Universidad Cenfotec

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

Propuesta de un Modelo de Seguridad para Infraestructura de Tecnología Operacional

Estudiante:

Ugalde Ugarte Miguel Mauricio

Agosto, 2019

DECLARATORIA DE DERECHOS DE AUTOR

AGRADECIMIENTOS

Agradezco primeramente a Dios, por permitirme siempre alcanzar mis metas por sobre las adversidades. También a mi familia, por su apoyo incondicional durante este camino, especialmente a mis padres quienes siempre se han esforzado por darme una buena educación desde pequeño, por acompañarme siempre brindándome su guía y afecto, permitiéndome ser hoy un profesional formado con los mejores valores.

Quiero agradecer también a mi tutor don Arturo Ramirez, por su guía durante el desarrollo de este proyecto, y a don Claudio Valverde, por asistir a mi defensa y brindarme su colaboración como primer lector.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El auge de las tecnologías en los diversos ámbitos de la industria propicia la búsqueda de flexibilidad, escalabilidad y una mayor disponibilidad de sus servicios. Esto ha hecho que las compañías adquieran, de manera indiscriminada, todo tipo de soluciones para el control de sus procesos en aras de obtener una mayor eficiencia, sin considerar la seguridad, ni las implicaciones que estas puedan tener en caso de ser vulneradas.

La integración de estas tecnologías OT (Operational Technology) con infraestructura convencional de IT (Information Technology) es inevitable, ya que ambos entornos necesitan compartir información en tiempo real para dar flexibilidad y rapidez de actuación a la compañía. Sin embargo, en muchas ocasiones, la criticidad y especificidad del entorno industrial no permiten implantar las mismas contramedidas que en un entorno de IT tradicional, por lo que es necesario entender que estas tecnologías pueden convertirse en un problema si no se adoptan controles adecuados que aseguren el tránsito y procesamiento de la información, de forma segura.

En este contexto y al entender que los Sistemas de Control Industrial están presentes en diversos campos de la industria costarricense como refinerías, plantas de tratamiento de aguas y redes de energía, se creó un modelo ajustable a las necesidades de cada escenario. Este debía contemplar medidas básicas de seguridad a partir de los estándares internacionales y las mejores prácticas aceptadas por las grandes industrias.

Palabras Clave: OT, IT, seguro, industria.

Capítulo I. Introducción

1.1. Generalidades

El propósito de este capítulo es brindar el conocimiento general acerca de por qué surgen términos como el de Ciberseguridad Industrial y la importancia que tiene la seguridad sobre las tecnologías operacionales en las compañías. Los Sistemas de Control Industrial (ICS por sus siglas en inglés) han logrado crear ambientes de rápida adaptabilidad para las compañías, con el fin de ajustarse al entorno. Sin embargo, en los últimos años, se ha visto como cibercriminales se han aprovechado de estos sistemas con objetivos diversos que van desde atacar infraestructuras críticas, con el fin de causar daño o interrupción en las operaciones de competidores, hasta vandalismo y ciberterrorismo, cuyas repercusiones podrían causar un impacto mayor a la salud, la seguridad, el bienestar económico de los ciudadanos o el funcionamiento de las instituciones estatales y la administración pública.

En la presente entrega, se detallan los objetivos y alcances que tendrá la presente investigación la cual será *sistemática*, con el propósito de crear un modelo de ciberseguridad operativa, adaptable a las necesidades del entorno nacional, a partir de un proceso de análisis sobre guías o normas existentes y reconocidas internacionalmente.

1.2. Antecedentes del problema

De acuerdo con estudios recientes realizados por Kaspersky Labs, el 41.2 % de las computadoras que son parte de un Sistema de Control Industrial (ICS) han sido blanco de ataque al menos una vez durante la primera mitad del 2018. Este dato sugiere un incremento en los ataques con respecto al 2017 que durante la primera mitad reportó un 36.61 %. Como se indica en el informe, la mayor parte de los ataques se dan a través del Internet y son los equipos situados en países en desarrollo los que más ataques experimentaron, como se puede observar en la siguiente gráfica:

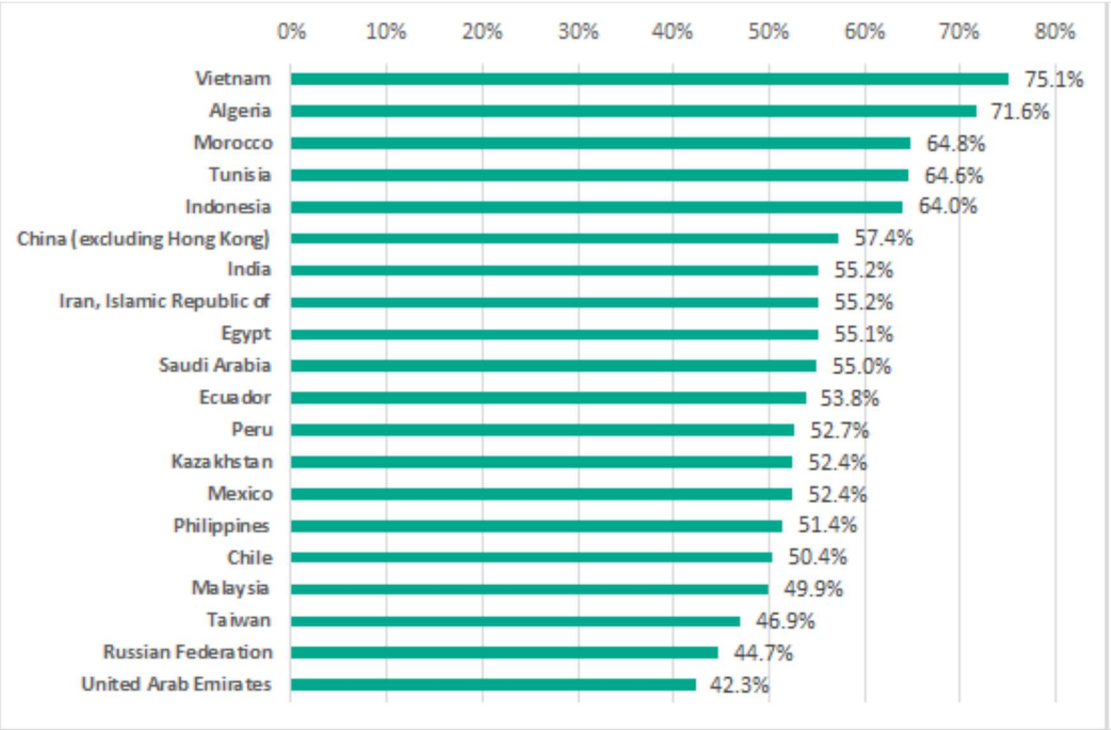

Figura 1. Threat Landscape For Industrial Automation Systems (mayor incidencia)

Fuente: Kaspersky Labs, 2018.

En contraste, en la siguiente gráfica se pueden apreciar los 10 países con la menor incidencia de ataques a Sistemas de Control Industrial (ICS) durante la primera mitad del 2018:

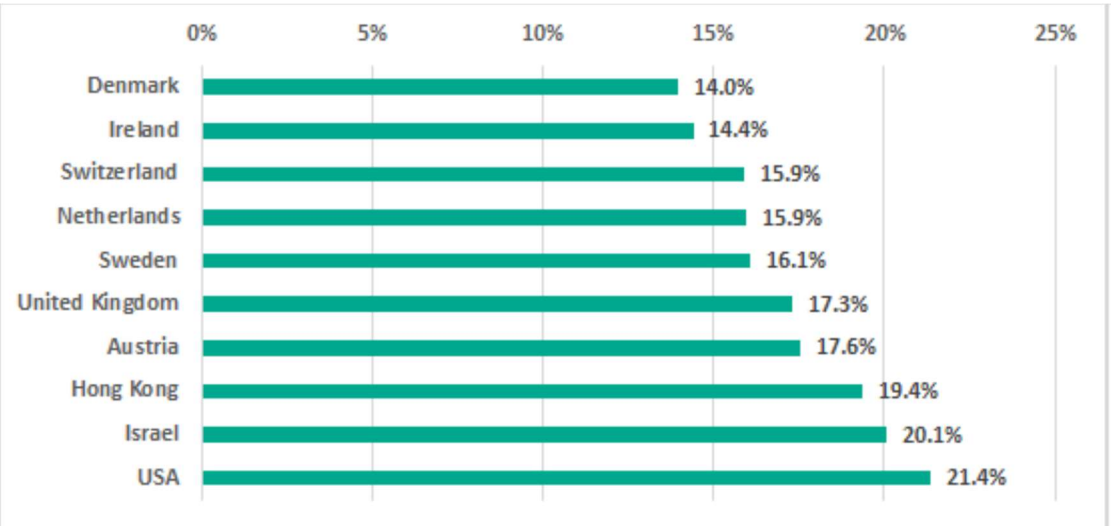

Figura 2. Threat Landscape For Industrial Automation Systems (menor incidencia)

Fuente: Kaspersky Labs 2018.

Como se indica en el informe, los principales vectores de ataque son tres (Internet, Medios Extraíbles y Correo Electrónico). En la siguiente gráfica se puede apreciar su incidencia durante los últimos tres años:

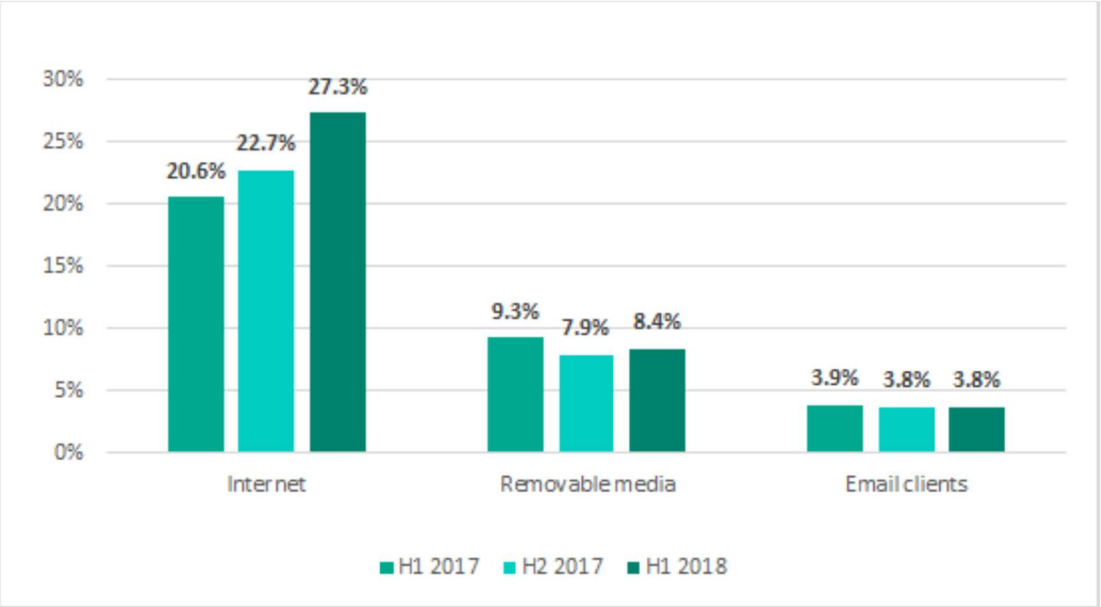

Figura 3. Threat Landscape For Industrial Automation Systems (Vectores)

Fuente: Kaspersky Labs 2018.

En la siguiente figura, extraída de un informe reciente de ITS, se puede observar una línea del tiempo con los principales ataques al sector industrial durante los últimos años:

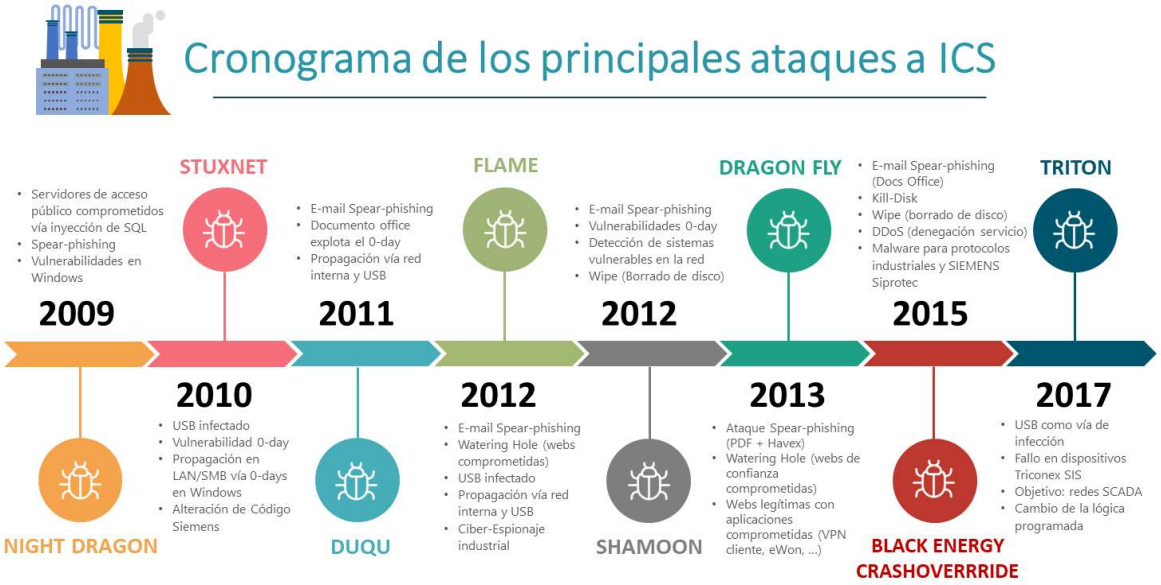

Figura 4. Ics – Principal Objetivo de los Ciberatacantes

Fuente: ITS Security, 2018.

Las redes industriales modernas difícilmente pueden considerarse redes aisladas a sistemas externos. La red industrial es necesaria, tanto para controlar los procesos internos como para proporcionar administración, a través de redes corporativas. Asimismo, la posibilidad de acceder a Internet desde la red industrial podría ser una necesidad forzada para organizaciones cuyo soporte a estos sistemas lo brinda personal contratista, de forma remota.

1.3. Definición y Descripción del Problema

La convergencia entre IT y OT es una realidad, esto gracias a que, en las organizaciones, es necesario optimizar flujos de trabajo y procesos empresariales, con el fin de mantener una eficiencia operativa. Hasta hace pocos años, estos desarrollos eran paralelos, en la actualidad, las ventajas de uno pueden aprovecharse en el otro. Por ejemplo, la evolución de los dispositivos móviles y la tecnología inalámbrica ha permitido abaratar costos de tecnología OT en procesos que, anteriormente, involucraban cableado y terminales especiales para el monitoreo. Sin embargo, no todos son beneficios, ya que los males y desventajas se transfieren de un mundo al

otro con la misma velocidad. Esto hace que el OT se enfrente a problemas desconocidos en el pasado como la seguridad.

Es posible afirmar que la criticidad y especificidad del entorno industrial no permite implantar las mismas contramedidas que en un entorno IT tradicional. De hecho, existen diferencias entre los ámbitos IT y OT que justifican la necesidad de abordar del desarrollo e implantación de programas de ciberseguridad industrial específicos que estén alineados con las políticas de seguridad IT de la organización. Es importante resaltar que el desarrollo e implantación de los programas de ciberseguridad industrial debe considerar tres pilares: sistemas, procesos y personas.

1.4. Justificación

El principal para abordar este tema es ver el crecimiento desmedido en la adopción de estos sistemas en Costa Rica, sin considerar factores básicos como la seguridad y escalabilidad de estas soluciones. En años recientes, estos han sido blanco de sofisticados ataques que buscan dañar los equipos y producir pérdidas millonarias en los diferentes sectores de la industria. Sin embargo, la interrupción de infraestructura crítica proveedora de servicios básicos como la electricidad, el suministro de agua y el transporte público, constituyen también un riesgo elevado que no se puede pasar por alto ante estas amenazas a las que está expuesta la población y que pueden provenir de cualquier región del mundo.

1.5. Viabilidad

1.5.1. Punto de vista técnico

Ser miembro de un Departamento de Infraestructura de TI ofrece una gran ventaja al conocer los entornos sobre los cuales se instauran estos sistemas. Los privilegios de administración sobre los diversos recursos de la red hacen posible la interacción directa con este tipo de tecnología y, la coordinación e implementación de soluciones previas a corta escala, ofrecen el conocimiento base para el desarrollo de este proyecto.

1.5.2. Punto de vista operativo

Laborar para una compañía que posee diversidad de sistemas de esta índole, permite aplicar el modelo desarrollado dentro de la organización, con el fin de probar si es efectivo, al mismo tiempo que se mejora la seguridad de los procesos en la organización.

1.5.3. Punto de vista económico

Como esta es una investigación que implica estándares mundialmente aceptados, con abundancia de reportes y que incluye marcos de referencia accesibles de forma gratuita a través de la *web*, se determina que no habrá que incurrir en costos económicos que deban considerarse en el desarrollo y aplicación de este proyecto.

1.6. Objetivos

1.6.1. Objetivo general

Proponer un modelo de seguridad para infraestructura OT que se adapte a las necesidades del ámbito nacional, con base en las mejores prácticas de seguridad, aceptadas mundialmente.

1.6.2. Objetivos específicos

1. Recopilar información sobre las mejores prácticas de seguridad que son reconocidas internacionalmente como estándar en la industria.
2. Proponer un modelo de seguridad ajustable a las necesidades en cada escenario.
3. Aplicar el modelo en un escenario real de negocio.

1.7. Cronograma del Proyecto

	Entregables	Octubre				Noviembre				Diciembre			
		Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8	Semana 9	Semana 10	Semana 11	Semana 12
ETAPA I	**INVESTIGACIÓN**												
	Recolección de información general sobre Sistemas de Control Industrial												
	Indagación sobre principales amenazas al sector industrial e infraestructuras críticas												
	Investigación sobre estándares, protocolos y componentes de infraestructura OT												
	Determinación de objetivos y alcance												

	Entregables	Enero						Febrero			Marzo				Abril			
		Semana 11	Semana 12	Semana 13	Semana 14	Semana 15	Semana 16	Semana 17	Semana 18	Semana 19	Semana 20	Semana 21	Semana 22	Semana 23	Semana 24	Semana 25	Semana 26	Semana 27	Semana 28
ETAPA II	**DISEÑO**																		
	Selección de muestra																		
	Instrumentos de recolección de información																		
	Traducción y análisis de información																		
	Selección de normas y prácticas de seguridad																		
	EJECUCIÓN																		
	Aplicación y documentación de resultados mostrando su uso en un escenario real de negocio																		
	PRESENTACIÓN																		
	Revisión de filologo																		
	Correcciones																		
	Envío a decanatura																		
	Preparación de presentación																		
	Defensa																		

1.8. Alcances y limitaciones

1.8.1. Alcances

El alcance de este proyecto se delimita por la investigación sobre las buenas prácticas en el manejo de tecnologías operacionales (OT). Después de recabar y analizar la mayor cantidad de información posible, se confeccionará una guía para obtener una seguridad razonable, esta contendrá las principales consideraciones y recomendaciones de seguridad para la instauración y administración de estas tecnologías. Finalmente, se aplicará el modelo en un escenario real de negocio en el que se pueda analizar su viabilidad.

1.8.2. Limitaciones

El proyecto se limita a la investigación y propuesta de un modelo que funcione como guía de seguridad en el ámbito nacional y no contempla disposiciones técnicas específicas en las leyes o regulaciones que se aplican los grandes conglomerados industriales.

1.9. Estado de la cuestión

En la actualidad, son pocos los modelos de seguridad específicos para infraestructura de Tecnología Operacional (OT) como Sistemas de Control Industrial (ICS) o sistemas de Supervisión, Control y Adquisición de Datos (Scada). A continuación, se muestran los dos modelos con más trascendencia, enfocados en plataformas de diversas industrias.

1.9.1. ISA/IEC-62443 (anteriormente ISA 99)

Uno de los principales objetivos de seguridad de esta norma es la defensa en profundidad, al extenderla desde los fabricantes hasta los operadores. La norma IEC 62443 se compone de los siguientes documentos:

IEC 62443-1-1	"Models and Concepts"	Terminología, conceptos y modelos para ICS.
IEC TR 62443-1-2	"Master Glossary of Terms and Abbreviations"	Contiene el glosario y abreviaturas utilizadas en la serie.
IEC 62443-1-3	"System Security Compliance Metrics"	Define las métricas de cumplimiento para la seguridad en los ICS.
IEC TR 62443-1-4	"Security Life Cycle and Use Cases"	Se centra en el ciclo de vida y en dar ejemplos de uso para aplicaciones típicas entre los sistemas de control.
IEC 62443-2-1	"Requirements for an IACS Security Management System"	Define los elementos necesarios para establecer un sistema de gestión de la ciberseguridad.
IEC TR62443-2-2	"Operating a Control Systems Security Program"	Aborda la operación eficiente de un programa de ciberseguridad en ICS.
IEC TR 62443-2-3	"Patch Management in the IACS Environment"	Guía práctica para llevar a cabo un programa de gestión de actualizaciones.
IEC 62443-2-4	"Certification of IACS supplier security policies and practices"	Se centra en la certificación de proveedores de productos de seguridad para los ICS.
IEC TR62443-3-1	"Security Technologies for IACS"	Ofrece una descripción de tecnologías existentes para la protección de redes y

		sistemas industriales, exponiendo sus ventajas y limitaciones.
IEC 62443-3-2	"Security Risk Assessment and System Design"	Describe los conceptos de security zone y Conduit. Indica cómo se debe llevar a cabo la segmentación siguiendo estos principios.
IEC 62443-3-3	"System Security Requirements and Security Levels"	Describe los requisitos técnicos del sistema para definir el nivel de seguridad del activo analizado.
IEC 62443-4-1	"Product Development Requirements"	Define el proceso de desarrollo que tienen que llevar a cabo los nuevos dispositivos que se creen para los ICS.
IEC 62443-4-2	"Technical Security Requirements for IACS Components"	Requisitos técnicos para mejorar la seguridad de los componentes, de forma individual, dentro de la red industrial.

Tabla 1. *Documentos que componen la Norma IEC 62443*

Fuente: elaboración propia.

1.9.2. NIST 800-82 r2

Provee una guía sobre cómo asegurar Sistemas de Control Industrial (ICS), incluye el sistema Scada, Sistemas de Control Distribuidos (DCS) y otros sistemas configurables como Controles Lógicos Programables (PLC), mientras se abordan sus requisitos de rendimiento, confiabilidad y seguridad. El documento proporciona una descripción general de los ICS y sus topologías, identifica amenazas y vulnerabilidades típicas proporcionando medidas de seguridad recomendadas para mitigar los riesgos asociados.

Estructura del Documento:

Sección 1	"Introduction"	Propósito y Alcance.
Sección 2	"Overview of Industrial Control Systems"	Visión general de ICS y comparación con sistemas IT.
Sección 3	"ICS Risk Management and Assessment"	Evaluación y Administración de Riesgos.
Sección 4	"ICS Security Program Development and Deployment"	Desarrollo y Despliegue de un programa de seguridad para ICS.
Sección 5	"ICS Security Architecture"	Recomendaciones para integrar

		seguridad dentro de arquitecturas típicas de ICS.
Sección 6	“Applying Security Controls to ICS”	Resumen de controles administrativos, operacionales y técnicos.

Tabla 2. *Estructura de la Norma Nist 800-82 R2*

Fuente: elaboración propia.

Capítulo II. Marco conceptual

2.1. Tecnología operacional

Gartner (2012), define la Tecnología Operacional (OT por sus siglas en inglés) como *hardware* y *software* que detecta o causa un cambio, a través de monitoreo directo y control de dispositivos críticos, procesos y eventos en una empresa. En el pasado, OT se usaba principalmente en sistemas de control industrial para manufactura, transporte y servicios públicos y, a diferencia de la tecnología de la información (TI), la tecnología que controlaba las operaciones en esas industrias no estaba conectada a la red. Muchas de las herramientas para monitorear o hacer ajustes a los dispositivos físicos eran mecánicas y las que tenían controles digitales utilizaban protocolos propietarios cerrados (Rouse, 2016).

Según un estudio realizado por Fortinet en el 2018, tres de cada cuatro organizaciones han comenzado a converger su infraestructura de tecnología de la información (TI) con sus redes de tecnología operativa (OT). Con el advenimiento de la Internet de las Cosas, existe un desafío de gestión y aseguramiento de las redes y los sistemas que se vuelve crítico.

2.2. Sistemas de Control Industrial (SCI)

Trent Micro (s. f.), define a los Sistemas de Control Industrial (ICS por sus siglas en inglés), como un término colectivo utilizado para describir diferentes sistemas de control e instrumentación asociada, que incluye los dispositivos, sistemas, redes y controles utilizados para operar y automatizar procesos industriales.

2.3. Supervisory Control and Data Acquisition (Scada)

Según Wikipedia (s. f.), un Sistema de Control y Adquisición de Datos, es un sistema que incluye componentes *hardware* y *software* para la recolección de información en tiempo real, procesamiento y activación de alarmas en caso de encontrar condiciones peligrosas.

2.4. Controlador Lógico Programable (PLC)

Instrumento electrónico, que utiliza memoria programable para guardar instrucciones sobre la implementación de determinadas funciones, como operaciones lógicas, secuencias de acciones, especificaciones temporales, contadores y cálculos para el control mediante módulos de E/S analógicos o digitales sobre diferentes tipos de máquinas y de procesos (Asociación Nacional de Fabricantes Eléctricos - NEMA).

2.5. Sistema de Control Distribuido (DCS)

Yokogawa, uno de los líderes mundiales en SCI, define un sistema de control distribuido (DCS) como una plataforma para el control automatizado y el funcionamiento de una planta o de un proceso industrial. Un DCS combina, en un sistema automatizado único, interfaz hombre máquina (HMI), solucionadores lógicos, historiador, base de datos común, administración de alarmas y una suite de ingeniería común.

2.6. La Ciberseguridad en la Industria 4.0

De acuerdo con Sevillano (s. f.), en la actualidad paradigmas tecnológicos como Cloud Computing, Computación Ubicua, BYOD (Bring Your Own Device) o IoT (Internet of Things) han revolucionado la forma de entender la tecnología y la forma en que las personas interactúan con ella. Esto también repercute ámbito industrial, acuñándose términos como WSN (Wireless Sensor Networks), IIoT (Industrial Internet of Things), M2M (Machine to Machine), etc. Cuando la industria empieza a utilizarlos para integrar los dispositivos de campo y sistemas horizontalmente y facilitar la integración vertical de sistemas de información de planta, para optimizar los procesos de fabricación y para incrementar la productividad de las personas, se empieza a hablar de la Cuarta Revolución Industrial o Industria 4.0 (Fernando Sevillano, 2015).

Mientras que la industria se ha preocupado tradicionalmente por desarrollar normativas específicas que protegen la seguridad de las personas en los entornos industriales, la parte de la ciberseguridad industrial no se ha tenido en cuenta hasta hace poco.

Los fallos de seguridad provienen de sistemas heredados y del ascenso de la conectividad. La implementación y el uso de dispositivos conectados de la IoT industrial con sistemas operativos desfasados y con distintos protocolos de redes, hacen compleja la garantía de la seguridad, a través de soluciones comunes, utilizadas en entornos de TI de otros segmentos de actividad (Almeida, 2018).

Abrir la frontera de los Sistemas de Control Industrial (ICS) a la digitalización, implica hacer frente a las amenazas y ataques a las que las áreas de TI se enfrentan a diario. Por ejemplo, el robo de información, la posible alteración de los procesos de negocio o de las recetas de elaboración de ciertos productos, sobre todo en el caso de la industria de alimentos. De esta forma, es importante destacar que la seguridad informática en la Industria 4.0, no solo se centrará en la protección de los datos, sino en los dispositivos electrónicos conectados a las redes e Internet para su operación, ya que son susceptibles de ser hackeados (IT Business Solutions, 2018).

2.7. Convergencia IT/OT

Existen claras diferencias entre los ámbitos IT y OT, que justifican la necesidad de abordar del desarrollo e implantación de programas de ciberseguridad industrial específicos que estén alineados con las políticas de seguridad IT de la organización. En la siguiente figura se describen estas diferencias:

IT	Aspecto	OT
Confidencialidad, Integridad y Disponibilidad	**Objetivo**	Disponibilidad, integridad y confidencialidad
2/3 años con la existencia de gran número de proveedores	**Ciclo de vida**	10/20 años con reducido número de proveedores específicos y sectoriales
Práctica habitual que conduce a inversión en ciberseguridad	**Evaluación cuantitativa del riesgo**	Práctica realizada si es obligatoria
Habitual e integrada en la operación	**Desarrollo de sistemas de gestión de la seguridad**	No habitual y no integrada
Común , fácil de actualizar y con políticas bien definidas y automatizadas	**Antivirus y parches**	Poco habitual por la criticidad de los sistemas, complejo de desplegar y actualizar y sin políticas específicas
Normativas genéricas	**Cumplimiento normativas**	Normativas específicas y/o sectoriales
Utilización de las metodologías estándares más actuales	**Testeo y auditorías**	Realización de test específicos e inexistencia de metodologías estándares
Fácil despliegue y en ocasiones carácter obligatorio	**Respuesta a incidencias y análisis forense**	Poco habitual, no realizándose análisis forense

Figura 5. Seguridad IT vs. Ciberseguridad Industrial

Fuente: Logitek, 2014.

Según Guerrero (s. f.), el riesgo que corremos si no convergen IT y OT, es que en lugar de optimizar flujos de trabajo y procesos empresariales para crear nuevos productos que les interesen a los clientes, las organizaciones mantendrán cierto nivel de ineficiencia operativa.

La ineficiencia operativa implica que las empresas tendrán una estructura de costos más alta que la competencia y sin la visibilidad necesaria del modo y el lugar en que pueden llevarse a cabo mejoras. Además, los costos de IT y OT aumentarán mientras los componentes tecnológicos sigan desconectados y no se utilicen lo suficiente.

2.7.1. Las mejoras que aporta la convergencia

Los procesos industriales que se ven mejorados por la Integración IT y OT serán:

- Energéticos: adaptar el consumo energético en aquellas en las que la energía es más económica y reducirlo en aquellas que es más cara, gracias a los nuevos dispositivos interconectados.

- Medioambiente: los dispositivos inteligentes pueden medir datos meteorológicos, energéticos, etc., para que la planta pueda cumplir con los niveles de polución medioambientales establecidos por la ley y adaptar toda la producción a estos.
- Productivos: hace posible adaptar la demanda del cliente a la producción, para optimizarla y ahorrar costes.
- Control de calidad: permite fabricar con precisión y rapidez sin afectar al ritmo de producción.
- Mantenimiento: con la posibilidad de proceder a un mantenimiento predictivo que reduzca las averías y permita diseñarlo mejor para reducir las pérdidas.

Asimismo, las mejoras también se incorporan en el proceso comercial y logístico y agilizarán el proceso de venta del producto.

2.7.2. Diferencias

Según Oasys Outsourcing Automation Systems (2018).

La Tecnología de la Información se caracteriza por la aplicación de equipos de telecomunicación como ordenadores para tratar datos. IT Suele utilizarse en el ámbito de los negocios y las empresas. En cambio, la Tecnología de las Operaciones está dedicada a encontrar o cambiar los procesos físicos, a través de la monitorización y el control de dispositivos también físicos, como tuberías o válvulas. A continuación, exploraremos cómo se caracteriza cada una de estas tecnologías en diferentes situaciones (s. p.):

2.7.3. Necesidades tecnológicas

El primer factor a tener en cuenta lo forman las necesidades de sendas tecnologías. En IT, el número de componentes tecnológicos suele ser similar al número de profesionales en activo en una oficina, por ejemplo. Sin embargo, en OT se despliega una gran cantidad de dispositivos muy repartidos entre sí. Además, la cantidad de personas suele ser inferior en este último caso. Podríamos decir que los dispositivos IT siempre requieren de un profesional que lo controle, mientras que la tecnología OT es más autónoma (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.7.4. Condiciones de conservación

Otra de las diferencias entre IT y OT son las condiciones bajo las que se encuentran. En el caso de las OT, sus entornos suelen ser mucho más duros que con las IT, puesto que aguantan altas temperaturas, grandes niveles de humedad y ataques climatológicos en general. Las IT suelen ser bastante más frágiles y deben recibir un cuidado constante. Además, por lo general se sitúan en entornos controlados en los que no suelen haber cambios (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.7.5. Seguridad

En el caso de OT se prioriza el trabajo con máquinas y dispositivos como sensores para IIoT. Por ello, es mucho más habitual encontrar riesgos a la hora de trabajar con estas tecnologías. En este sentido, queda patente una de las diferencias entre IT y OT: la seguridad. Los sistemas IT tratan de priorizar la confidencialidad que los datos por encima de otros elementos. Así, la integridad de la información generada queda en un segundo plano y la disponibilidad de la misma se relega todavía más. Sin embargo, los sistemas OT y de control industrial ponen por delante la disponibilidad de su tecnología, puesto que se trata de un sector más pragmático y que depende en gran medida de la funcionalidad de su maquinaria. La integridad queda como el segundo objetivo más importante y la confidencialidad deja de priorizarse en estos casos (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.7.6. Normativa y Protocolos

En el ámbito de las OT, la normativa suele adaptarse a cada sector industrial de forma específica. De este modo, en casi ningún caso encontraremos una normativa generalista en el ámbito de las Tecnologías de las Operaciones. Sin embargo, las TI pueden utilizarse en varios sectores sin importar el ámbito con el que están relacionados. Por ello, la normativa suele ser mucho menos exhaustiva y mucho más abierta. En este sentido, este tipo de tecnologías suelen regularse por organismos internacionales, más globalizados, mientras que en OT se siguen procedimientos específicos convenidos por reguladores independientes en función del sector (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.7.7. Datos vs. procesos

En los sistemas IT, las vías comunicativas suelen estar congestionadas a causa de las grandes cantidades de información enviadas y recibidas. Por contra, en OT la infraestructura informativa es más bien secundaria y simple. De hecho,

en OT las organizaciones suelen desplegar un conjunto reducido de aplicaciones de control para administrar y mantener los sistemas. Además, este entorno permanece relativamente estático. Las prioridades son distintas, y es que en IT se busca analizar datos para tomar decisiones de forma óptima y el objetivo de OT es asegurar la calidad de los procesos físicos (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.7.8. Frecuencia de actualización

Existe un abismo entre el tiempo que se tarda en actualizar un sistema IT y uno OT. La tecnología IT es más vulnerable y por ello necesita actualizaciones constantes. Al tratarse de entornos más dinámicos, es fácil encontrar estos errores y solventarlos. Sin embargo, los sistemas OT deben permanecer en marcha durante largos periodos de tiempo, por lo que no pueden ser parcheados a menudo, puesto que esto requeriría de un reinicio. Si estos sistemas se desactivan, entonces se detendrían todos los procesos productivos con todas las pérdidas económicas que esto conlleva. Por desgracia, esto causa que a menudo se utilicen sistemas obsoletos en OT […].
Aunque ambas tecnologías pueden trabajar en conjunto para potenciar sus funcionalidades debemos comprender que sus utilidades son muy distintas y que los entornos en los que deben conservarse también difieren. Conocer las diferencias entre IT y OT es importante para asegurar una convergencia responsable y funcional en el sector de la Industria 4.0 (Oasys Outsourcing Automation Systems, 2018, s. p.).

2.8. Protocolos presentes en las Tecnologías OT

2.8.1. Modbus

Es uno de los protocolos de control industrial más veteranos. Hoy en día es ampliamente utilizado en un amplio espectro de industrias, incluyendo infraestructuras críticas. Modbus es un protocolo de comunicaciones industriales que se sitúa en la capa de aplicación, permitiendo por ello utilizar diferentes soportes físicos para el transporte. Proporciona comunicación en modo cliente/servidor entre diferentes equipos conectados a través de diferentes tecnologías de capas inferiores entre las que se incluye, pero no se limita, la capa de protocolos de TCP/IP (Incibe-cert.es, 2017, s. p.).

En cuanto a seguridad, carece de autenticación, solo es necesaria una dirección y un código de función que sean válidos. Estos datos se consiguen fácilmente a través de Internet y un *sniffer* de red. Tampoco permite cifrado de la información (Incibe-cert.es, 2017).

2.8.2. DNP3

Se utiliza en el sector eléctrico principalmente en USA y Canadá, principalmente en empresas de servicios públicos como electricidad y agua. Es un protocolo de tres capas que actúa en las capas de nivel de enlace, de nivel de aplicación y de nivel de transporte. En cuanto a su seguridad, es un protocolo diseñado para maximizar la disponibilidad del sistema, pero descuida la confidencialidad e integridad de los datos (Incibe-cert.es, 2017).

2.8.3. Profibus

Se basa en comunicaciones serie con soporte sobre cable (RS-485, MBP) o sobre fibra óptica. En la actualidad, tiene dos variantes, reflejadas en la Ilustración Profibus DP (periféricos descentralizados) que se usa para la operación de sensores y actuadores, a través de un controlador centralizado y Profibus PA (Automatización de Procesos). Este último se usa para la monitorización de equipos de medida, a través de un sistema de control del proceso. En cuanto a seguridad, es susceptible a ataques de inyección de tráfico o denegación de servicio (Incibe-cert.es, 2017).

2.8.4. Profinet

Es un estándar basado en Profibus que adopta como interfaz física de conexión Ethernet en lugar de RS485. Ofrece, para la transmisión de datos, la funcionalidad completa de TCP/IP, lo que le proporciona aplicaciones inalámbricas y alta velocidad de transferencia. Los equipos que utilizan Profinet están orientados a la fiabilidad y a la comunicación en tiempo real, junto con la usabilidad. Al igual que en otros protocolos, la ausencia de autenticación y la falta de seguridad del protocolo exigen el aislamiento del resto de la red (Incibe-cert.es, 2017).

2.8.5. BACnet

Es un protocolo de comunicaciones para redes de automatización y control de edificios. Fue diseñado para permitir para aplicaciones como calefacción, aire acondicionado, iluminación y sistemas detectores de incendios. En cuanto a seguridad,

es susceptible a ataques de *spoofing* y DoS (Shodan, 2018).

2.8.6. S7 (S7 Communication)

Es un protocolo propietario de Siemens que se ejecuta entre controladores lógicos programables (PLC) de la familia Siemens S7. Se han encontrado vulnerabilidades explotadas por fuerza bruta y evasión de protección (Shodan/Incibe, 2018).

2.9. Ciberseguridad en Infraestructuras Críticas

El término Infraestructura Crítica se refiere a activos o sistemas físicos computarizados, esenciales para la operación mínima de un gobierno y su economía. Incluye campos como el de las telecomunicaciones, energía, banca y finanzas, transporte, agua y servicios de emergencia, tanto en el sector público como en el privado.

La infraestructura crítica ha estado conformada por sistemas físicos y lógicos separados que han tenido una pequeña interacción o dependencia. Con el avance tecnológico, estas infraestructuras han crecido en automatización e interconectividad. Estas mejoras han incorporado nuevas vulnerabilidades como fallas en equipos, error humano, causas naturales, así como diversas amenazas físicas y computacionales (Leclair y Burns, 2018).

2.10. Protección en Infraestructuras Críticas

En Costa Rica se depende de instalaciones (aeropuertos, puertos, hospitales, etc.), redes de distribución (agua, electricidad, telecomunicaciones, etc.) y otros activos relacionados con servicios esenciales, necesarios para el buen y continuo funcionamiento de un país. Los incidentes cibernéticos son los que producen un gran impacto en el ámbito mundial. El uso de Internet y las tecnologías de la comunicación y la información para gestionar, operar y controlar las infraestructuras críticas hacen que los niveles de criticidad y probabilidad se incrementen exponencialmente.

El Foro Económico Mundial (s. f.), en sus últimos reportes *Riesgos globales*, ha

identificado las disrupciones o daños a la infraestructura crítica como uno de los riesgos tecnológicos más críticos, por el impacto que podrían causar y la alta probabilidad de que sucedan. Los incidentes cibernéticos que amenazan a las infraestructuras críticas pueden provenir de diferentes actores como cibercriminales, infiltrados, ciberactivistas, pero sobre todo de organizaciones patrocinadas por otros Estados. Estos, mediante operaciones de inteligencia o militares, llevan a cabo este tipo de ataques para vulnerar los servicios esenciales de un país y afectar su funcionamiento normal, incluso poniendo en riesgo vidas humanas que dependen de esos servicios.

Ante este escenario, surgen las dudas como cuánto ha avanzado Costa Rica en la protección de las *infraestructuras críticas* y cuán seguras se encuentran esas *infraestructuras críticas*. Es probable que las organizaciones públicas y privadas, por iniciativa propia, tomen previsiones para prevenir y mitigar los efectos de incidentes naturales y físicos, pero queda en duda si también consideran los incidentes cibernéticos.

En Costa Rica no existe un marco regulatorio ni se han identificado los sectores sensibles o las instalaciones y servicios críticos, por ende, los niveles de preparación y madurez son bajos, esto hace que el país sea vulnerable a las amenazas cibernéticas. Es necesario desarrollar un marco regulatorio adecuado y sentar las bases de cooperación público-privada para preservar el buen funcionamiento de las infraestructuras críticas (Ávila, 2017).

Capítulo III. Marco metodológico

3.1. Tipo de investigación

Este trabajo se desarrolló mediante el método de investigación aplicada, para utilizar conocimientos e información que se encontraba dispersa en variedad de idiomas y estándares. Asimismo, se empleó un análisis evaluativo, mediante el cual se buscó extraer la información más relevante para cumplir con el objetivo de asegurar las infraestructuras operacionales, en el ámbito nacional.

3.2. Alcance investigativo

Esta investigación se desarrolló de manera exploratoria, con el objetivo de examinar un campo muy poco conocido en Costa Rica, es decir, seguridad en infraestructura y procesos de automatización que se han desarrollado al margen de las buenas prácticas en ciberseguridad. Es necesario entender que la convergencia IT/OT es un hecho imprescindible para sacar el mayor provecho a las operaciones, por esto, que el análisis abarcó infraestructura operacional, desde el nivel más bajo, hasta el más complejo.

3.3. Enfoque

Se utilizó un enfoque mixto para tomar lo mejor de ambas partes y fusionar el conocimiento obtenido en una guía sencilla, práctica y de fácil implementación que sea provechosa para aquellas personas encargadas de resguardar los recursos tecnológicos y que, además, no están familiarizadas con el tema de la seguridad en la Tecnología Operacional.

3.4. Diseño

Este trabajo se desarrolló mediante un diseño mixto, en el que primero se empleó una metodología no experimental para recolectar toda la información referente a tendencias de seguridad en las compañías que utilizan tecnología operacional. La información obtenida, se subdividió en bloques o categorías, con el fin de integrar

características de seguridad que abarcaran, tanto aspectos técnicos como de gestión administrativa. La información fue tabulada, con el fin de hacer más fácil su análisis mediante la revisión de aspectos específicos relevantes para nuestro objetivo.

Con base en esto, se confirmó un modelo para entrar en una fase experimental, en la cual se buscaba usarlo en un escenario real de negocio. El éxito fue determinado por su ajuste en el entorno de aplicación, en tanto se cumpla con una seguridad razonable.

3.5. Población y muestreo

Se tomaron en cuenta las principales normas que abarcan el sector de infraestructuras críticas en los Estados Unidos y Europa, líderes en este ámbito. Estas normas que se han convertido en estándares mundialmente aceptados por las grandes industrias. Finalmente, se consolidó la información más importante de estas normas para formar nuestro propio modelo, con el fin de aplicarlo dentro de un escenario real de negocio.

El estudio se enfocó en una compañía de manufacturera de dispositivos médicos, que no se nombrara por razones de confidencialidad, sin embargo, se mencionarán algunas características para entender el entorno en el que se llevó a cabo este proyecto. Es una compañía transnacional con más de 15 años de presencia en Costa Rica y, en la actualidad, cuenta con más de 4600 colaboradores entre sus dos sitios, uno en la provincia de Heredia y el otro en la provincia de Alajuela. El alcance de la investigación se enfocó específicamente en las plataformas de tecnología operacional utilizadas por el Departamento de Facilidades, esto en las instalaciones ubicadas en El Coyol de Alajuela y sus sistemas encargados de la automatización de las condiciones ambientales para el funcionamiento óptimo de sus operaciones.

3.6. Instrumentos de recolección de datos

3.6.1. Mapas conceptuales

Esta herramienta se utilizó para extraer la información relevante, se resumieron y esquematizaron los conceptos clave que componen las principales normas de

seguridad en este ámbito, lo que hace más sencillo entenderlas.

3.6.2. Tabla de consolidación de datos

Producto de las tablas de cotejo, se recopilaron las características de seguridad más relevantes para la investigación. Los datos se tabularon en una tabla resumen y, finalmente, se eligieron aquellas que serán parte de la guía de seguridad.

3.6.3. Lista de verificación

Producto de los dos anteriores, se estableció una lista de verificación para aplicarla en el escenario real de negocio. Esta nos brindó información sencilla, específica y estructurada del *status* actual de la seguridad en los diferentes escenarios de gestión de tecnología operacional.

3.6.4. Entrevista a personal del departamento encargado

Este instrumento fue de gran importancia en la parte final de nuestra investigación, ya que proporcionó datos sobre la postura actual de seguridad en la compañía.

3.7. Técnicas de análisis de información

Una vez que la información fue recolectada, se inició con un proceso de codificación para agrupar las transcripciones en categorías, esto con el fin de relacionar los datos con el objetivo de la investigación. La información se recolectó desde el nivel más bajo o capa 1 del modelo OSI hasta los niveles superiores, para finalizar con una serie de aspectos de gestión administrativa hicieron de la guía un modelo adaptable a múltiples escenarios.

3.8. Variables

Las variables de investigación sentaron las bases de este estudio al determinar la información que será sujeto de recolección y evaluación. Como se mencionó en el apartado anterior, la información sujeta a este estudio fue recolectada mediante la

entrevista y la aplicación de una lista de verificación que, además, en englobó siguientes variables de estudio.

3.8.1. Diseño seguro con base en mejores prácticas

Esta variable tenía como objetivo, determinar si la red de control contaba con una arquitectura segura mediante la existencia de segmentos de red diferenciados. Además, se relacionaba con el establecimiento de niveles de seguridad para su infraestructura y mecanismos de control de tráfico que eviten el transporte del tráfico innecesario en la red de control.

3.8.2. Conocimiento por parte del personal de mejores prácticas utilizadas

Aunque se tenían bases comunes, la seguridad en el ámbito industrial difiere de la seguridad en el ámbito corporativo, sobre todo en el momento de aplicarla. Esta variable buscó determinar si el personal a cargo de la infraestructura operacional contaba con procedimientos específicos, enfocados en resguardar la seguridad de los sistemas operacionales. Además, midió si contaban con el conocimiento necesario para aplicarlos en sus labores, con la conciencia de las repercusiones que ocasionaría el no hacerlo.

3.8.3. Verificar la operacionalización de estas prácticas de diseño seguro

Después de su implementación y debido a las variaciones que tienen lugar a lo largo de los años, ya sea por cambios de administración, en las tecnologías o en las necesidades de negocio, es muy común que el enfoque de seguridad inicial se pierda con el paso del tiempo. Esta variable, buscaba determinar si el sistema seguía las prácticas básicas de seguridad, mediante su aplicación efectiva en el entorno operacional. Se verificó la existencia de los mecanismos de control y si se aplicaban.

3.8.4. Control de acceso físico

Se valoró la existencia de mecanismos de restricción de acceso con base en roles que regulen el acceso a áreas sensibles, donde se encuentren equipos,

infraestructura de comunicaciones o zonas catalogadas de alto riesgo. El acceso a estos lugares debía estar permitido solo al personal encargado de dar mantenimiento a los equipos o ejecutar operaciones en estas áreas.

3.8.5. Autenticación y autorización

Para este caso se pretendía verificar la existencia de una gestión de accesos efectiva basada en roles operativos creados con base en las funciones de cada usuario. Se evaluó, además, el nivel de seguridad de estos mecanismos de control interpuestos para la restricción de acceso lógico, en función de lo que se deseaba proteger.

3.8.6. Cifrado

La mayoría de los protocolos utilizados en sistemas de control industrial no incorporan mecanismos de cifrado en su implementación, esto hace que la intercepción, inspección y manipulación del tráfico sea algo sencillo para un atacante. Esta variable pretendía verificar la existencia y el uso de protocolos seguros como HTTPS, SNMP v3 o SSH para el acceso a los dispositivos de la red operacional.

3.8.7. Menor privilegio

Esta variable se trata de una estrategia de seguridad aplicable a distintos ámbitos. Con ella, se buscaba determinar si el nivel de acceso físico/lógico otorgado a los usuarios se basaba en la concesión de permisos estrictamente necesarios para el desempeño de sus funciones. La asignación de permisos a un usuario más allá de los necesarios, pueden permitirle llevar a cabo acciones para las cuales no estaba autorizado, lo que compromete la seguridad de la organización.

3.8.8. Segmentación (lógica y física)

A partir del modelo de arquitectura de la red segmentada por zonas, se pretendía diferenciar y aplicar medidas de seguridad enfocadas en cada segmento, según su función y objetivo. Al mismo tiempo, se buscaba contener y minimizar cualquier daño que pueda producirse debido a uno o varios dispositivos

comprometidos dentro de la red.

En este ámbito, se propone una arquitectura de red que cuente como mínimo con tres zonas, una para la Red de Control, otra para la Red Corporativa y una tercera en medio ambas que actúe como zona desmilitarizada (DMZ). Con esto y, a través de equipos de control de flujo de datos, se pretende evitar llevar tráfico innecesario a la red de control, liberándola, por ejemplo, de servicios de Internet o mensajería que pudieran utilizarse por atacantes para propagar *software* malicioso.

3.8.9. Monitoreo

La importancia de esta variable radica en el hecho de que era imprescindible tener visibilidad en tiempo real del estado del sistema, con el fin de encontrar anomalías en su funcionamiento, para ejecutar ajustes o correcciones oportunas, de forma manual o automática. Esto debía implementarse antes de que estas pudieran repercutir negativamente en el desarrollo de los procesos, causar daño a la integridad de los componentes del sistema o de que propiciaran condiciones inseguras para la vida humana.

3.8.10. Redundancia

Evaluación de la capacidad de continuar con la operación de procesos críticos, mediante mecanismos de control alternos hasta lograr la rehabilitación normal del sistema.

3.8.11. Registro de actividades

Además de evaluar el almacenamiento o procesamiento de datos, referente a la instrumentación del sistema y a los datos de control, el sistema deberá contar con una manera de dar trazabilidad a la actividad de los usuarios, en un marco de tiempo determinado en el que, como mínimo, se aprecie cuando un usuario inició y finalizó una sesión en el sistema.

3.8.12. Control y documentación de cambios

Al igual que en las infraestructuras de TI, estos sistemas cambian con la implementación de nuevas tecnologías y la adaptación a nuevos requisitos del negocio. Esta variable tenía como finalidad corroborar la existencia de una gestión adecuada de cambios, en la que se registraran datos como:

- Descripción del cambio.
- Impacto que tendrá el cambio sobre los dispositivos y sistemas asociados.
- Información de contacto para todos los involucrados en el cambio.
- Aprobación del cambio.
- Riesgos asociados.
- Plan de reversión o mitigación de los riesgos asociados.

3.8.13. Auditoría

El fin de esta variable era comprobar el cumplimiento de la seguridad operacional mediante la existencia de revisiones periódicas documentadas. El personal y su interacción con los componentes de sistema pueden influir directamente en la operación segura de los procesos que este controla.

3.8.14. Detección y respuesta a incidentes

Es la verificación de la existencia de documentación que contenga un predeterminado set de instrucciones o procedimientos para encontrar y responder ante un incidente que comprometa la seguridad de los sistemas de la organización. Estos deben responder no solamente al sistema que fue comprometido, sino también al servicio impactado.

Capítulo IV. Análisis de Información

Después de analizar y extraer la información más relevante de las principales normas en el ámbito internacional, se aplicó un cuestionario (Anexo 3) a los encargados del área, con el fin de nutrir las variables de investigación con los datos del negocio objeto de estudio. A continuación, se detalla la postura de seguridad del área estudiada, según los hallazgos por cada variable.

4.1. Sistemas de tecnología operacional encontrados

Durante la entrevista al personal encargado del Área de Facilidades en la empresa, se encontró que la compañía contaba con los siguientes sistemas para el mantenimiento y control de las condiciones ambientales en su edificio de 3 plantas. Estas condiciones son necesarias para el desarrollo de sus operaciones más críticas.

4.1.1. Andover Continuum

Instalado en 2009, este sistema aún funciona como tecnología de control de temperatura y humedad para áreas de oficina, bodega y ambientes controlados. Se trata de una de las primeras versiones de sistema BMS del fabricante europeo Schneider Electric. Cuenta con una cantidad de 244 sensores a lo largo del edificio concentrados por zonas y unidos por un bus de datos que se conecta a la red corporativa.

4.1.2. Ecostruxure Building Operation (EBO)

Instalado en 2016, cuenta con más de 244 sensores y está pensado que sea el sucesor del Andover Continuum. En la actualidad, se trabaja en migrar las zonas de control a este nuevo sistema que también pertenece al fabricante Schneider Electric.

4.1.3. Power Monitoring Expert (PME)

Es un sistema de monitoreo y análisis de energía que permite habilitar la gestión energética para optimizar la eficiencia energética y mejorar su rentabilidad. En la

actualidad, se utiliza para monitorear cientos de paneles eléctricos distribuidos a lo largo y ancho del edificio. Los sensores están interconectados a cada panel eléctrico y, a la vez, a la red corporativa.

4.1.4. Vaisala ViewLinc

Se utiliza para el monitoreo de ambiente (temperatura, humedad y presión diferencial), este sistema está validado por un riguroso sistema de calidad que dicta los rangos aceptables de operación en las áreas controladas o cuartos limpios en los que se manufacturan los dispositivos médicos. Su instalación fue ejecutada en el 2015 y cuenta con más de 89 sensores que monitorean 8 áreas de ambiente controlado.

4.2. Análisis de variables

Para nuestro estudio, decidimos tomar como objeto de análisis y aseguramiento al sistema EBO. Al tratarse de un sistema BMS que monitorea y controla las condiciones ambientales del edificio en general, este consolidaría la información de monitoreo obtenida por los sistemas Continuum y ViewLinc.

Por otro lado, este sistema no solamente monitorea las áreas donde se manufacturan dispositivos médicos, sino que mantiene y controla automáticamente las condiciones ambientales para estas zonas. Esto lo convierte en un sistema crítico para las operaciones de la compañía y objeto de aseguramiento para el modelo.

4.2.1. Diseño

El sistema EBO cuenta con 244 sensores o registradores de datos de diferentes tipos distribuidos por toda la planta. Desde sus inicios, el sistema BMS, a través de su primer versión Andover Continuum, se implantó bajo su propio dominio (BMS), es decir, un ambiente de autenticación separado de la red corporativa y que en su momento solamente poseía dos usuarios, uno para la administración y otro para la operacionalización del sistema. Sin embargo, en la actualidad, el sistema está siendo migrado a su nueva versión EcoStuxure Building Operation (EBO) para reutilizar los componentes del sistema Continuum. Esto sucede bajo el mismo dominio en el que se

encuentra la red de oficina. A continuación, se listan los componentes del nuevo sistema:

- **Sensores:** interconectados a través de cableado TFFN de bajo voltaje hasta llegar a dispositivos PLC.
- **Protocolos:** Modbus, BACnet.
- **Fabricante:** Schneider Electric.
- **PLC:** dispositivos que funcionan como controlador de dispositivos. En promedio se cuenta con 4 sensores conectados a cada controlador.
- **Actuadores**: en la forma de amortiguadores (*dampers*) y válvulas.
- **Servidores de Automatización (ASP): (**llamados SmartX Controller por el fabricante), se encargan del control de tráfico, comunicación multiprotocolo, gestión de alertas y envío de datos al servidor de aplicación y base de datos. Esta comunicación se da a través de la red corporativa. Tiene a cargo la lógica de control, el registro de tendencias y la supervisión de las alarmas, respalda la comunicación y la conectividad a los buses de campo y módulos de E/S.
- **Servidor de Aplicación:** plataforma Windows virtualizada desde la cual corre el sistema y se administra la parametrización y graficación.
- **Servidor de Base de Datos:** plataforma Windows/SQL virtualizada en la misma subred del servidor de aplicación, funciona como historiador de datos.
- **Estaciones de Control:** el Departamento de Facilidades utiliza dos *workstations* HP con sistema operativo Windows para el monitoreo, control y envío de notificaciones (solamente una de estas se configura para el envío de alertas mediante el protocolo SMTP).

4.2.2. Conocimiento del personal sobre mejores prácticas

El personal encargado de interactuar con el sistema tiene dos roles:

- **Ingenieros:** encargados de la implantación, mantenimiento, administración de alertas y medidas de corrección.
- **Técnicos:** encargados de efectuar rondas, atender alertas y escalar problemas a los ingenieros.

Ambos se encargan de efectuar sus labores con la mayor eficacia, sin embargo, muchas veces se desatienden aspectos básicos de la ciberseguridad como la administración de las contraseñas, el estado de las estaciones de control que permanecen desbloqueadas y la posibilidad de conectar dispositivos USB a sus puertos, que se encuentran habilitados sin ninguna necesidad aparente.

4.2.3. Verificación de operacionalización de prácticas de diseño seguro

El sistema BMS inicial mostraba su propia estructura de autenticación, a través de su primera versión (Andover Continuum). Sin embargo, con la nueva versión EBO, esta independencia de dominio se perdió al implantar dos servidores virtualizados en la red corporativa. Por lo demás, el sistema actual conserva la misma estructura de seguridad de su antecesor.

4.2.4. Control de acceso físico

Los dispositivos principales como los PLC y servidores de control se encuentran dentro de gabinetes anclados, sellados y con cerradura. Estos, a la vez, están en un área especial de edificio, administrada por el Departamento de Facilidades, a la cual se accede a través de lector de tarjeta. Las estaciones de control (*workstations*) se encuentran en áreas de acceso restringido a las que solamente el personal de facilidades tiene acceso.

4.2.5. Autenticación y autorización

Tanto los servidores como las estaciones de control utilizan los mecanismos de autenticación estándar de la red corporativa. Por otro lado, los dispositivos de la red de control utilizan sus contraseñas por defecto.

4.2.6. Cifrado

No existe cifrado.

4.2.7. Menor privilegio

en la actualidad, el sistema se encuentra en fase de transición y solamente es operado por un único ingeniero quien posee el privilegio más alto. Una vez implementado al 100 %, se espera que el sistema sea operado por 15 personas, entre ingenieros, técnicos y personal supervisor que tendrán los siguientes roles de acceso:

- Programador → Privilegio más alto, este usuario tiene control del sistema y es capaz de crear y modificar pantallas.
- Administrador → Capaz de configurar parámetros y administrar la seguridad.
- Técnico → Con privilegios para el encendido o arranque de equipos.
- Viewer → Puede ingresar al sistema, pero no puede llevar a cabo ningún cambio.

4.2.8. Segmentación

No existe segmentación entre la red de control y la red corporativa. Los componentes se encuentran distribuidos a lo largo del edificio y conectados entre las diferentes subredes de oficina, bodega y áreas de manufactura. Durante un ejercicio de prueba básica de penetración, se logró llegar hasta el controlador de una de las subestaciones eléctricas del edificio, conectados a un teléfono IP ubicado en un cubículo.

4.2.9. Monitoreo

Se cuenta con un sistema centralizado de monitoreo para la visualización de alarmas que se disparen al dañarse un componente o traspasarse algún umbral establecido. En la actualidad, este monitoreo se lleva a cabo desde el mismo servidor en el que reside la aplicación (EcoStruxure Building Operation).

4.2.10. Redundancia

Se maneja un inventario de dispositivos de repuesto que son reemplazados en el momento de encontrar una falla. Por otro lado, todos los componentes críticos del sistema se encuentran conectados a circuitos de emergencia, lo cual quiere decir que cuentan con respaldo de UPS y generador eléctrico.

4.2.11. Registro de actividades

El sistema registra en una bitácora todo tipo de actividad generada por los usuarios dentro del sistema. El periodo de retención de esta información es indefinido.

4.2.12. Control y documentación de cambios

Los cambios son ejecutados una vez que el equipo de facilidades ha tomado la decisión de llevar a cabo alguna mejora al sistema. La autorización es dada por los gerentes del área y un ingeniero se encarga de organizar los cambios en el campo y en el sistema. Los cambios son ejecutados, de forma paralela, con el sistema Continuum, con el fin de mantener el área protegida.

4.2.13. Auditoría

El sistema no cuenta con ningún tipo de revisión periódica o regulatoria.

4.2.14. Detección y respuesta a incidentes

La detección se realiza, de forma automática y el sistema dispara alertas, a través de notificaciones por correo electrónico. Las alertas son monitoreadas 24x7 por técnicos que se encuentran en el sitio.

4.3. Exploración de otros entornos en el ámbito nacional

Con la finalidad de enriquecer el modelo y adaptarlo a las necesidades del ámbito nacional, se decidió considerar otros entornos con diferentes giros de negocio. Para esto, se entrevistó al personal de 2 diferentes compañías integradoras, encargadas de la implantación de estas tecnologías en diversas empresas a lo largo y

ancho del país. La entrevista se resume en 10 preguntas esenciales que se detallan a continuación:

PREGUNTAS	INTEGRADOR #1					INTEGRADOR #2				
	1	2	3	4	5	1	2	3	4	5
¿Se entrega documentación del sistema instalado? (Diagramas de interconexión, inventario, configuraciones)		X								X
¿Se capacita al personal en el uso del sistema?					X				X	
¿Cuán frecuente encontrar un ambiente con redes separadas? (Red de oficina separada de la red de control)			X						X	
¿Cuán frecuente es encontrar equipos de seguridad que restrinjan el acceso desde la red de oficina?				X				X		
¿Los componentes y el cableado se instalan, en un lugar, con acceso restringido?					X					X
¿Se instruye al cliente en cuanto a la protección y localización de componentes ante condiciones ambientales? (temperatura, humedad, polvo, radiación o vibración)			X				X			
¿Se cambian las contraseñas por defecto a los componentes del sistema?		X							X	
¿Los componentes del sistema tienen acceso a Internet?			X				X			
¿Se registran las actividades de los usuarios dentro del sistema de control?			X			X				
¿Cuán común es que se adquiera un contrato de soporte o mantenimiento?	X					X				

ESCALA DE 1-5

1 – Nunca
2 – Poco frecuente
3 – Ocasionalmente
4 – Frecuentemente

5 – Siempre

Se recibió retroalimentación muy similar de parte de ambos integradores, con resultados positivos en cuanto a la restricción de acceso físico a los componentes del sistema y al adiestramiento del personal en el uso del sistema de control. Sin embargo, se pueden encontrar grandes oportunidades de mejora en el tema del mantenimiento y resolución de problemas, ya que cuando se les consultó por contratos de mantenimiento o de soporte, en ambos casos la respuesta fue contundente: *nunca*.

Capítulo V. Propuesta del modelo

5.1. Creación del modelo

A través de la tabla de consolidación de datos (Anexo 1) se recolectaron los puntos más importantes y en los que las principales normas y estándares internacionales se enfocaban. De esta manera, se confeccionó el modelo con base en siete controles principales. Estos, a la vez, contienen una serie de subcontroles que conforman una guía de cincuenta aspectos de seguridad en el marco de la tecnología operacional. A continuación, se listan los siete controles principales que conforman el modelo:

- Control 1: documentos, políticas y requerimientos.
- Control 2: diseño seguro.
- Control 3: seguridad física.
- Control 4: seguridad lógica.
- Control 5: gestión de cambios.
- Control 6: mantenimiento.
- Control 7: manejo de incidentes y recuperación.

5.2. Aplicación del modelo

Como se mencionó en el punto anterior, el modelo tenía como objeto de estudio al sistema EcoStruxure Building Operation, actualmente instalado en los predios de la empresa. Con la autorización previa del área encargada, se aplicó el modelo propuesto (Anexo 2). A continuación, se describe cada uno de los aspectos tomados en cuenta y cómo se planteó el aseguramiento del sistema, a través de cada uno.

5.3. Aseguramiento del diseño actual

5.3.1. Control 1 (documentación, políticas y requerimientos)

Se propuso la creación de dos documentos:

- Especificaciones Técnicas del Sistema (arquitectura y diseño).
- Operación, Soporte y Mantenimiento del Sistema.

Por otro lado, se determinó que el segundo debía cargarse a la plataforma electrónica de entrenamientos de la compañía, para que fuera asignado al currículo del personal a cargo.

5.3.2. Control 2 (diseño seguro)

Al tratarse de un sistema ya en operación, la única observación es el acceso lógico que podría obtenerse desde la red de oficina a los componentes de la red de control. La colocación y configuración de un cortafuegos (*firewall*) es altamente recomendada. Se determina que la ubicación de los componentes, así como el acceso a estos no amerita un riesgo para la integridad de los dispositivos del sistema.

5.3.3. Control 3 (seguridad física)

Las áreas donde se ubican los componentes del sistema son de acceso restringido, a través de cerraduras que solamente se abren por medio de tarjeta electrónica. El acceso solo es otorgado al personal del Departamento de Facilidades. Por otro lado, los componentes más sensibles como los PLC o dispositivos AS-P se encuentran en de gabinetes con cerradura y el cableado se canaliza, a través de tubería metálica EMT.

5.3.4. Control 4 (seguridad lógica)

El sistema cuenta con bitácoras detalladas que registran todo tipo de actividad de los usuarios. Sin embargo, hay dos aspectos que se deben corregir, ya que representan un riesgo alto para las operaciones en caso de un ataque cibernético:

- Se debe restringir el acceso a Internet desde la red de control.
- Se debe cambiar la contraseña por defecto de los dispositivos conectados, a través de conexiones Ethernet.

5.3.5. Control 5 (gestión de cambios)

En la actualidad, no se cuenta con ningún tipo de control sobre los cambios que se ejecutan al sistema. Los cambios se ejecutan directamente en el ambiente en producción y obedecen a mejoras en la capacidad o al crecimiento de áreas que se encuentran en construcción. Es recomendable habilitar un ambiente de pruebas y documentar cada cambio realizado en el sistema, esta documentación debería incluir lo siguiente:

- Descripción del trabajo que se debe llevar a cabo y por quién.
- Horario en el que se hará el cambio.
- Aprobación del cambio.
- Análisis del riesgo con su respectiva mitigación.

5.3.6. Control 6 (mantenimiento)

El sistema cuenta con alertas configuradas para situaciones específicas, las cuales son recibidas por el personal técnico de Facilidades. Esto con el fin de aplicar medidas correctivas con la mayor brevedad posible.

En este aspecto se recomienda el establecimiento de al menos dos ventanas de mantenimiento al año, para actualizar el *software* y el *firmware* de los dispositivos. Además, se recomienda la gestión de un contrato de soporte y mantenimiento para ejecutar estas tareas en las ventanas de mantenimiento programadas.

5.3.7. Control 7 (gestión de incidentes y recuperación)

En este sentido, el departamento posee un plan general de continuidad de negocio que cubre este sistema. Para este último apartado y como se mencionó en el

control 2, se recomienda la implementación de un cortafuegos entre la red del sistema BMS y la red de oficina. Esto no solo con el fin de restringir el tráfico, sino también para encontrar y contener actividad maliciosa que pueda interferir con los procesos de control. Por último, este equipo debe ser administrado y supervisado por el personal de seguridad de TI, con el fin de aplicar medidas para repeler cualquier intento de ataque y alertar a las autoridades correspondientes.

Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

- La ciberseguridad en las operaciones es una disciplina en la que cada día surgen nuevas preguntas y desafíos, ya que las amenazas también se adaptan a los esfuerzos por hacer nuestra forma de vida más segura. Para asegurar los entornos de control operativo, es de vital importancia mantener alineados los controles de seguridad a las nuevas tecnologías. Esta guía, logra recopilar los principales aspectos, establecidos por estándares reconocidos mundialmente. Se presentan, de una manera, sencilla y estructurada, los principales puntos de enfoque de la seguridad en la tecnología operativa.

- Debido a que los sistemas de tecnología operacional están conectados típicamente a las redes de TI, es usual que representen el eslabón más débil en la cadena de seguridad. Esto se debe a que los sistemas de control utilizan tecnología más antigua, mecanismos de seguridad menos desarrollados y, en algunos casos, inexistentes, lo que ofrece a los atacantes una mayor tasa de éxito en su explotación.

- A lo largo de los años, la utilización de protocolos propietarios ha complicado la creación general de soluciones de seguridad compatibles para proteger estas tecnologías. Esto hace que los fabricantes creen sus propias soluciones homologadas para sus productos. Es por esta razón que esta guía se presenta como un modelo ajustable a las necesidades de cada escenario, además, ofrece un compendio de 50 controles extraídos de las principales normas en el campo de la ciberseguridad industrial. Asimismo, se señalan 20 controles como esenciales, esto permite a cada organización adaptarse al modelo, según sus necesidades, manteniendo siempre una seguridad razonable.

- El modelo logró aplicarse en una compañía *madura* a nivel de operaciones,

pero que todavía presenta grandes oportunidades de mejora en el área de ciberseguridad. Este estudio encontró algunas deficiencias en materia de documentación, seguridad lógica y gestión de cambios, sin embargo, los controles corporativos aplicados en materia de TI y control de acceso físico, parecen actuar como medidas compensatorias a ciertas deficiencias.

6.2. Recomendaciones

- Es imperativo pensar en un enfoque holístico de la seguridad para las organizaciones. TI y TO deben derribar las barreras culturales que históricamente los ha mantenido separados y trabajar para incluir la seguridad desde su etapa de diseño, sometiendo a las tecnologías operacionales a los mismos niveles de protección y estándares de seguridad. De lo contrario, estos sistemas continuarán como el eslabón más débil por el que los atacantes conseguirán infiltrarse en las operaciones. Este modelo recopila las mejores prácticas de seguridad, señaladas por los principales estándares en el ámbito mundial (NIST800-82r2, IEC62443, NERCCIP, ISO27000 y CIS). Sin embargo, se recomienda mantenerse expectante ante futuros cambios en estas normas, ya que la seguridad es un proceso cambiante.

- Para los próximos años, como lo indican los más recientes informes en seguridad, se espera un incremento en la incidencia de ataques en los sistemas de control. Por esto, se vuelve indispensable elegir una solución de seguridad adecuada que proteja no solamente la infraestructura de TI, sino también los entornos de control. Esta solución debe estar acompaña de un programa integral de seguridad que, además de proteger activos, penetre en la conciencia de cada uno de los colaboradores.

- Los riesgos son reales y se hacen cada vez más grandes y complejos. La mejor forma de protegernos es tener un enfoque estratégico que proteja a toda la organización. Por eso, elegir al proveedor adecuado es vital para un programa de seguridad efectivo. Para hacerlo, las organizaciones deben

tener en cuenta que, a largo plazo, la seguridad es más que un simple producto. Se debe pensar en la seguridad como un proceso cambiante que se transforma, como respuesta a las nuevas tecnologías y a las subsecuentes amenazas del entorno.

6.3. Trabajo futuro

Esta guía está pensada para todas aquellas personas encargadas de administrar o dar soporte a tecnologías operacionales. Está adaptada para cumplir con los principales aspectos de seguridad establecidos por estándares internacionales, mundialmente reconocidos. Para asegurar los entornos de control, es vital mantener actualizados los controles, de acuerdo con las tendencias tecnológicas del momento y con los panoramas de las principales amenazas en el ámbito mundial.

Además, será de gran valor proveer una guía para la instalación y configuración de un cortafuegos (de uso libre) con parámetros básicos de seguridad que faciliten la implementación de los controles de seguridad lógica mencionados en esta guía. Se espera que también pueda ser utilizado por organizaciones de todo tipo para proveer una seguridad razonable a sus operaciones, sin incurrir en grandes gastos monetarios.

Referencias bibliográficas

Gartner. (2012). Gartner IT Glossary. Operational Technology (OT). Recuperado de: https://www.gartner.com/it-glossary/operational-technology-ot/

Guerrero, M. (2018). Necesitamos el entendimiento IT & OT. Recuperado de: https://manuelguerrerocano.com/it_ot_convergencia/

Incibe-cert.es. (2018). Protocolos y seguridad de red en infraestructuras SCI. Recuperado de: https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf

Industrial Control System - Definition - Trend Micro USA. (2018). Trendmicro.com. Recuperado de: https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

Infochannel. (2018). El papel de la seguridad en la Industria 4.0. Recuperado de: https://www.infochannel.info/el-papel-de-la-seguridad-en-la-industria-40-0

Larepublica.net. (2017). Infraestructuras críticas, ¿están seguras? Recuperado de: https://www.larepublica.net/noticia/infraestructuras-criticas-estan-seguras

Nema.org. (2018). Programmable Controllers - NEMA. Recuperado de: https://www.nema.org/Products/Pages/Programmable-Controllers.aspx

Oasys Outsourcing Automation Systems. (2018). Diferencias entre IT y OT y su convergencia. Recuperado de: https://oasys-sw.com/diferencias-entre-it-y-ot/

Sevillano, F. (2014). Seguridad IT versus Ciberseguridad Industrial. Ciberseguridad Industrial by Logitek. Recuperado de: http://www.ciberseguridadlogitek.com/seguridad-it-versus-ciberseguridad-industrial/

Sevillano, F. (2015). ¿Qué es la Industria 4.0? Ciberseguridad Industrial, by Logitek. Recuperado de; http://www.ciberseguridadlogitek.com/que-es-la-industria-4-0/

Shodan.io. (2018). Industrial Control Systems. Recuperado de: https://www.shodan.io/explore/category/industrial-control-systems

Solutions, R. (2018). Conozca la importancia de la seguridad informática en la Industria 4.0. Itbusiness-solutions.com.mx. Recuperado de: https://www.itbusiness-solutions.com.mx/conozca-la-importancia-de-la-seguridad-informatica-en-la-industria-4.0

Uniss.org. (2018). Recuperado de: http://www.uniss.org/docs/CYBER%20SECURITY%20POLICIES%20AND%20CRITICAL%20INFRASTRUCTURE%20PROTECTION_v3.1-small.pdf

WhatIs.com. (2018). What is operational technology (OT). Recuperado de: https://whatis.techtarget.com/definition/operational-technology

Yokogawa.com. (2018). Who we are. Recuperado de: https://www.yokogawa.com/mx/about/careers/who-we-are/

Anexos

Anexo 1. Tabla de consolidación de datos

ASPECTO GENERAL	ASPECTOS ESPECÍFICOS	NIST 800-82r2	IEC 62443	NERC-CIP	ISO 27000	CIS
Documentación, Políticas y Procedimientos	Arquitectura del sistema	✔	✔			
	Soporte				✔	
	Procedimientos y capacitación del personal de operación	✔	✔	✔	✔	
	Políticas de seguridad	✔	✔	✔	✔	✔
	Control de cambios	✔	✔	✔	✔	
	Respaldo y retención de información	✔	✔	✔	✔	
	Protocolos de emergencia	✔	✔	✔	✔	✔
	Concienciación del personal	✔	✔	✔	✔	✔
	Evaluación y clasificación de riesgos	✔	✔	✔		✔
Diseño	Requerimientos de control de tiempo	✔				
	Separación de redes	✔	✔			✔
	Segmentación (Modelo de zonas y conductos)	✔	✔	✔	✔	✔
	Defensa en profundidad	✔	✔		✔	
	Supervisión	✔		✔		
	Disponibilidad y tolerancia a fallos	✔	✔	✔		

	Capacidad de funcionamiento degradado	✔		✔		
	Protección y localización de componentes	✔		✔		
	Seguridad del personal	✔	✔	✔		
	Componentes críticos redundantes	✔		✔		
	Servicios de autenticación dentro de la red de control	✔	✔	✔		✔
	Protección contra disrupciones eléctricas				✔	
	Habilitación de logs de auditoría, en un lugar, seguro	✔		✔	✔	✔
Seguridad Física	Limitaciones de acceso basada en roles	✔			✔	
	Restricción de acceso a los componentes del sistema	✔	✔	✔	✔	
	Restricción de conexión a puertos	✔		✔		✔
	Protección de componentes / condiciones ambientales	✔		✔	✔	
	Registro de acceso	✔		✔	✔	
	Gestión de dispositivos extraíbles (USB)	✔		✔		✔
Seguridad Lógica	Autenticación multifactor para acceso administrativo	✔		✔		✔
	Uso de certificados		✔	✔	✔	✔
	Políticas de contraseña	✔		✔	✔	

	Cambio de contraseñas por defecto y desactivación de servicios no esenciales	✔		✔		✔
	Protección contra malware con gestión centralizada	✔		✔	✔	✔
	Protección *firewall* (protocolos, servicios) e implementación de listas blancas	✔	✔	✔		✔
	Restricción de acceso a Internet desde la red de control	✔	✔			✔
	Restricción por dirección MAC	✔				✔
	Comunicación inalámbrica cifrada	✔	✔	✔	✔	✔
	Gateways unidireccionales	✔				
	Registro de actividades de usuario	✔	✔	✔		✔
Gestión de Cambios	Ambiente de pruebas	✔		✔	✔	✔
	Ventanas de mantenimiento	✔	✔	✔		
	Gestión automatizada de actualizaciones	✔	✔	✔		✔
	Análisis de riesgos	✔	✔			
	Registro de cambios	✔	✔	✔	✔	
	Posibilidad de reversión a un estado anterior	✔				
Mantenimiento	Conexión remota / Cifrado con autenticación multifactor	✔		✔		✔
	Mantenimiento a componentes	✔	✔		✔	
	Inventario / Administración de	✔	✔	✔	✔	✔

	Activos Hardware					
	Monitoreo / Alertas	✔	✔	✔	✔	✔
	Actualizaciones (*firmware*)	✔	✔	✔		
	Actualizaciones (*software*)	✔	✔	✔	✔	
	Testeo de reglas de *firewall*	✔		✔		
	Respaldos de información y configuraciones	✔	✔		✔	✔
	Protección y pruebas de los respaldos	✔	✔			✔
	Soporte del proveedor *software* / *hardware*					✔
	Desactivación / Modificación oportuna de accesos	✔		✔	✔	
Manejo de Incidentes y Recuperación	Detección y Contención	✔	✔	✔		✔
	Estructura de respuesta con autorización y personal competente	✔	✔	✔	✔	✔
	Activación manual o métodos alternos para procesos críticos	✔	✔			
	Contacto con autoridades o grupos de interés	✔	✔	✔	✔	✔
	Pruebas de penetración y funcionalidad de los planes			✔	✔	✔
	Restauración de servicios	✔	✔	✔		
	Reportes	✔	✔	✔	✔	✔

Anexo 2. Guía de seguridad para tecnología operacional

C-01 | Documentación, políticas y procedimientos

ID	SUBCONTROL	DESCRIPCIÓN
SC-01	Documentación del Sistema	Organigrama, arquitectura, soporte, control de cambios, respaldo y retención de información.
SC-02	Protocolos de emergencia y evaluación de riesgos	Plan de continuidad, recuperación de desastres. Varios tipos de incidentes deben identificarse y clasificados de acuerdo con su potencial impacto para asegurar una respuesta y asignación de recursos adecuada.
SC-03	Procedimientos	Operación del sistema / Alertas.
SC-04	Entrenamientos Regulatorios	Capacitación y evaluación del conocimiento del personal / Concienciación.
SC-05	Políticas de seguridad	Contraseñas, cuentas compartidas, uso de activos.

C-02 | Diseño seguro

ID	SUBCONTROL	DESCRIPCIÓN
SC-06	Seguridad en Capas	Definición de los equipos y procesos más importantes donde las comunicaciones más críticas se encuentran en la capa más segura.
SC-07	Separación de redes	Red de oficina separada de la red de control.
SC-08	Requerimientos de control de tiempo	Evitar latencia y que el procesamiento de información se realice, de manera oportuna, para los procesos de control. (Respuesta en tiempo real)
SC-09	Segmentación	Establecer zonas y aplicar controles de seguridad con base en categorización de activos (Nivel de criticidad).
SC-10	Supervisión (monitoreo)	Contar con una interfaz de visualización centralizada que muestre en tiempo real todos los subsistemas y el estado de sus componentes.

SC-11	Disponibilidad	El sistema debe poseer redundancia para componentes y servicios críticos (ej. Generador/UPS/repuestos).
SC-12	Capacidad de funcionamiento degradado	El diseño debe prevenir fallos en cascada y proveer métodos alternos (ej. manuales) para la ejecución de procesos críticos hasta la recuperación de condiciones seguras.
SC-13	Protección y localización de componentes	Protección contra: humedad, polvo, vibración, radiación y vandalismo.
SC-14	Autenticación	Autenticación entre componentes del sistema, a través de certificados o contraseñas complejas únicas y aleatorias por cada conexión.
SC-15	Servidor de autenticación	Dentro de la red de control
SC-16	Seguridad del personal	Detección de condiciones inseguras y capacidad de alertar o ejecutar procesos de corrección automáticos. La supervisión humana es esencial.
SC-17	Registros de auditoría	Habilitar registros de eventos del sistema con restricción de acceso para auditorías.

C-03 | Seguridad física

ID	SUBCONTROL	DESCRIPCIÓN
SC-18	Limitación de acceso basada en roles	Proveer acceso a las áreas sensibles solamente a personal calificado, con el fin de prevenir incidentes.
SC-19	Restricción de acceso a componentes del sistema	Aislar los componentes del sistema de control y sus conexiones del alcance del personal común o visitantes (ej.: PLC's, cableado, placas de red).
SC-20	Registros de acceso	Utilizar algún mecanismo para registrar el acceso del personal en áreas restringidas. (ej.: lector de tarjetas electrónicas).
SC-21	Gestión de dispositivos extraíbles	Restringir la conexión de dispositivos extraíbles en componentes o estaciones del sistema de control mediante la deshabilitación de puertos sin uso (ej.: desactivar puertos USB/Serial).

C-04 | Seguridad lógica

ID	SUBCONTROL	DESCRIPCIÓN
SC-22	Autenticación multifactor para acceso administrativo	Uso de token, tarjetas inteligentes con PIN, autenticación biométrica, entre otros.
SC-23	Uso de encriptación o certificados cuando sea posible	Encriptación y autenticación entre dispositivos.
SC-24	Políticas de contraseña	Forzar el uso de complejidad y cambio periódico de contraseñas (recomendado 90 días).
SC-25	Cambio de contraseñas	Cambiar las contraseñas por defecto en todos los componentes del sistema.
SC-26	Protección contra *software* malicioso	Uso de herramienta antivirus/antimalware con gestión centralizada y actualizaciones oportunas. **Esta solución debe ser compatible con el sistema de control**.
SC-27	Implementación de cortafuegos (*firewall*)	Restricción de protocolos y servicios permitiendo únicamente aquellos que son esenciales para el funcionamiento del sistema (*whitelisting*)
SC-28	Restricción de acceso a Internet	No permitir el acceso a Internet desde la red de control. (Evitar la comunicación directa también hacia la red de control).
SC-29	Restricción por dirección MAC	Utilización de conmutadores (*switches*) administrables para restringir la conexión de dispositivos dentro de la red de control, a través de su dirección MAC.
SC-30	Comunicación inalámbrica cifrada	Uso de protocolos seguros de comunicación para aquellos casos en donde la conexión de componentes o estaciones remotas sea necesario (WPA2, Trusted Wireless, etc.)
SC-31	Tráfico unidireccional	Restringir el flujo de datos entre componentes o redes en un solo sentido, según su función (ej.: tráfico SMTP para el envío de alertas / saliente)
SC-32	Registro de actividades de usuario	Habilitar registros donde como mínimo se muestre: inicios de sesión, fallos de Inicio de sesión con cuentas administrativas, usuario, estación/componente,

		hora y fecha.

C-05 | Gestión de cambios

ID	SUBCONTROL	DESCRIPCIÓN
SC-33	Ambiente de pruebas	Habilitación de un ambiente de pruebas para garantizar la integridad del sistema posterior a cambios (actualizaciones de *firmware*, modificación de componentes, entre otros).
SC-34	Ventanas de mantenimiento	Programación previa de actividades para la aplicación de parches o ejecución de mantenimientos a componentes dentro de la red de control.
SC-35	Análisis de riesgos	Analizar los posibles impactos al llevar a cabo un cambio y establecer una mitigación ante su materialización (ej.: posibilidad de reversión a un estado funcional anterior)..
SC-36	Registro de cambios	Documentar el cambio y almacenar la información electrónicamente en una bitácora.

C-06 | Mantenimiento

ID	SUBCONTROL	DESCRIPCIÓN
SC-37	Conexión Remota	Utilización de protocolos seguros (SSH), encriptación de conexión (VPN), logs de auditoría y monitoreo en tiempo real.
SC-38	Mantenimiento de componentes	Considerar desgaste y vida útil de equipos, ejecutar labores de inspección y mantenimientos periódicos.
SC-39	Inventario y administración de activos	Supervisión general de los componentes de la red de control, con el fin de encontrar conexiones no autorizadas o averías en dispositivos.
SC-40	Control de Alertas	Definición de umbrales, con el fin de emitir alertas al personal y notificar oportunamente sobre fallas que puedan alterar el funcionamiento normal de los procesos, ya sea que puedan poner en riesgo la

		salud del personal y la ciudadanía, o bien tener repercusiones ambientales.
SC-41	Actualizaciones de Firmware	En muchas ocasiones es necesario mantener los equipos actualizados para recibir soporte del proveedor.
SC-42	Actualizaciones de *Software*	Al igual que el punto anterior, es necesario definir ventanas periódicas para mantener el *software* de estaciones de control actualizado, con el fin de tapar brechas de seguridad y asegurar el soporte del proveedor.
SC-43	Testeo de reglas *firewall*	Realización de pruebas periódicas, con el fin de comprobar que se está restringiendo el tráfico desde y hacia la red de control, de la forma, deseada.
SC-44	Respaldos	Realización de respaldos periódicos de información y configuraciones de componentes, red y seguridad.
SC-45	Soporte de proveedor	Utilización de mecanismos de autenticación seguros, contratos de soporte para *software* y componentes, definición de SLA's y escalación de incidentes.
SC-46	Desactivación o modificación oportuna de accesos	Revocación o modificación oportuna de privilegios para usuarios que han cambiado de rol dentro de la compañía o son dados de baja.

C-07 | Manejo de incidentes y recuperación

ID	SUBCONTROL	DESCRIPCIÓN
SC-47	Detección y Contención	Establecimiento de monitoreo pasivo de la red de control para encontrar activamente comunicaciones o comportamientos anómalos y activar oportunamente protocolos de seguridad.
SC-48	Protocolos de emergencia	Estos planes deberían de cubrir cualquier rango de incidente, incluyendo ciberataques. La conformación de una estructura de respuesta con personal competente es esencial.

		Los empleados deben conocer y estar entrenados en la ejecución de estos planes. Su finalidad radica en restaurar sistemas y servicios desde un nivel aceptable hasta sus niveles óptimos en el menor tiempo posible.
SC-49	Pruebas de penetración y funcionalidad de los planes	Ejecución periódica de ejercicios de seguridad simulando situaciones de emergencia para medir la efectividad de los planes y los controles de seguridad.
SC-50	Restauración de servicios y Reportes	Las acciones de recuperación deben documentarse paso por paso hasta que el sistema retorne a la normalidad. Además, se debe tomar nota de las lecciones aprendidas durante el incidente para evitar futuras fallas por las mismas causas o mejorar el tiempo de recuperación.

Resumen de controles esenciales

Control 01	**Documentos, Políticas y Procedimientos**
SC-01	Documentación del Sistema
SC-02	Protocolos de emergencia y evaluación de riesgos
SC-04	Entrenamientos Regulatorios
SC-05	Políticas de seguridad
Control 02	**Diseño Seguro**
SC-07	Separación de redes
SC-09	Segmentación
SC-13	Protección y localización de componentes
SC-16	Seguridad del personal
Control 03	**Seguridad Física**
SC-18	Limitación de acceso basada en roles
SC-19	Restricción de acceso a componentes del sistema
Control 04	**Seguridad Lógica**
SC-25	Cambio de contraseñas
SC-28	Restricción de acceso a Internet
SC-32	Registro de actividades de usuario
Control 05	**Gestión de Cambios**
SC-34	Ventanas de mantenimiento

SC-35	Análisis de riesgos
Control 06	**Mantenimiento**
SC-38	Mantenimiento de componentes
SC-39	Inventario y administración de activos
SC-40	Control de Alertas
SC-44	Respaldos
SC-45	Soporte de proveedor
Control 07	**Manejo de Incidentes y Recuperación**
SC-47	Detección y Contención
SC-48	Protocolos de emergencia

Recomendaciones para cortafuegos (*firewall*)

RECOMENDACIONES GENÉRICAS	
Reglas	▪ El conjunto de reglas de base debe ser denegar todo e ir permitiendo comunicaciones o servicios, según necesidades (listas blancas).
Internet	▪ Los dispositivos de la red de control no deben tener acceso a Internet.
Puertos y Servicios	▪ Habilitarse solamente de manera específica, según necesidades de cada caso.
Trafico entre red de control y red corporativa	▪ Todas las reglas deben restringir el tráfico a una dirección IP específica o rango de direcciones. Además, deben ser específicas para el puerto UDP/TCP. ▪ Denegar tráfico directamente desde la red corporativa hacia la red de control. ▪ Todo el tráfico saliente desde la red de control hacia la red corporativa debe estar estrictamente restringido por fuente y destino, así como también el servicio y puerto.
Administración	▪ Todo el tráfico de administración del *firewall* debe realizarse en una red separada o en una red cifrada con autenticación multifactor.
DMZ	▪ Todo el tráfico desde la red de control debe terminar en la DMZ, no permitir el tráfico directo desde la red de control a la red corporativa.
PROTOCOLOS	
DNS	▪ Las solicitudes de DNS de la red de control a la DMZ se otorgan caso por caso. ▪ Se recomienda el uso de un DNS local, o bien el uso de archivos de host.
HTTP	▪ En general, al protocolo HTTP no se le debería permitir cruzar de la red

	pública o corporativa a la red de control. ▪ En casos de excepción, aplicar control de acceso fuente/destino.
FTP y TFTP	▪ Toda comunicación, a través de TFTP debe bloquearse. ▪ FTP debería ser permitido solamente para sesiones salientes o si está asegurado con autenticación multifactor basada en token adicional y un túnel cifrado. ▪ Alternativas: SFTP y Secure Copy (SCP).
TELNET	▪ Las sesiones desde la red corporativa a la red de control deben prohibirse a menos que estén protegidas con autenticación multifactor basada en token y un túnel cifrado. ▪ Alternativa: SSH
DHCP	▪ Si la asignación dinámica es necesaria, se recomienda habilitar la indagación DHCP para defenderse contra servidores DHCP no autorizados.
SSH	▪ Se recomienda SSH como alternativa a telnet, rlogin, rsh, rcp y otras herramientas de acceso remoto inseguras.
SMTP	▪ El correo electrónico entrante no debe permitirse a ningún dispositivo de red de control. ▪ Los mensajes de correo SMTP salientes de la red de control a la red corporativa son aceptables para enviar mensajes de alerta.
SNPM	▪ La versión 3 es considerablemente más segura, pero todavía está limitada en uso. ▪ Los comandos SNMP V1 y V2, tanto desde como hacia la red de control deben estar prohibidos, a menos que se encuentren en una red de administración segura y separada.

Anexo 3. Lista de verificación para recolección de información

Compañía:		Fecha:	
Área:		Colaborador:	
Sistema:		Puesto:	
ÍTEM A EVALUAR		**EXISTENCIA**	**COMENTARIO**
Documentación, Políticas y Procedimientos			
Personal a cargo y roles.		☐	
Documentación sobre la versión del sistema y sus componentes.		☐	
Diagramas de interconexión del sistema		☐	

[Jerarquía, medios y protocolos de comunicación].		
Procedimientos acerca de la operación del sistema.	☐	
Políticas de seguridad y contraseñas.	☐	
Procedimientos o políticas sobre el control de cambios.	☐	
Administración de acceso físico.	☐	
Administración de acceso lógico.	☐	
Respuesta a incidentes [Protocolos de seguridad].	☐	
Respaldos y retención de la información.	☐	
Recuperación de desastres.	☐	
Entrenamientos periódicos del personal.	☐	
Concienciación del personal.	☐	
Seguridad del Diseño		
Requerimientos de control de tiempo [Procesamiento de información de sensores oportuna para la activación de actuadores].	☐	
Segregación de redes [Separación de la red industrial de la red de oficina].	☐	
Supervisión Sistema de centralizado capaz de obtener y desplegar información de todos los subsistemas y componentes.	☐	
Disponibilidad Adecuada evaluación del *uptime* del sistema en relación con sus componentes y conexiones.	☐	
Impacto ante fallas Capacidad de funcionamiento degradado	☐	

[De operación normal a funciones de emergencia].		
Localización de componentes Ubicación y conexión adecuada para la ejecución de mantenimientos.	☐	
Autenticación Autenticación entre componentes del sistema, a través de certificados o contraseñas complejas únicas y aleatorias por cada conexión.	☐	
Seguridad del personal Detección de condiciones inseguras y capacidad de alertar o ejecutar procesos de corrección automáticos.	☐	
Seguridad Física		
Limitaciones de acceso con base en roles (gabinetes o cuartos de equipos, comunicaciones y zonas de alto riesgo).	☐	
Restricción de acceso a componentes del sistema [sensores, paneles inteligentes, PLCs, etc.].	☐	
Protección del cableado.	☐	
Existencia de mecanismos de protección para componentes del sistema ante condiciones ambientales [temperatura, humedad, radiación polvo o vibración].	☐	
Registro de Acceso	☐	
Seguridad Lógica		
Implementación de seguridad en capas, donde las comunicaciones más críticas se encuentran en la capa más segura.	☐	
Servidor de autenticación.	☐	
Cambio de contraseña por defecto en *software* y componentes del sistema.	☐	

Complejidad de las contraseñas. [extensión y combinación de caracteres].	☐	
Cambio periódico de contraseña. [Recomendado: 30/60/90 días].	☐	
Software de protección contra *malware* (actualizado).	☐	
Desactivación de puertos y servicios no esenciales para la operatividad del sistema.	☐	
Restricción de privilegios mediante roles de seguridad.	☐	
Roles basados en el esquema del menor privilegio.	☐	
Utilización de mecanismos de autenticación separados [Red Industrial / Red de Oficina].	☐	
Comunicación inalámbrica cifrada (WPA2 Enterprise)	☐	
Utilización de protocolos de red conocidos y seguros (TLS/SSH/VPN).	☐	
Aplicación de encriptación en comunicaciones.	☐	
Autenticación entre dispositivos.	☐	
Restricción de comunicación directa entre la red de oficina y la red industrial.	☐	
Denegación de acceso desde y hacia Internet en los dispositivos de la red industrial.	☐	
Implementación de flujo de datos unidireccional hacia la red de oficina.	☐	
Tráfico entre la red industrial y la red de oficina restringido por puerto y tipo de servicio.	☐	
Whitelisting.	☐	
MAC Address Locking (seguridad de puertos ligando una dirección MAC a un puerto de *switch* administrable).	☐	
	☐	
Mecanismo de detección de	☐	

	☐	
Control de Cambios		
Cambios ejecutados durante ventanas de mantenimiento previamente programadas.	☐	
Implementación de un ambiente de pruebas antes de pasar los cambios a producción.	☐	
Uso de herramientas centralizadas para la gestión de actualizaciones.	☐	
Registro de los cambios.	☐	
Aprobación de los cambios.	☐	
Posibilidad de reversión a un estado anterior.	☐	
Mantenimiento		
Actualizaciones de *firmware* de componentes	☐	
Actualizaciones de *software* del sistema.	☐	
Frecuencia de actualizaciones.	☐	
Actualización de componentes. [*Software*/Firmware].	☐	
Monitoreo y registro de actividades.	☐	
Testeo periódico de las reglas de *firewall*.	☐	
Existencia de equipos de protección ante picos o caídas de voltaje.	☐	
Existencia de mantenimientos regulatorios a estos equipos.	☐	
Acceso remoto, a través de protocolos seguros: SSH/HTTPS/Token Based/Autenticación Doble Factor.	☐	
Contrato de soporte de proveedor / Sistema	☐	
Contrato de soporte de proveedor / Componentes de *hardware*	☐	
Actualización de componentes por obsolescencia [Impedimento de escalabilidad o utilización de protocolos inseguros].	☐	
Respuesta a Incidentes y Recuperación		

Existencia de componentes críticos redundantes.	☐	
Procesos alternos (ej.: autenticación / Ejecución Manual de procesos críticos).	☐	
Respaldos de información.	☐	
Respaldo de configuraciones.	☐	
Periodicidad de los respaldos.	☐	
Prueba de los respaldos.	☐	
Mecanismos de detección de instrucción.	☐	
Mecanismos de contención para evitar fallos en cascada.	☐	