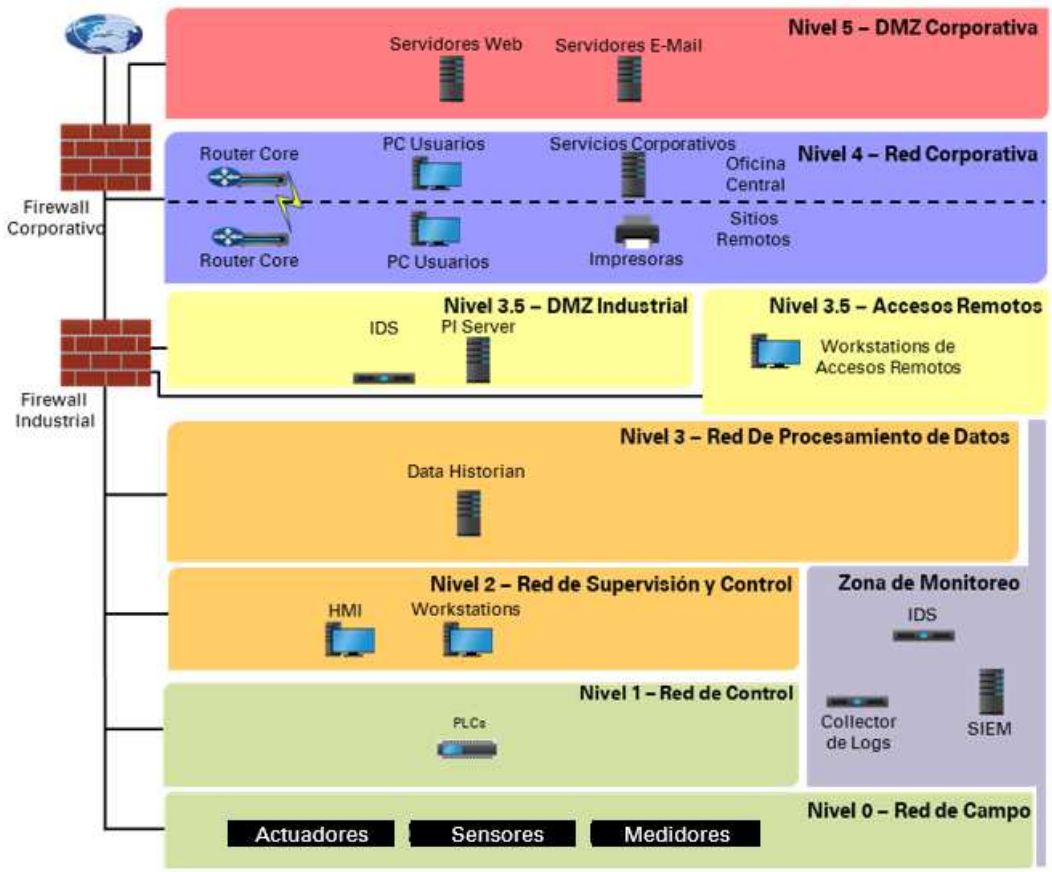


Ilustración 22 Arquitectura del modelo Purdue de segmentación de redes

Fuente: Elaboración propia

- Nivel 5: En este nivel se deben ubicar los sistemas que tengan contacto directo con internet como servidores web, email, entre otros.
- Nivel 4: En este nivel se deben ubicar los sistemas necesarios para el negocio, como aplicaciones corporativas.
- Nivel 3.5: En este nivel se deben ubicar todos los sistemas que serán accedidos por los usuarios de la red corporativa
- Nivel 2 y 3: En estos niveles deben ubicarse los colectores de datos del ICS, workstations y servicios IT que den soporte a la red (DNS, DHCP, AD, entre otros)
- Nivel 0 y 1: En estos niveles deben ubicarse los dispositivos de campo con sus respectivos dispositivos controladores (PLCs) o censadores de variables (RTUs).
- La zona de monitoreo contendrá equipos colectores de eventos que monitorearán los eventos de los dispositivos ubicados en los niveles 0, 1, 2 y 3.

- DMZ por sus siglas en inglés (Demilitarized Zone) es una subred física o lógica que contiene los servicios externos de una organización y los expone a una red no confiable como internet. La DMZ agrega una capa adicional de protección a la red local de la organización, pues si un usuario no autorizado obtiene acceso directo a un equipo que se encuentra dentro de la DMZ, este no será capaz de desplazarse a otra parte de la red.
- LAN Virtuales (VLAN) es una red local virtual que permite dividir las redes físicas en subredes lógicas más pequeñas que son utilizadas para aislar el tráfico entre subredes. Existen dos categorías de VLAN que serán explicadas a continuación:
    - Dinámicas: Son VLAN que se configuran automáticamente en función de direccionamiento IP o direcciones MAC.
    - Estáticas: También conocidas como VLAN basadas en puertos, ya que estas son asignadas a puertos específicos de un switch.

  En una arquitectura de un sistema de control industrial las VLAN son utilizadas para segmentar funcionalidades y capacidades de red. Por este motivo, las mejores prácticas recomiendan descomponer cada uno de los dominios operativos o líneas de proceso en segmentos y zonas más pequeñas a fin de facilitar la administración de estos.

Perímetro de seguridad del sistema de control industrial.

El perímetro de seguridad del sistema de control industrial abarca tanto la parte física como la lógica. En lo que respecta a la parte lógica del sistema de control industrial, antes de implementar medidas de protección de red se debe comprender claramente donde se encuentra el límite de comunicaciones, es decir que se debe identificar qué puntos de la red podrían ser aprovechados por agentes externos para infiltrarse en la arquitectura del sistema de control industrial. Una vez identificado, los posibles puntos vulnerables de la red, se puede aplicar el mecanismo de control que más se adecúe a la vulnerabilidad a fin de reducir el riesgo de esta. Entre los controles de seguridad lógica que se pueden aplicar están los siguientes:

- Mecanismos de autenticación.

- Controles de lista de acceso configuradas en los dispositivos de la red.
- Sistemas de detección/prevención de intrusiones (IDS/IPS)

Por otro lado, en lo que respecta al perímetro físico del sistema de control industrial se pueden utilizar los siguientes mecanismos de control:

- Tarjetas de acceso
- Sensores de movimiento
- Monitoreo CCTV
- Fuerzas de seguridad

Perímetro de seguridad de red

La seguridad de la red de un sistema de control industrial depende de una variedad de componentes, cada uno con una función específica.

Firewall

Los firewalls son la primera línea de defensa dentro de un entorno de red ICS. Estos componentes mantienen al intruso alejado mientras permiten el paso autorizado de datos necesarios para ejecutar la organización. Por lo tanto, el concepto de segmentación de red se aplica a la red en capas para proteger los activos en todos los niveles. Estos dispositivos actúan como guardianes entre zonas, es decir, solo permitirán tráfico esencial cruce los límites de seguridad. Esto siempre y cuando las reglas que se le configuren sean las adecuadas. De otro modo, podrían pasar fácilmente usuarios no autorizados, contenido no deseado a la red. De acuerdo a varios autores, se indica que la regla principal que debe ser configurada en un firewall es *"lo que no está explícitamente permitido debe ser negado"* [22, p. 189]. Las mejores prácticas recomiendan que las reglas de firewall sean revisadas y actualizadas periódicamente puesto que un cambio mínimo en la topología de la red que no sea tomado en cuenta puede suponer un riesgo de seguridad ya que expondría a la red a nuevos vectores de ataque o vulnerabilidades.

Gateways Unidireccionales

Son dispositivos que pueden ser desplegados dentro de la arquitectura de red que permite que el tráfico se dirija en un solo sentido. Se encuentran

comúnmente implementadas en entornos de alta seguridad, donde actúan como intermediario para las conexiones existentes entre dos o más redes que poseen distintos niveles de seguridad. Por este motivo, son generalmente halladas en plantas de generación de energía eléctrica o plantas de energía nuclear.

Controles de acceso y autenticación

En un entorno donde se encuentre desplegada una red de un sistema de control industrial, existen varios usuarios que utilizan una gran variedad de sistemas de control los cuales deben permitir el acceso oportuno a los mismos según lo requieran las operaciones de la compañía.

La autenticación, autorización y prácticas de control de acceso utilizadas en entornos corporativos, no se puede implementar de la misma manera en un sistema de control industrial, ya que estos por motivos operativos deben permanecer “siempre encendidos” por lo cual no es factible que los usuarios cierren sesión y vuelvan a iniciarla. Por lo general, los propietarios de los activos pueden controlar el acceso a los ICS utilizando dos metodologías, explicadas a continuación:

- Distribuido: La administración de los accesos bajo esta modalidad, requiere que la autenticación se realice en cada sistema por separado, es decir que cada sistema debe poseer un conjunto separado de cuentas de usuario, credenciales y roles. Este enfoque por lo general ha demostrado ser una buena solución para pequeñas implementaciones de ICS. [21]
- Centralizado: Este enfoque es normalmente utilizado para administrar una gran cantidad de usuarios y cuentas. Esto lo hace mediante un sistema de autenticación central para la administración de cuentas ya sea (Active Directory o LDAP). Este sistema actúa conjuntamente con un protocolo de autenticación (Kerberos, RADIUS o TACACS) para comunicarse entre el servidor de autenticación y el sistema de control industrial deseado. [21]

Traiga su propio dispositivo (BYOD)

En la actualidad, los dispositivos informáticos como tablets, smartphones y laptops están siendo ingresados en los entornos industriales, debido a que su uso ha aumentado debido a su popularidad. Esto conlleva ciertos problemas debido a que las organizaciones típicamente no administran estos dispositivos portátiles, por lo cual las políticas de seguridad no son aplicadas a los mismos. Por este motivo, los operadores que manejan estos dispositivos tienen acceso libre al correo electrónico personal, aplicaciones de redes sociales, páginas web. Esta situación representa un riesgo inherente alto para las infraestructuras críticas. Para este caso la organización debe adoptar medidas necesarias como la implementación de un sistema de administración de dispositivos móviles para mitigar este riesgo y llevarlo a un nivel aceptable.

Seguridad del host

La seguridad a nivel de host aporta una capa adicional de seguridad al ICS. Esto debido a que el concepto de defensa en profundidad requiere que todos los hosts del ICS sean protegidos contra intrusiones no deseadas. Los requisitos de seguridad que sean detallados a continuación tienen como objetivo proteger un host durante la instalación y uso de diversos sistemas operativos y aplicativos a fin de ayudar a mantener seguras las operaciones del ICS. Para las estaciones de operaciones como HMI los requisitos que contemplan las mejores prácticas son los siguientes:

- Cambiar las contraseñas cada 30 días.
- Si es posible instalar y mantener actualizados los parches de sistema operativo y firmware.
- Elegir contraseñas seguras para todas las cuentas del sistema, y cambiar cualquier cuenta predeterminada.
- No utilizar aplicaciones innecesarias como herramientas de ofimática, correo electrónico y accesos remotos.
- Configurar logs de eventos
- Realizar copias de seguridad periódicamente

- Configurar un firewall basado en hosts.

Por otro lado, las prácticas recomendadas anteriormente, suelen no ser compatibles con otras tecnologías de control operativo como PLC, RT. Para estos casos ser recomienda tomar las siguientes medidas:

- Deshabilitar servicios innecesarios.
- Deshabilitar puertos innecesarios
- Usar bloqueo de kernel.

Las configuraciones recomendadas deben ser gestionadas activamente durante todo el ciclo de vida del sistema.

Gestión de Parches y Vulnerabilidades

La aplicación de parches y actualizaciones a un componente del ICS presenta grandes desafíos puesto que estos pueden interferir con el normal funcionamiento del ICS. Esto debido a que “los parches o actualizaciones podrían modificar la forma en que funciona un componente, dando como resultado una operatoria anómala o pérdida de funcionalidad” [5]. Por este motivo, se recomienda que los parches sean aplicados en un entorno de prueba que emule la operación normal del ICS para determinar si el parche puede traer consecuencias o no al mismo. Así mismo, antes de aplicar un parche se debe pedir la aprobación del proveedor del sistema de control, esto dificulta muchas veces las tareas de aplicación de parches. Una vez que el parche ha sido probado y verificado por el proveedor, se debe proceder a aplicar el parche durante una parada de planta, a fin de no comprometer el funcionamiento normal de la misma.

Protección de dispositivos de campo

Algunos dispositivos utilizados en campo que son antiguos como PLC, RTU, IED entre otros por lo general no son compatibles con un mecanismo de administración central que distribuya medidas de seguridad. Esto debido a que muchos de ellos por defecto no poseen las mismas capacidades de seguridad que otros componentes. Por este motivo, los administradores de la organización deben optar por brindar una protección física a estos dispositivos utilizando mecanismos como cercas, puertas cerradas y racks cerrados.

Monitoreo de seguridad

El concepto de defensa en profundidad propone utilizar “un mecanismo de monitoreo que permita alertar a los operadores ante el acceso no autorizado a los activos críticos de la organización, así como los cambios no autorizados y comportamientos anómalos” [21]. Estas alertas deben ser enviadas apenas sean detectadas pues esto ayudará a tomar medidas defensivas necesarias antes que ocurra un evento no deseado de gran magnitud. Los mecanismos de monitoreo que se pueden desplegar en un ambiente industrial son:

- Uso de servidores syslog.
- Uso de soluciones SIEM.
- Uso de soluciones de monitoreo pasivo de tráfico.

Sistemas de detección y prevención de intrusiones

Los sistemas *IDS* pueden funcionar adecuadamente en un entorno ICS típico puesto que ya existen predefinidos que componentes se van a comunicar entre sí, esto permite a la organización que utiliza un IDS monitorear y generar alarmas cuando exista una desviación de tráfico normal. Los IDS funcionan de forma pasiva, es decir solo escucha el tráfico de red y evalúa que este se encuentra acorde a la operatoria normal del ICS

Por otro lado, se encuentran los IPS que tienen un funcionamiento parecido a los firewalls. Sin embargo, estos sistemas no son recomendados puesto que tienen la capacidad de tomar acciones en caso de que reciban una alarma. Por ejemplo, podrían detener un proceso normal del ICS cuando reciban una alarma. Sin embargo, como todas las soluciones los IPS son susceptibles a obtener falsos positivos.

Registros de auditoría de seguridad

Los registros de auditoría de seguridad son a menudo utilizados para obtener información relevante acerca de la actividad que se produce en un componente del sistema de control industrial. Entre las características que se pueden obtener de los registros están:

- Inicios de sesión.

- Modificaciones de archivos.
- Uso de aplicaciones.
- Entre otros.

Estos registros son esenciales para el equipo de respuesta ante incidentes, pues le permite tener una trazabilidad correcta y pueden determinar la importancia de un posible evento. De esta manera se pueden tomar las medidas necesarias dependiendo de la criticidad del evento.

Monitoreo de incidentes y eventos de seguridad

Las tecnologías SIEM pueden soportar tanto al proceso de respuesta ante incidentes como al mantenimiento de las operaciones del sistema de control industrial. Un SIEM configurado correctamente, puede ayudar a predecir la falla de un equipo mientras proporciona información de seguridad del mismo. Dentro del SIEM, es posible configurar un nodo central el cual almacena datos de los dispositivos que conforman la red del sistema de control, sistemas operativos, registros de aplicaciones y bases de datos. Tener almacenado centralmente estos registros, agiliza el proceso de revisión de los mismos, puesto que no se debe revisar uno a uno los registros de cada dispositivo. A partir del análisis de los registros del SIEM se puede elaborar un informe más compacto y preciso, lo cual permitirá tomar acciones correspondientes cuando se detecte un evento anómalo dentro de la red del sistema de control industrial.

Gestión de proveedores

Dentro del enfoque de Defensa en Profundidad los proveedores representan un elemento a tener en cuenta. Por este motivo, en los últimos años los proveedores han estado integrando la seguridad desde el inicio del ciclo de vida de desarrollo de los componentes que proveen. Sin embargo, aunque la gran mayoría de proveedores lo realiza, no todos adoptan este enfoque. Por lo cual, la organización debe tener en cuenta este factor y para abordar este problema se debe realizar un listado detallado de los requisitos de seguridad que deben cumplir los componentes que deseen ser agregados como parte del sistema de control.

Gestión de la cadena de suministro

La compra de tecnologías comerciales estándar aumenta potencialmente la probabilidad de recibir soluciones falsas. Además, desde el ICS-CERT se ha informado que “muchos de los componentes que ingresaron a los sistemas de control industrial desde su fabricación poseían una puerta trasera que permitía el acceso no autorizado a estos componentes” [21]. Por este motivo, la organización debe tomar en cuenta estas vulnerabilidades y realizar un control exhaustivo durante el control de calidad de los componentes antes que estos sean incorporados al sistema de control a fin de mitigar estas amenazas.

Tercerización

En las industrias, ya sean energéticas, de manufactura o petróleo es común encontrar servicios tercerizados, especialmente roles de especialistas en TI.

Para gestionar de la mejor manera la seguridad de un servicio tercerizado, es fundamental desarrollar un acuerdo de nivel de servicio (SLA), donde se detallen los requisitos, roles y responsabilidades de la empresa subcontratada. De esta forma la organización se reserva el derecho de rescindir el contrato si es que la empresa subcontratada falta a los requisitos acordados.

El elemento humano

Todas las actividades descritas previamente, no tendrían efectividad y representarían un gasto si el personal no se encuentra capacitado y concientizado, debido a que muchas veces las infraestructuras son susceptibles a errores cometidos por el propio personal los cuales exponen a la organización a distintos riesgos de ciberseguridad. Por este motivo, es necesario aplicar las siguientes medidas para tener una gestión efectiva del personal.

Políticas

Las políticas de la organización deben ser claras y describirán las reglas y controles necesarios para asegurar el desempeño óptimo del sistema de control industrial. Estas reglas y controles detallarán cuales son los

comportamientos esperados dentro del ámbito operativo y los controles. La política también deberá reflejar cuales son las sanciones que se deberán aplicar en caso de incumplimiento de la misma.

Procedimientos

Debido a la creciente integración de los ambientes IT/OT, las organizaciones deben actualizar los procedimientos de seguridad que tenían para los sistemas IT, con objeto de que los nuevos procedimientos también alcancen a los sistemas de control existentes. Estos procedimientos deben establecer la metodología que se deberá utilizar para llevar a cabo un proceso o configuraciones de un sistema de control, en función de asegurar su funcionamiento. A su vez, estos procedimientos proporcionan una metodología estándar para llevar acabo determinadas funciones. Un procedimiento de seguridad bien definido permite capacitar rápidamente al nuevo personal que se adhiera a la compañía. Los procedimientos de seguridad del ICS también abarcan instrucciones para que los operadores conozcan cuales son las tareas a realizar en caso de detectar un incidente, de manera que desde esta primera línea de defensa se pueda proteger a los sistemas de control.

Capacitación y Concientización

La organización debe desarrollar un programa de capacitación y concientización que alcance a todos los usuarios del sistema de control industrial. Este programa debe ser enfocado en brindar talleres donde se impartan conocimientos básicos acerca de las medidas básicas y acciones necesarias que deben cumplir los usuarios para asegurar la protección del sistema, así como los pasos necesarios para responder ante un incidente.

También se deberá abordar una temática que permita asegurar que los usuarios que tienen acceso al sistema de control tengan claros cuáles son sus roles y responsabilidades con respecto a ciberseguridad mientras realizan sus tareas diarias.

Conclusiones

Resumiendo, de los principales riesgos a los que se encuentra expuesto el sistema de control industrial, se puede destacar la falta de una segmentación clara entre la red corporativa y la red industrial ya que generalmente existen servicios del ámbito corporativo que son utilizados directamente desde la red industrial los cuales podrían ser utilizados por un atacante como punto de pivot para saltar desde la red corporativa hacia la red industrial y de esta forma tomar control de los sistemas involucrados en el ámbito industrial. Por este motivo, la implementación de una correcta separación de estas redes siguiendo las guías propuestas acorde al modelo Purdue para segmentación de redes podría evitar que el dominio de control pueda ser alcanzado si la red IT se viera comprometida.

A mi punto de vista, la interconexión de las redes de control con redes externas y la automatización exponencial que están adoptando los sistemas de control industrial, aumenta la superficie de ataque lo cual expone a la infraestructura a una mayor cantidad de riesgos. Por ende, la organización no puede contar con una sola medida mitigante, por esto es necesario que se apliquen múltiples contramedidas alineadas a una estrategia de Defensa en Profundidad en función de reducir el riesgo al que se encuentran expuestos los sistemas de control. Cabe mencionar que esta estrategia se utiliza principalmente para que, durante la etapa de intrusión de un atacante, el mismo tenga que realizar esfuerzos de una determinada complejidad. Además, servirán para que el equipo de ciberseguridad industrial pueda detectar y responder a las amenazas en tiempo y forma.

En base a lo identificado durante mi experiencia profesional, uno de los motivos por el cual las infraestructuras críticas se han visto comprometidas ha sido por la falta de conocimiento y desatención ya sea del personal del ámbito corporativo o el ámbito industrial respecto a ciberseguridad. Esto ha conllevado a que el personal de la organización cometa errores inconscientemente, los cuales son aprovechados por los atacantes para poder

cumplir con su objetivo. Es por esto, que un programa de concientización que refuerce los conocimientos de las mejores prácticas de ciberseguridad debe ser brindado dentro de la organización.

Una vez relatados los hallazgos mas críticos a los que se encuentran expuestas las infraestructuras críticas, debo reforzar la idea que un ciberataque a una infraestructura de generación de energía tendría un alto impacto puesto que la energía es considerada un recurso crítico y la interrupción de la misma provocaría graves consecuencias para la mayoría de las industrias productivas y usuarios finales que consumen sus servicios. Debido a esto es fundamental resaltar la importancia que tiene la ciberseguridad para las infraestructuras críticas, por lo cual su cumplimiento en los tiempos actuales se ha convertido en una necesidad para las organizaciones.

Bibliografía

[1] D. o. H. Security. [En línea].

[2] Anónimo, «Realising European Resilience for Critical Infraestructure,» [En línea]. Available: http://resilens.eu/about-resilience/critical-infrastructures/. [Último acceso: 10 09 2019].

[3] E. Knapp y J. Langil, Industrial Network Security, Massachusetts: Elsevier, 2015.

[4] Anónimo, «5 Common Vulnerabilities in Industrial Control Systems,» [En línea]. Available: https://www.lanner-america.com/blog/5-common-vulnerabilities-industrial-control-systems/. [Último acceso: 08 09 2019].

[5] R. Lee, Assessing, Hunting and Monitoring Industrial Control System Networks, Las Vegas: Dragos, 2017.

[6] D. Correa, «Qúe es un PLC y para qué sirve,» [En línea]. Available: https://intrave.wordpress.com/2015/02/20/para-que-sirve-un-plc/ . [Último acceso: 15 08 2019].

[7] Anónimo, «Remote Terminal Unit,» [En línea]. Available: https://en.wikipedia.org/wiki/Remote_terminal_unit. [Último acceso: 14 07 2019].

[8] Anónimo, «Intelligent Electronic Devices Increase Availability, Power Quality in Power Distribution Network,» [En línea]. Available: https://www.utilityproducts.com/vehicles-accessories/article/16002728/intelligent-electronic-devices-increase-availability-power-quality-in-power-distribution-networks. [Último acceso: 10 10 2019].

[9] Anónimo, «7 Things To Know About Human Machine Interface,» [En línea]. Available: https://blog.industrialmegamart.com/things-know-human-machine-interface/. [Último acceso: 10 08 2019].

[10] Anónimo, «WorkStations on Rent,» [En línea]. Available: http://mumbai.indianrenters.com/pages/workstation.php. [Último acceso: 08 10 2019].

[11] Anónimo, «Plant Data Historian Software,» [En línea]. Available: http://www.iconics-uk.com/solutions/data-historian. [Último acceso: 05 08 2019].

[12] Anónimo, «Electrical SCADA,» [En línea]. Available: https://etap.com/packages/electrical-scada. [Último acceso: 07 07 2019].

[13] CheckPoint, «What is a Cyberattack,» [En línea]. Available: https://www.checkpoint.com/definitions/what-is-cyber-attack/. [Último acceso: 02 10 2019].

[14] W. Schwab, «The State of Industrial Cybersecurity 2018,» Kaspersky, Berlín, 2018.

[15] Anónimo, «What is Stuxnet?,» [En línea]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html. [Último acceso: 25 09 2019].

[16] M. McElfresh, «Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done,» [En línea]. Available: https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802. [Último acceso: 26 07 2019].

[17] Anónimo, «Red Tiger Security "PCD Security Training v3.2",» Red Tiger Security, Manhattan, 2012.

[18] Anónimo, «ISA99, Industrial Automation and Control Systems Security,» [En línea]. Available: https://www.isa.org/isa99/. [Último acceso: 25 07 2019].

[19] S. Keith, L. Suzanne y P. Victoria, «Guide to Industrial Control Systems (ICS) Security,» NIST, Florida, 2015.

[20] Anónimo, «NERC CIP v5,» NERC, Chicago, 2017.

[21] F. E. G. Mark, «Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,» ICS_CERT, Washington, 2016.

[22] E. Ariganello, Redes CISCO. CCNP a fondo. Guía de estudio para profesionales, Madrid: RA-MA, 2015.