DISEÑO DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE LA CIBERSEGURIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIAL (SCADA).

CHRISTIAN CAMILO MENDIETA MARTÍNEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

GIRARDOT

2020

DISEÑO DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE LA CIBERSEGURIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIAL (SCADA).

CHRISTIAN CAMILO MENDIETA MARTÍNEZ

Trabajo de grado presentado para optar por el título de Especialista en Seguridad Informática

DIRECTOR: MARTÍN CAMILO CANCELADO RUIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
GIRARDOT
2020

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Girardot, 11 de febrero de 2020.

DEDICATORIA

A mi padre y a mis tíos quienes abandonaron el mundo de manera intempestiva dejando un dolor imborrable en nuestras vidas.

A mi madre, por todo su apoyo en cada uno los proyectos emprendidos, por todo el amor que me ha brindado y por ser el soporte en momentos de dura enfermedad.

A mi familia, amigos y mi pareja por todo su apoyo, confianza y amor.

AGRADECIMIENTOS

Quiero agradecer en primer lugar a mi madre por todo el apoyo brindado para poder dedicar el tiempo suficiente al estudio y luego al desarrollo de este proyecto.

A mi familia, mi pareja y mis amigos por su acompañamiento durante este durísimo año.

A los profesionales a quienes indagué por información que me permitiera desarrollar este documento, sus contribuciones han sido de gran importancia y fueron tomadas en cuenta siempre, entre ellos al Ingeniero Martín Camilo Cancelado Ruíz por la guía que me brindó para el desarrollo de la monografía y al Ingeniero Christian Reynaldo Ángulo por sus importantes aclaraciones y explicaciones que me ayudaron a desarrollar un documento más sólido.

TABLA DE CONTENIDO

INTRODUCCIÓN 12
PLANTEAMIENTO DEL PROBLEMA 14
DEFINICIÓN DEL PROBLEMA 14
DESCRIPCIÓN DEL PROBLEMA 14
FORMULACIÓN DEL PROBLEMA 15
JUSTIFICACIÓN 16
ALCANCES Y LIMITACIONES 18
ALCANCE 18
LIMITACIONES 18
OBJETIVOS 19
OBJETIVO GENERAL 19
OBJETIVOS ESPECÍFICOS 19
1. MARCO REFERENCIAL 20
1.1 ANTECEDENTES 20
1.2 MARCO TEÓRICO 22
1.2.1 Sistemas de control industrial 22
1.2.2 Evolución de los sistemas de control industrial. 24
1.2.3 Elementos de un sistema de control industrial 25
1.2.4 Protocolos 31
1.2.5 Definición de seguridad en los sistemas de control industrial 34
1.2.6 Vulnerabilidades comunes y factores de riesgo 34
1.2.7 Protección de los sistemas de control industrial 35
1.3 MARCO CONCEPTUAL (GLOSARIO DE TÉRMINOS) 36
1.4 MARCO CONTEXTUAL 37
1.5 MARCO LEGAL 37
2. ESTADO DEL ARTE 39
3. ACTUALIDAD DE SISTEMAS DE CONTROL INDUSTRIAL Y METODOLOGÍAS DE EVALUACIÓN 40

3.1 ACTUALIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIAL 40
3.2 ACTUALIDAD DE LAS METODOLOGÍAS DE EVALUACIÓN 47
3.2.1 IEC 62443.....47
3.2.2 NERC CIP 002-009 48
3.2.3 NIST SP800-82.....48
3.2.5 NESCOR 49
4. PROBLEMAS DE SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL.....50
4.1 FUENTES DE AMENAZA.....50
4.2 AMENAZAS.....51
4.2.1 Amenazas intencionales.....52
4.2.2 Amenazas accidentales.....52
4.2.3 Amenazas estructurales. 53
4.2.4 Amenazas ambientales. 54
4.3 VULNERABILIDADES.....54
4.3.1 Vulnerabilidades en políticas y procedimientos. 55
4.3.2 Vulnerabilidades en la arquitectura y el diseño del ICS.....56
4.3.3 Vulnerabilidades de configuración y mantenimiento.....56
4.3.4 Vulnerabilidades de índole físico. 57
4.3.5 Vulnerabilidades en el software. 58
4.3.6 Vulnerabilidades en las comunicaciones y configuraciones de red. 58
5. PASOS METODOLÓGICOS DE LA EVALUACIÓN DE SEGURIDAD 60
5.1 DEFINICIÓN DEL ALCANCE Y TÉRMINOS DE LA EVALUACIÓN.....60
5.1.1 Objetivo de la evaluación 60
5.1.2 Alcance de la evaluación.....61
5.1.3 Limitaciones de la evaluación.....61
5.1.4 Objeto de evaluación. 61
5.1.5 Roles y responsabilidades.....62
5.1.6 Ubicación del evaluador 62
5.1.7 Tipo de evaluación 62
5.1.8 Equipamiento del evaluador 63

5.1.9 Cronograma de la evaluación....63
5.1.10 Comunicaciones....64
5.1.11 Manejo de la evidencia....64
5.1.12 Autorización....64
5.2 RECOLECCIÓN DE INFORMACIÓN....65
5.2.1 Técnicas de recolección pasivas.....65
5.2.2 Técnicas de recolección activas....68
5.3.3 Checklist para activos hallados. 69
5.3 ANÁLISIS DE VULNERABILIDADES....70
5.3.1 Vulnerabilidades de los sistemas de control industrial. 71
5.3.3 Checklist análisis de vulnerabilidades. 72
5.4 VERIFICACIÓN DE LOS CONTROLES IMPLEMENTADOS....73
5.5 PRESENTACIÓN DE LOS RESULTADOS DE LA EVALUACIÓN....76
5.5.1 Objetivo de la evaluación de seguridad.....77
5.5.2 Tiempo total de la evaluación.....77
5.5.3 Alcance y limitaciones de la prueba. 77
5.5.4 Objetos de evaluación....77
5.5.5 Descripción de las amenazas y vulnerabilidades encontradas 77
5.5.6 Descripción de los controles hallados. 78
5.6.7 Recomendaciones....78
6. REPRESENTACIÓN GRÁFICA DE LA METODOLOGÍA DE EVALUACIÓN .79
CONCLUSIONES 81
RECOMENDACIONES....83
BIBLIOGRAFÍA....85
RESUMEN ANÁLITICO ESPECIALIZADO (RAE) 91

LISTA DE TABLAS

Tabla 1. Amenazas intencionales. 52
Tabla 2. Amenazas accidentales. 53
Tabla 3. Amenazas estructurales.....53
Tabla 4. Amenazas ambientales.....54
Tabla 5. Vulnerabilidades en políticas y procedimientos. 55
Tabla 6. Vulnerabilidades en la arquitectura y el diseño.....56
Tabla 7. Vulnerabilidades de configuración y mantenimiento. 56
Tabla 8. Vulnerabilidades físicas. 57
Tabla 9. Vulnerabilidades en el software. 58
Tabla 10. Vulnerabilidades en las comunicaciones y configuraciones de red. 59
Tabla 11. Checklist identificación de activos.....70
Tabla 12. Checklist análisis de vulnerabilidades.....73
Tabla 13. Evaluación de controles implementados.....74

LISTA DE FIGURAS

Figura 1. Diseño general de un sistema SCADA. 23
Figura 2. Controlador Lógico Programable (PLC).....26
Figura 3. Robots industriales. 27
Figura 4. RTU. 28
Figura 5. Periferia distribuida. 29
Figura 6. Human Machine Interface (HMI). 30
Figura 7. Intelligence Electronic Device (IED). 30
Figura 8. Países con mayores ataques de ransomware a sus ICS. 41
Figura 9. Países con menos ataques a sus ICS. 41
Figura 10. Empresas víctimas de ataques a sus sistemas de control industrial. ...42
Figura 11. Porcentaje de ataques desde diferentes fuentes de amenaza. 42
Figura 12. Vulnerabilidades encontradas en ICS desde 2013 hasta 2018. 43
Figura 13. Vulnerabilidades por proveedor de equipos. 44
Figura 14. Tipos de vulnerabilidades en ICS en 2017. 44
Figura 15. Tipos de vulnerabilidades en ICS en 2018. 45
Figura 16. Vulnerabilidades en componentes ICS en 2017 y 2018. 45
Figura 17. Criticidad de las vulnerabilidades en ICS en 2017 y 2018. 46
Figura 18. Documentos de la serie IEC 62443 47
Figura 19. Representación gráfica de la metodología de evaluación propuesta. ...80

RESUMEN

Los sistemas de control industrial se conforman por un conjunto de dispositivos conectados que recogen y analizan información para controlar de forma automatizada procesos industriales complejos. Por lo general, son sistemas estables y robustos que requieren de poca intervención humana para realizar su actividad, puesto que esta es repetitiva y está programada desde el inicio para desarrollarse de una forma específica. Si bien es cierto que son sistemas robustos y confiables para su labor, esto no quiere decir que sean seguros o que estén preparados para conectarse a redes no confiables como Internet, incluso cuando cuentan con los puertos y los protocolos que le permiten conectarse a esas redes. Muchos sistemas de control industrial no cuentan con componentes de seguridad informática en sus protocolos, ni con dispositivos que garanticen la disminución de los riesgos en esos entornos y es solo recientemente cuando la industria de las TIC empieza a mirar estos entornos y su seguridad. Los sistemas de control industrial se encuentran en todos los procesos críticos de la economía y también son fundamentales para la seguridad nacional, es por ello, que su protección y aseguramiento son una tarea fundamental en nuestro tiempo.

Una metodología que permita evaluar la seguridad en los sistemas de control industrial se constituye en una herramienta muy importante e imprescindible para tener una mejor perspectiva del estado de la seguridad de los sistemas de control evaluados y sus resultados se pueden usar como la base para entender cómo protegerlos a futuro. En este proyecto de trabajo de grado se pretende diseñar una metodología para la evaluación de la ciberseguridad en los sistemas de control industrial que satisfaga las necesidades del sector en Colombia. Para conseguir ese objetivo, en primer lugar, se recolectará información técnica referente a los sistemas de control industrial SCADA y las metodologías de evaluación de ciberseguridad existentes en la actualidad, con el fin de establecer una base teórica firme que permita avanzar en el proceso. En segundo lugar, se buscará identificar las principales amenazas, ataques, vulnerabilidades y controles de seguridad relacionados a los sistemas de control industrial. En tercer lugar, se definirán los pasos metodológicos que permitirán adelantar la evaluación de seguridad sobre el sistema de control industrial. Finalmente, se presentará la metodología diseñada con el fin de que pueda ser usada por todas las partes interesadas en los sistemas de control industrial y su seguridad.

INTRODUCCIÓN

Desde hace mucho tiempo el hombre ha creado máquinas que facilitan sus labores, aumentan su productividad y realizan trabajos repetitivos. Estas máquinas antes de la llegada de la electricidad eran dispositivos mecánicos constituidos principalmente por poleas, palancas y piñones que realizaban la acción que fue diseñada siguiendo las órdenes de un operador. A pesar de su uso extendido, las máquinas tenían funciones fijas y muy limitadas que dependían de la potencia de la hidráulica, el vapor o la tracción animal.

La llegada de la electricidad a la industria mejoró notablemente las características de potencia de los sistemas e introdujo las bases del control industrial; se empezaron a desarrollar dispositivos eléctricos que realizaban tareas complejas y simplificaban el tamaño de los sistemas industriales. Sin embargo, a pesar de que estas nuevas tecnologías mejoraron los sistemas de industriales, estos aún estaban compuestos por una gran cantidad de componentes electromecánicos unidos por un cableado complejo.

A inicios de 1970, la industria automovilística americana lanza al mercado el MODICON 084 un controlador lógico programable (PLC, *Programmable Logic Controller)* que ejecutaba un programa preestablecido que tenía como entradas señales eléctricas provenientes de elementos del sistema y salidas digitales o analógicas que controlan otros componentes, como válvulas, motores, o switches, fue así como desde la aparición del PLC, la automatización y el control industrial ha avanzado de manera ininterrumpida, encontrando en el mercado diversas tecnologías con diferentes funcionalidades para una gran cantidad de procesos, que han ido creciendo en sus capacidades de forma exponencial, adhiriendo características como soporte de lenguajes de programación y conectividad a través de tecnologías más populares como WIFI, Ethernet, USB, o Bluetooth.

El ámbito de aplicación de los sistemas de control industrial se extiende a una gran cantidad de industrias, como la energética, acueductos, aguas residuales, producción de alimentos, petróleo, gas natural, transporte, farmacéutica, automotriz, o militar y aunque inicialmente eran sistemas que se encontraban aislados, que ejecutaban protocolos de control propietarios y utilizaban hardware y software especializado, lo cierto es que, la expansión de los dispositivos IP ha desplazado

las soluciones propietarias debido a su gran disponibilidad y bajo costo, razón por la cual, la seguridad de estos sistemas se ve más expuesta a las redes convencionales, incrementando la necesidad de asegurarlos.

Los sistemas de control industrial por las características de su operación y su funcionalidad son muy importantes para los intereses económicos y el funcionamiento de las infraestructuras críticas de Colombia, es por ello, que en el presente documento se pretende aportar una herramienta que ayude a los gobiernos, las organizaciones involucradas y a los profesionales del sector a pensar en cómo proteger los sistemas de control industrial.

PLANTEAMIENTO DEL PROBLEMA

DEFINICIÓN DEL PROBLEMA

Se requiere diseñar un método para la evaluación de la seguridad de los sistemas de control industrial de forma técnica y organizada, que permita conocer el estado de su seguridad y servir de base para desarrollar estrategias de mitigación frente a posibles amenazas y vulnerabilidades.

DESCRIPCIÓN DEL PROBLEMA

Los sistemas de control industrial se encuentran prácticamente en todas las empresas que requieren del control y automatización de sus procesos, incluyendo sectores de la industria de bienes y servicios, así como infraestructuras críticas[1]. Desde hace varios años con la aparición de Stuxnet estos sistemas vienen siendo víctimas de ataques especializados que han tenido implicaciones importantes en su seguridad y pueden producir efectos desastrosos en infraestructuras críticas, como es el caso de Industroyer, un malware capaz de controlar directamente los interruptores de una subestación eléctrica y causante de un gran apagón eléctrico en Ucrania en diciembre de 2016[2].

Los ataques a sistemas de control industrial tienden a aumentar, mientras no se tomen medidas preventivas, como la actualización de los sistemas y la detección temprana de amenazas mediante inspecciones constantes[3]. Un mecanismo que puede ayudar en el aseguramiento y mitigación de las amenazas y ataques en los sistemas de control es la evaluación de la seguridad siguiendo una metodología formal y técnica.

---

[1] REVISTA DINERO. Plantas industriales de alto desempeño en Colombia. {En línea}. {09 de mayo de 2018}. Disponible en: https://www.dinero.com/edicion-impresa/informe-especial/articulo/plantas-industriales-alto-desempeno-colombia/198889

[2] CHEREPANOV, Anton. Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet. {En línea}. {09 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/

[3] COBB, Stephen. Aumentan los ataques a infraestructuras críticas. 1 ed. ESET, pp.11-13. [ebook]. {En línea}. {09 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

FORMULACIÓN DEL PROBLEMA

¿Cómo brindar unas pautas generales clave para evaluar la seguridad en los sistemas de control industrial de manera formal y técnica?

JUSTIFICACIÓN

Los sistemas de control industrial gestionan procesos muy importantes en diferentes sectores de la industria y también en las infraestructuras críticas del país. Es por ello, que la materialización de una amenaza de ciberseguridad en un sistema de control industrial puede traer consecuencias desastrosas, no sólo para el funcionamiento de una industria en específico sino también a la seguridad nacional de un país, como ha quedado evidenciado con incidentes como el virus Stuxnet en Irán o el ransomware Industroyer en Ucrania[4].

Los sistemas de control industrial son robustos y estables, gestionan y automatizan procesos muy complejos y se encuentran presentes desde hace mucho tiempo en la industria y en las infraestructuras críticas de muchos países, pero tienen ciclos de actualización muy largos y en su diseño inicial no fueron concebidos para conectarse a redes poco confiables como internet o redes públicas, de hecho muchos tienen protocolos de comunicación propietarios que no tienen capas de seguridad, como autenticación o cifrado; y esto es un factor de debilidad muy común. Todo esto hace que conocer el estado actual de la seguridad de un sistema de control industrial se vuelva una prioridad al momento de fortalecerlo y protegerlo frente a amenazas o ataques informáticos.

Una metodología para evaluar la seguridad de los sistemas de control industrial permite conocer el estado actual de la seguridad del sistema evaluado, evidenciar las amenazas y vulnerabilidades a las que está expuesto, los ataques de los que puede ser víctima, servir de base para implementar los controles de seguridad que pueden reducir el impacto de la materialización de una amenaza y disminuir el riesgo de ocurrencia[5].

Éste trabajo de grado busca diseñar una metodología que permita realizar la evaluación de los sistemas de control industrial con base en las metodologías de test de penetración actuales y el conocimiento general de los sistemas de control industrial, buscando aportar una herramienta metodológica formal a todos las partes

[4] CERTSUPERIOR. Protección de Sistemas Industriales. {En línea}. {20 de mayo de 2018}. Disponible en: https://www.certsuperior.com/Blog/proteccion-de-sistemas-industriales.
[5] HERRERO, Miguel. Guía de seguridad de Sistemas de Control Industrial. {En línea}. {24 de mayo de 2018}. Disponible en: https://www.certsi.es/blog/guia-nist

involucradas en el fortalecimiento de la seguridad de dichos sistemas y aportando al sector un documento que les permita afrontar este nuevo escenario de la ciberseguridad, que son los sistemas de control industrial.

ALCANCES Y LIMITACIONES

ALCANCE

En este proyecto se pretende diseñar una metodología para realizar evaluaciones de seguridad a los sistemas de control industrial. Se expone una visión general de los sistemas de control industrial, se establecen pautas para definir el alcance de una evaluación de seguridad, los términos de la evaluación, la forma en la que se recolecta la información sobre los activos objeto de evaluación, se mencionan las técnicas para la determinación de las amenazas y vulnerabilidades en los sistemas de control industrial, se diseñan listas de chequeo de los controles más importantes y se da una guía para la elaboración del informe de la evaluación.

LIMITACIONES

El documento no está destinado a ser una norma o un manual paso a paso para evaluar un sistema de control industrial. Tampoco pretende limitar el tipo de sistema de control a evaluar, y no se mencionan herramientas de software o hardware específicas.

El ámbito de aplicación del proyecto se restringe a los sistemas de control industrial regidos por la normatividad nacional de la república de Colombia.

OBJETIVOS

OBJETIVO GENERAL

Diseñar una metodología para la evaluación del estado de la ciberseguridad en los sistemas de control industrial.

OBJETIVOS ESPECÍFICOS

- Recolectar información referente a sistemas de control industrial y metodologías de evaluación de seguridad informática.

- Identificar las amenazas, las vulnerabilidades más comunes, los principales ataques y los controles de seguridad a tener en cuenta en los sistemas de control industrial.

- Definir los pasos metodológicos para la evaluación de seguridad en los sistemas de control industrial.

- Presentar el diseño de la metodología de evaluación de seguridad en sistemas de control industrial.

1. MARCO REFERENCIAL

1.1 ANTECEDENTES

En la actualidad, existen muchas metodologías para realizar evaluaciones de seguridad en los sistemas informáticos y estas difieren entre sí en la forma en la que abordan la evaluación de seguridad y el sistema informático objeto de estudio.

Information Systems Security Assessment Framework (ISSAF), es una metodología de evaluación de la seguridad en sistemas de información desarrollada en el año 2006 por el Open Information Systems Security Group, que busca evaluar las políticas y procesos de seguridad de la información de una organización, teniendo en cuenta los estándares y leyes aplicables. Con ISSAF se pueden realizar pruebas de penetración para identificar las vulnerabilidades que pueden generar riesgos potenciales para los activos de información de una compañía[6]. ISSAF organiza la información en criterios de evaluación definidos y revisados por expertos en cada uno de esos dominios. Estos criterios de evaluación incluyen: Una descripción de los criterios de evaluación, sus fines y objetivos, los requisitos previos para realizar las evaluaciones, el proceso para la evaluación, los resultados esperados, las contramedidas recomendadas, y referencias a documentación externa[7].

ISSAF no ha sido actualizado desde el lanzamiento de la versión 0.21 y en la actualidad se encuentra en desuso[8].

PENETRATION TESTING MODEL BY BSI, es una metodología para realizar evaluaciones de seguridad que fue creada en Alemania en el año 2008 por la oficina federal para la seguridad de la información (En alemán BSI), en él se sigue el proceso del test de penetración desde la solicitud de una propuesta hasta la finalización de la prueba. El modelo consta de 5 fases, estás son preparación, reconocimiento, análisis de información y riesgos, intentos activos de intrusión y análisis final[9]. También en el año 2008 el National Institute of standards and

[6] OISSG. ISSAF. {En línea}. {09 de mayo de 2018}. Disponible en: http://www.oissg.org/issaf.
[7] RATHORE, Balwant. DILAJ, Miguel & HERRERA, Omar. Information Systems Security Assessment Framework (ISSAF). 0.21 ed. 2006, p. 18.
[8] BERGEL, Gabriel. #11PathsTalks: metodologías testing de seguridad. {En línea}. {09 de mayo de 2018}. Disponible en: https://www.youtube.com/watch?v=r2VidIXdKOc
[9] BSI. A Penetration Testing Model by BSI. 1 ed. 2009, pp. 4-8.

Technology (NIST) publica la metodología NIST SP 800-115, que tiene como objetivo principal proporcionar recomendaciones prácticas para diseñar, implementar y administrar información técnica relacionada con las evaluaciones de seguridad de un sistema o red y verificar el cumplimiento de una política de seguridad u otros requisitos.

Penetration Technical Guidelines (PTES), es una metodología que proporciona a los proveedores de servicios de seguridad un lenguaje común y un alcance para realizar evaluaciones de seguridad. Se desarrolló en el 2009 por parte de varios expertos en seguridad de todas las áreas de la industria[10]. El estándar consta de siete secciones principales en las que se cubre todo lo relacionado con una prueba de penetración desde las interacciones previas al contrato de auditoría, la recolección de información, el modelado de amenazas, el análisis de vulnerabilidades, la explotación, la post-explotación, y el reporte final[11].

Hacia finales de 2010 ISECOM publica la versión 3 de la metodología The Open Source Security Testing Methodology Manual (OSSTMM), creada por Pete Herzog. En la actualidad, la versión 4 se encuentra en desarrollo. El propósito de OSSTMM es ofrecer una metodología científica para la medición de la seguridad operacional, las interacciones humanas y todas las formas de comunicación, como inalámbrica, cableada, analógica y digital y ser una guía para el desarrollo de una auditoría que asegure la rigurosidad de la evaluación, evitar falsos positivos, cumplir con las regulaciones, y cuantificar los resultados[12].

En el Reino Unido (UK) Kevin Orrey publica en el año 2014 la metodología para la evaluación de seguridad conocida como PENETRATION TESTING FRAMEWORK 0.59, en la que se encuentran guías y herramientas que se pueden utilizar para hacer el reconocimiento pasivo, así como ataques de password cracking, y testing a diferentes infraestructuras, sistemas y redes. No es un estándar muy utilizado puesto que se encuentra en continuo desarrollo y no tiene una versión estable[13].

---

[10] FAQ - The Penetration Testing Execution Standard. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.pentest-standard.org/index.php/FAQ

[11] Ibíd.

[12] HERZOG, Pete. OSSTMM Open Source Security Testing Methodology Manual. 3 ed. New York: ISECOM, 2010, p.12-15.

[13] Penetration Testing Framework 0.5. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html#

En el año 2017 se lanza la actualización más reciente de OWASP, que es una metodología desarrollada por el Open Web Application Security Project, una organización mundial sin ánimo de lucro que tiene como finalidad hacer visible importancia de la seguridad del software. OWASP pone a disposición de cualquier persona u organización herramientas y documentación relacionada con la seguridad en las aplicaciones web[14]. OWASP pone a disposición de la comunidad el OWASP Top Ten 2017, un documento sobre la seguridad en aplicaciones web en el que se plantean los riesgos más críticos para las aplicaciones web, de acuerdo con la experiencia de miembros del proyecto y expertos en seguridad en todo el mundo[15].

Finalmente, en abril de 2018 el NIST publica la versión 1.1 del Framework for Improving Critical Infrastructure Cybersecurity, el cual es desarrollado para mejorar la gestión del riesgo de cibersegruidad en tecnologías de la información, sistemas de control industrial, sistemas ciberfísicos e internet de las cosas. El marco ayuda a las organizaciones, independientemente de su tamaño, grado de riesgo de seguridad o sofisticación de seguridad, a aplicar los principios y buenas prácticas de gestión de riesgos para mejorar su seguridad y su resistencia a los ataques[16].

1.2 MARCO TEÓRICO

1.2.1 Sistemas de control industrial

Los sistemas de control industrial se pueden describir como un conjunto de elementos, sensores y actuadores, conectados a dispositivos de control en los que se ejecutan programas específicos que se encargan de administrar, supervisar y controlar de forma automatizada uno o varios procesos industriales fundamentales[17]. Los sistemas de control industrial se conocen también como ICS (Industrial Control Systems), e incluyen a los sistemas de control y supervisión de datos (SCADA - Supervisory Control And Data Acquisition), los sistemas de control distribuido (DCS – Distributed Control Systems), y otros menos robustos como los controladores lógicos programables (PLC – Programmable Logic Controllers). Los sistemas de control se usan en muchas industrias que difieren entre sí en cuanto al proceso que adelantan, como la industria eléctrica, industrias de petróleo y gas, acueductos, industrias de transporte, productos químicos, automotriz, imprentas,

[14] OWASP. {En línea}. {10 de mayo de 2018}. Disponible en: https://www.owasp.org/index.php/Main_Page
[15] OWASP Project. OWASP Top 10 - 2017. 1 ed. 2017, p. 7.
[16] NIST. Framework for Improving Critical Infrastructure Cybersecurity. 1.1 ed. 2018, pp 1-10.
[17] PÉREZ SAN-JOSÉ, Pablo. Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA). 2012. pp 17-30.

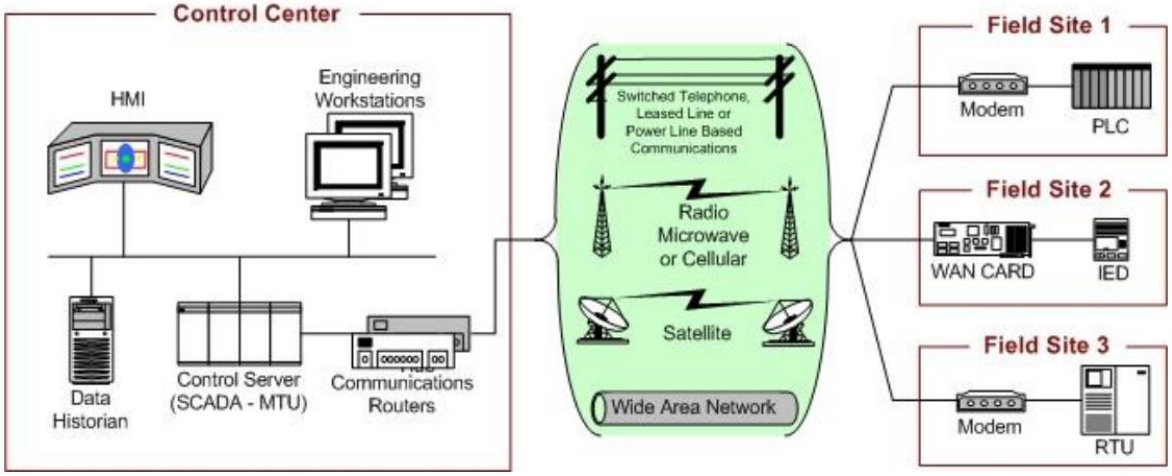
fabricación de alimentos, bebidas y control de tráfico aéreo. Los sistemas de control son de vital importancia para la economía y el funcionamiento de los países.

Los sistemas SCADA se utilizan por lo general para controlar y monitorear activos dispersos mediante la adquisición, el control y la supervisión de datos centralizado, ejemplo de esto son las estaciones meteorológicas, centros de tratamiento de agua, industrias energéticas, gas, entre otras.

Los sistemas de control distribuido (DCS – Distributed Control Systems) se usan para controlar los sistemas de producción dentro de un área local, como por ejemplo la imprenta de un periódico o la línea de ensamblaje de una empresa. Finalmente, los controladores lógicos programables (PLC – Programmable Logic Controllers) se utilizan para el control discreto de aplicaciones específicas de supervisión y control regulado, como pueden ser controles de ventilación, calefacción y aire acondicionado.

En la práctica los sistemas de control industrial se componen de PLCs, DCSs y SCADA y los profesionales del sector para referirse en general a un sistema de control industrial suelen llamarlo SCADA.

Figura 1. Diseño general de un sistema SCADA.



Fuente: STOUFFER, Keith. PILLITTERI, Victoria [Imagen]. Guide to Industrial Control Systems (ICS) Security. 2da Edición. Washington: NIST 2015. pp 21.

1.2.2 Evolución de los sistemas de control industrial.

En sus inicios los sistemas de control fueron diseñados para procesos tecnológicamente simples, eran sistemas aislados que ejecutaban protocolos de control propietarios mediante hardware y software especializado, las medidas de seguridad con las que contaba por lo general eran físicas y no estaban conectados a las redes TI, a medida que la tecnología avanza y con ella los procesos industriales, los sistemas de control industrial se fueron volviendo cada más complejos, llegando a tener hoy en día sistemas en los que conviven diferentes tecnologías, que incluso se conectan a Internet para ser controladas remotamente[18]. El bajo costo y la alta disponibilidad en el mercado de los dispositivos IP (Internet Protocol), ha provocado que las industrias empiecen a utilizarlos en los sistemas de control, aumentando la posibilidad de sufrir amenazas o estar expuestos a vulnerabilidades e incidentes de seguridad. Por lo cual, hoy en día es más necesario el aseguramiento de estos sistemas.

En Colombia cada vez son más las compañías que se conectan a Internet[19], y con ellas sus sistemas de control, situación que representa un grave riesgo para la seguridad y funcionamiento de estas industrias si no se tienen en cuenta medidas de protección frente a las amenazas de seguridad de los sistemas de control industrial. Según expertos en seguridad informática los ataques a los sistemas de control industrial vienen en aumento desde hace algunos años y seguirán creciendo durante los siguientes años y con ellos la probabilidad de la materialización de una amenaza, puesto que, muchos sistemas de control industrial en su diseño inicial no fueron concebidos para ser conectados a Internet y aunque muchos se están actualizando, esto no disminuye el riesgo, debido a que se están remplazando dispositivos con circuitos integrados de aplicaciones específicas (ASIC) por sistemas en arquitecturas de sistemas en chip (SoC) que tienen vulnerabilidades conocidas y fácil acceso librerías de código[20].

---

[18] SOTO, Carlos. (SCADA, el peligro asecha a los sistemas de infraestructura crítica. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.securitic.com.mx/reportaje-especial/2373-scada-el-peligro-asecha-a-los-sistemas-de-infraestructura-critica

[19] COLPRENSA BOGOTÁ. (2015). Más de 74% de pequeñas y medianas empresas están conectadas a Internet. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.vanguardia.com/mundo/tecnologia/323706-mas-de-74-de-pequenas-y-medianas-empresas-estan-conectadas-a-internet

[20] COBB, Stephen. TENDENCIAS EN CIBERSEGURIDAD 2018: EL COSTO DE NUESTRO MUNDO CONECTADO. {En línea}. {10 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

Con el uso creciente de dispositivos IP, redes inalámbricas y demás dispositivos provenientes de las redes TI convencionales, los sistemas de control industrial han heredado nuevos riesgos de seguridad, lo que provoca que haya un menor aislamiento para el sistema de control industrial comparado con sus predecesores y una mayor exposición a amenazas, vulnerabilidades e incidentes de seguridad que no son propias de su naturaleza, esto representa un desafío importante para las organizaciones y para los profesionales del sector, además es importante, puesto que los sistemas de control intervienen en procesos clave para la salud, seguridad, medio ambiente, los sistemas financieros y los procesos de producción de un país y una falla de seguridad en una infraestructura crítica puede provocar un impacto negativo profundo en la economía y en la seguridad nacional, llegando incluso a causar víctimas mortales.

1.2.3 Elementos de un sistema de control industrial

1.2.3.1 PLC. Los controles lógicos programables (en inglés, Programmable Logic Controller) son dispositivos diseñados específicamente para el control industrial, su aplicación está ligada al control de una única máquina o un único proceso, no interrelacionados con otros procesos o máquinas vecinas. Los PLC son diseñados para soportar un entorno industrial con altas temperaturas, polvo, humedad, vibraciones, etc. Su sistema operativo es de inicio rápido y muy estable. Por lo general, tienen memorias de estado sólido. Son compactos, no tienen partes móviles. Tienen entradas y salidas con niveles y protección industriales. Tienen un tiempo de vida mucho mayor a muchas tecnologías electrónicas.

En la unidad de procesamiento de los PLC se ejecuta el programa de control que tiene como entrada la información enviada por sensores y detectores, que a su vez recogen datos de la instalación. Sus salidas son contactos eléctricos o señales que actúan sobre diferentes elementos de la máquina, como motores, válvulas o pilotos.

Los PLC son parte importante de los sistemas de control industrial debido a que se usan para la administración local de procesos que se ejecutan a través de sensores o actuadores, aunque en algunos casos se usan como unidades terminales remotas, debido a que algunos vienen con implementaciones de conexión a redes GPRS, WIFI, o LAN.

Figura 2. Controlador Lógico Programable (PLC)

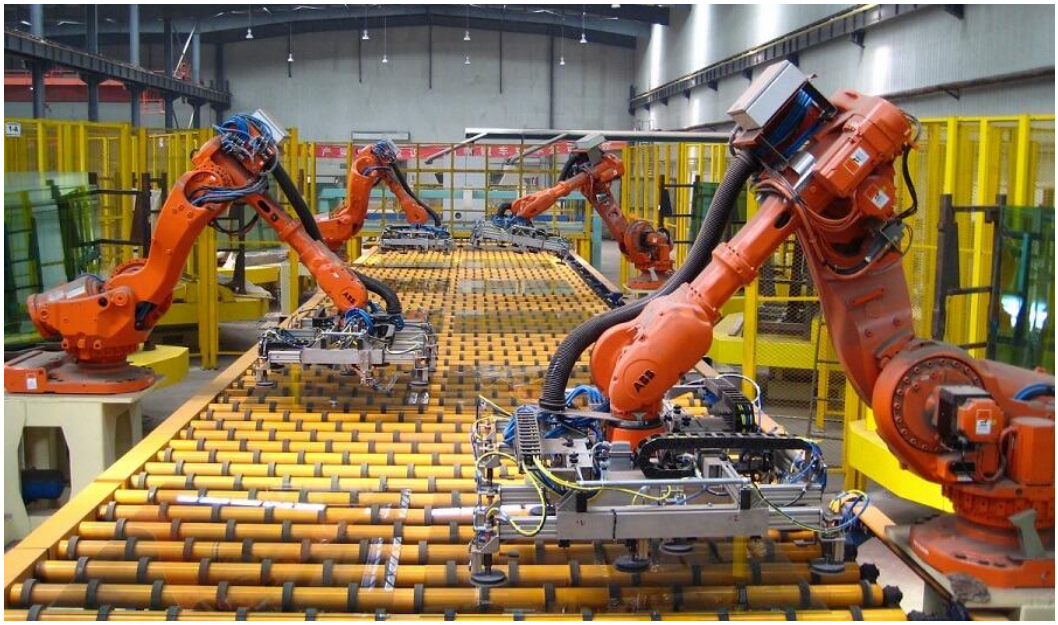
Fuente: FERNANDEZ, Oscar. Código Electrónica [imagen]. Qué es un PLC Siemens logo. [Consultado: 19 de febrero de 2019]. Disponible en: http://codigoelectronica.com/blog/que-es-un-plc-siemens-logo

1.2.3.2 DCS. Los sistemas de control distribuidos (en inglés, Distributed Control Systems), se componen de un conjunto de dispositivos inteligentes con una funcionalidad determinada que se comunican entre sí para controlar un proceso productivo más o menos extenso en una misma ubicación física. De manera adicional a los dispositivos de control, incorporan también workstations para la programación, configuración, monitorización, control, recopilación de datos y comunicación con sistemas superiores. Además de funcionalidades de PLC industriales, los DCS incorporan funciones avanzadas de gestión de eventos, alarmas de proceso, optimización de recursos, Hot Swappping o cambios en caliente, control de activos, entre otras características.

La ventaja principal de los DCS es la de disponer en una sola solución de un fabricante de todos los módulos software y hardware necesarios para el control industrial de un proceso de tipo mediano o grande. Los lenguajes de programación y configuración son propietarios de cada de fabricante y por lo general, se utilizan en instalaciones industriales donde existen gran cantidad de procesos interrelacionados entre sí en una misma localización geográfica, por ejemplo, instalaciones de petróleo y gas, plantas químicas, etc.

1.2.3.3 Robots y Máquinas dedicadas. Son componentes electromecánicos estándar, capaces de realizar manipulaciones y acciones repetitivas, pero con una máxima precisión. Su control por lo general se realiza mediante dispositivos propietarios del fabricante, algunos de ellos basados en PC. Regularmente, se conectan con el exterior a través de conexiones Ethernet, mediante protocolos propios, tanto para el envío del programa, como para la monitorización de los datos. También suelen tener conectividad con buses de campo, como periferia distribuida.

Figura 3. Robots industriales.

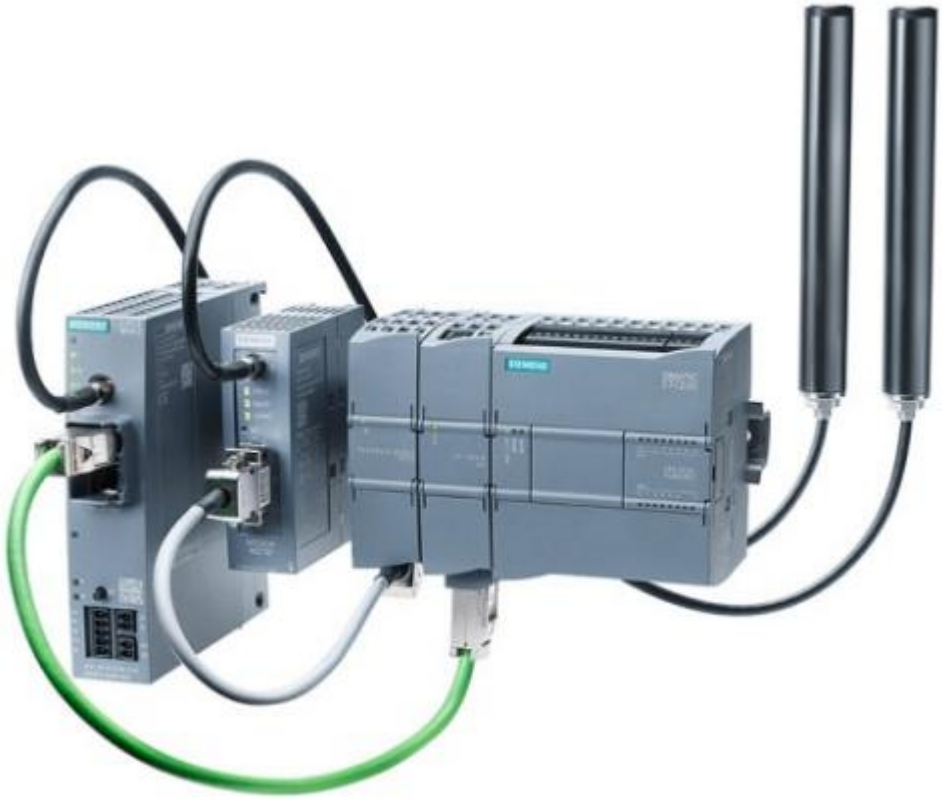


Fuente: MATSUZAKI, Kan. Desinformemonos.org [imagen]. Más robots, menos derechos: tendencias laborales en la industria de productos electrónicos. [Consultado: 20 de febrero de 2019]. Disponible en: https://desinformemonos.org/mas-robots-menos-derechos-tendencias-laborales-la-industria-productos-electronicos/

1.2.3.4 Control por PC y dispositivos híbridos. En una planta industrial es frecuente encontrar ordenadores personales haciendo tareas de configuración, monitorización y comunicación con sistemas superiores. También se encuentran en tareas de control como PLC, DCS o robots.

1.2.3.5 RTU. Unidad de terminal remota (en inglés, Remote Terminal Unit), son dispositivos diseñados para la adquisición y transmisión de datos a un control superior más o menos lejano (remoto). Por lo general, tienen conectividad Ethernet, Radio, GPRS, Sátelite, redes TETRA, etc. Algunas RTU incorporan procesamiento local para la ejecución de pequeñas secuencias de control de forma autónoma, como si fuera un pequeño PLC. Las RTU se usan comúnmente en lugares alejados del centro de control, que no requieren el envío de medidas en tiempo real, por ejemplo, instalaciones de abastecimiento de agua, sistemas de monitorización de movimientos telúricos, etc.

Figura 4. RTU.



Fuente: Siemens. Modular RTUs [imagen]. Modular Remote Terminal Units (RTUs) based on SIMATIC. [Consultado: 11 de marzo de 2019]. Disponible en: https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/telecontrol/rtu-remote-terminal-unit/rtu-simatic-s7-1200-1500-et-200sp.html

1.2.3.6 Periferia Distribuida. La periferia distribuida permite conectar a los diferentes dispositivos de control (PLC o DCS) módulos de entradas y salidas a través de un bus de comunicaciones o bus de campo. Mediante este sistema también es posible la conexión de dispositivos más complejos como variadores de frecuencia, instrumentación o actuadores. Muchos elementos de periferia distribuida están diseñados para soportar condiciones industriales difíciles. La periferia distribuida está basada en comunicación RS-485 o en Ethernet.

Figura 5. Periferia distribuida.

Fuente: PÉREZ ZENTENO, Francisco. Autracen [imagen]. ¿Qué es la periferia descentralizada?. [Consultado: 15 de marzo de 2019]. Disponible en: http://www.autracen.com/la-periferia-descentralizada/

1.2.3.7 HMI. Pantallas de operador (en inglés, Human Machine Interface), también conocidas como interfaces hombre máquina. Permiten a un usuario la monitorización de un proceso industrial. Normalmente se programan usando un software específico proporcionado por el fabricante.

Figura 6. Human Machine Interface (HMI).

Fuente: System Automation Service. sas-ics.com [imagen]. PLC-HMI-SCADA. [Consultado: 27 de marzo de 2019]. Disponible en: / https://sas-ics.com/services/plc-hmi-scada/

1.2.3.8 IED. Dispositivos de inteligencia electrónica (IED), son dispositivos que realizan una funcionalidad avanzada determinada, capaces tanto de adquirir, procesar y controlar datos del proceso industrial, así como de comunicarse con otros dispositivos, se usan para realizar controles a nivel local automáticamente.

Figura 7. Intelligence Electronic Device (IED).

Fuente: GÜZEL, Hüseyin. Huseyinguzel.net [imagen]. Applications for SIPROTEC Protection Relays. [Consultado: 3 de abril de 2019]. Disponible en: https://www.huseyinguzel.net/post/2017/08/29/applications-for-siprotec-protection-relays-by-siemens?wix-vod-comp-id=comp-j1faqxgt

1.2.4 Protocolos

Para los sistemas de control industrial la transmisión y recepción de información son la parte más importante del proceso de control, para ello, se hace uso de protocolos de comunicaciones, algunos son propietarios y están diseñados para un fin específico, otros han sido diseñados para hacer uso de tecnologías de medios de transmisión más modernas y para garantizar la interoperabilidad entre los diferentes fabricantes de dispositivos de control. A continuación, se detallan los protocolos de comunicaciones más comúnmente usados en los sistemas SCADA:

1.2.4.1 MODBUS. Es un protocolo de comunicaciones desarrollado por Modicon en 1979 y que se sitúa en la capa de aplicación del modelo de referencia OSI. Inicialmente fue diseñado para interactuar con PLCs utilizando comunicaciones en serie. Su estructura lógica trabaja en modo cliente/servidor, en la cual, el acceso al medio es controlado por el maestro (servidor), el intercambio de mensajes puede darse de dos formas, una es punto a punto, el servidor se comunica con el cliente correspondiente directamente, la otra es a través de mensajes de difusión a todos los clientes de la red.

En la actualidad, existen dos tipos de implementaciones del protocolo, MODBUS SERIE, que utiliza comunicación serial y protocolos como HDLC, RS232, y RS485 para la transmisión de datos y MODBUS TCP/IP que hace uso de la pila de protocolos TCP/IP para transmitir la información.

MODBUS no implementa ninguna característica de seguridad ni en la capa de transporte ni en la capa de aplicación, sin embargo, es posible aplicar medidas de seguridad basadas en TCP/IP únicamente a las implementaciones que hacen uso de MODBUS TCP/IP.

1.2.4.2 PROFIBUS. Acrónimo de Process Field Bus, es un protocolo de comunicaciones desarrollado en 1989 por el departamento alemán de educación e investigación y usado por Siemens, se basa en comunicaciones seriales con soporte sobre cable usando RS485 o sobre fibra óptica. En la actualidad existen dos implementaciones del protocolo, PROFIBUS DP y PROFIBUS PA, la primera se utiliza para la operación de periferia distribuida (sensores y/o actuadores) a través de un controlador centralizado, la segunda se utiliza para la monitorización de equipos de medición a través de un sistema de control del proceso.

PROFIBUS utiliza el método de transmisión asíncrona orientada al carácter. Las estaciones principales envían o piden datos a otras estaciones del bus cuando tienen el permiso correspondiente, por otra parte, las estaciones subordinadas solo intercambian datos con otras estaciones cuando alguna estación principal se lo solicita a través de la dirección única en la red que posee cada estación, la cual lo identifica y da permiso al intercambio de información entre estaciones específicas.

PROFIBUS no añade ninguna característica de seguridad en las comunicaciones, por lo que se considera un protocolo inseguro.

1.2.4.3 PROFINET. Es un protocolo de comunicaciones industriales basado en PROFIBUS que usa Ethernet para la transmisión de datos en los buses de campo. Puede hacer uso completo de la pila de protocolos TCP/IP por lo que puede hacer uso de diferentes medios de transmisión, como cableado, fibra e inalámbricos, por lo que soporta altas velocidades de transferencia.

PROFINET carece de medidas de seguridad, como autenticación y cifrado, pero su seguridad puede ser reforzada usando métodos de segmentación de redes, cifrado de tráfico e IDS.

1.2.4.4 POWERLINK ETHERNET. Es un sistema de comunicaciones para Ethernet en tiempo real. Transmite información con sincronización precisa a intervalos de tiempo predecibles, evitando colisiones mediante un procedimiento de software superpuesto conocido como Slot Communication Network Management (SCNM), que gestiona la red dedicando intervalos de tiempo a las transmisiones síncronas y asíncronas mientras asegura que sólo los equipos de la red acceden al medio de transmisión. La forma de operación del protocolo es Esclavo/Maestro, donde un dispositivo maestro llamado nodo gestor (NM) controla todo el tráfico en la red y los dispositivos esclavos llamados nodos controlados (CN) sólo pueden transmitir en los intervalos asignados para cada uno en el NM, además el NM es el único dispositivo que puede enviar mensajes de forma independiente, los CN envían mensajes sólo cuando el NM se los pide y lo hacen en forma de broadcast.

Es un protocolo que carente de mecanismos de autenticación para sus nodos y el uso de mensajes de difusión en las comunicaciones lo hace vulnerable a escuchas en la red, por lo cual se considera un protocolo inseguro.

POWERLINK ETHERNET debe aislarse de otras redes basadas en Ethernet, puesto que esos dispositivos pueden alterar el funcionamiento del protocolo y el comportamiento del bus de campo, ya que los dispositivos estándar no tienen interoperabilidad con el protocolo.

1.2.4.5 ETHERCAT. Conocido también como Ethernet for Control Automation Technology es un protocolo de código abierto estandarizado en el IEC 61158 totalmente compatible con Ethernet y utilizado en entornos industriales. Su comunicación es completamente en el hardware y tiene un rendimiento máximo, este es un protocolo altamente eficiente, puede implementarse cualquier tecnología, es una mezcla de datos a tiempo real con TCP/IP estándar.

La comunicación entre componentes estándar y equipos EtherCAT nunca se realiza de forma directa, sino siempre a través del llamado "Switch Virtual" en el PLC. Para el análisis de la red se necesitan equipos de análisis especiales, ya que el flujo de datos depende del punto de medición.

Al ser un protocolo basado en Ethernet le afectan todas las vulnerabilidades del estándar, no cuenta con métodos de autenticación para los nodos, por lo que es recomendable separar la red del sistema de control de la red corporativa.

1.2.4.6 DNP3. Acrónimo de Distributed Network Protocol, es un protocolo de comunicaciones industriales abierto desarrollado en 1993 y utilizado principalmente por industrias del sector energético, hidráulico, telemetría, monitoreo en tiempo real, entre otros sistemas SCADA. DNP3 actúa en las capas de aplicación, enlace de datos y transporte. En la actualidad se está promoviendo una implementación segura del protocolo, conocida como DNP3 seguro, la cual incluye métodos de autenticación.

Actualmente el desarrollo de DNP3 está a cargo del grupo de usuarios DNP3, el cual está constituido por empresas de servicios públicos y proveedores que utilizan el protocolo.

1.2.4.7 OPC UA. Es un protocolo de comunicaciones abierto desarrollado por la OPC Foundation y lanzado en 2006 que se utiliza para la comunicación con equipos y sistemas industriales con el fin de recolectar y controlar datos, es multiplataforma y está basado en una arquitectura orientada a servicios SOA. Su seguridad es robusta, incluye autenticación a nivel de aplicación, cifrado y autenticación de mensajes. Usa los puertos TCP 80 y 443 lo que hace que la configuración de los firewalls sea más sencilla.

1.2.5 Definición de seguridad en los sistemas de control industrial

En lo referente a la seguridad, en los sistemas de control industrial se usan dos conceptos, *safety* y *security.*

Safety en los sistemas de control industrial se asocia con la prevención de los daños a nivel de equipamiento, instalaciones, personas o la misma comunidad, que pudieran impactar en la operación, automatización, control y supervisión del proceso industrial.

Security, está relacionado con la prevención de eventos malintencionados, potencialmente dañinos, como sabotajes, robos, ciberataques, tanto en el ámbito de la seguridad lógica, donde se pueden utilizar elementos como Firewalls, IDS/IPS, Antivirus, entre otros; como en el ámbito de la seguridad física, donde se utilizan controles de acceso, dispositivos biométricos, sensores de movimiento, cámaras de vigilancia, etc.

1.2.6 Vulnerabilidades comunes y factores de riesgo

Las vulnerabilidades comunes representan los problemas más encontrados en los sistemas de control industrial, mientras que los factores de riesgo potencian la probabilidad de que dichas vulnerabilidades sean explotadas.

De la relación entre las vulnerabilidades y los factores de riesgo pueden surgir los posibles ataques a los sistemas de control industrial.

Algunas vulnerabilidades comunes que se pueden encontrar son:

- Perímetro de red indefinido.
- Seguridad por oscuridad.
- Puertos físicos accesibles.
- Configuraciones por defecto.
- Aplicaciones y servicios innecesarios.
- Protocolos de comunicación vulnerables.
- Vulnerabilidades Zero-Day.
- Deficiente instalación de parches de seguridad.
- Controles de acceso inadecuados o inexistentes.
- Falta de gestión de logs.

Algunos factores de riesgo que pueden potenciar las vulnerabilidades son:

- Interconexión de los sistemas de control industrial con sistemas TI tradicionales.
- Acceso a datos del proceso desde cualquier ubicación.
- Sistemas de control industrial conectados a internet.
- Profesionales de seguridad que no son involucrados en el diseño y mantenimiento del sistema.
- Falta de procesos y herramientas de seguridad.
- Uso de tecnologías de TI de propósito general, como TCP/IP.
- Inexistencia de un marco regulador o política de seguridad.

1.2.7 Protección de los sistemas de control industrial

Los sistemas de control industrial aprovechan las herramientas, procesos y tecnologías de seguridad existentes en el ámbito de las tecnologías de información para implementar medidas de protección que, aunque no pueden ser aplicadas directamente sobre el entorno por sus características intrínsecas si pueden adaptarse para prevenir la materialización de amenazas. Algunas soluciones de seguridad que se pueden utilizar para asegurar los sistemas de control industrial son:

- Firewalls.
- IDS/IPS.

- VPNs host to host y site to site.
- Evaluaciones técnicas de seguridad.

1.3 MARCO CONCEPTUAL (GLOSARIO DE TÉRMINOS)

Activo: Es un elemento, función o recurso de un sistema de información que puede ser atacado deliberada o accidentalmente trayendo consecuencias para la organización.

Amenaza: Evento que puede desencadenar un incidente en un sistema, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Acción que vulnera o intenta asaltar la seguridad de un sistema o red informática.

DCS: Distributed Control System. Sistema de control distribuido.

EMS: Energy Management System. Sistema de gestión de energía.

Exploit: Es una forma específica de aprovechar una vulnerabilidad para lograr un ataque informático.

Impacto: Es la medida del daño sobre un activo que se produce como consecuencia de la materialización de una amenaza

Riesgo: Es la medida del daño posible sobre un sistema, puede ser cuantitativo o cualitativo.

RTU: Remote Terminal Unit. Unidad terminal remota.

SCADA: Supervisory Control And Data Acquisition. Control por supervisión y adquisición de datos.

Seguridad informática: Estado de bienestar aceptable en lo que respecta al riesgo al que están expuestos los activos de un sistema o una red informática.

Vulnerabilidad: Existencia de una debilidad en el diseño de una aplicación o un error que puede conducir a un acontecimiento inesperado y no deseable, el cual pone en peligro la seguridad del sistema.

1.4 MARCO CONTEXTUAL

El marco contextual de este proyecto está comprendido por todos los sistemas de control industrial y/o SCADA situados en el territorio nacional de Colombia.

1.5 MARCO LEGAL

Dentro del marco legal que rige sobre este trabajo de grado se encuentran:

- El acuerdo 0029 del 13 de diciembre de 2013. Por el cual se expide el reglamento estudiantil de la Universidad Nacional Abierta y a Distancia (UNAD), especialmente el artículo 65, parágrafo 2 y 3, y el artículo 68.

- La Ley 1273 de 2009, que regula la protección de la información y de los datos, así como, preserva integralmente los sistemas que utilizan las tecnologías de la información y las comunicaciones a través de los siguientes artículos:

    - Artículo 269A: Acceso abusivo a un sistema informático.
    - Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
    - Artículo 269C: Interceptación de datos informáticos.

  - Artículo 269D: Daño Informático.
  - Artículo 269E: Uso de software malicioso.
  - Artículo 269F: Violación de datos personales.
  - Artículo 269G: Suplantación de sitios web para capturar datos personales.
  - Artículo 269H: Circunstancias de agravación punitiva.
  - Artículo 269I: Hurto por medios informáticos y semejantes.
  - Artículo 269J: Transferencia no consentida de activos.

- La Ley 1581 de 2012, la cual dicta disposiciones para la protección de los datos personales.

- El documento CONPES 3854, que define los lineamientos para fortalecer las capacidades de los múltiples interesados en identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

2. ESTADO DEL ARTE

Para la realización de la monografía titulada diseño de una metodología para la evaluación de la ciberseguridad de los sistemas de control industrial (SCADA).se investigaron diferentes fuentes documentales de diferentes tipos de organizaciones de índole público y privado dedicadas a la seguridad informática y el control industrial. Se analizaron las metodologías encontradas identificando los pasos para evidenciar amenazas, vulnerabilidades y controles comunes a los sistemas de control industrial, luego, se procedió a documentar información relevante referente a sistemas de control industrial, sus amenazas, vulnerabilidades y controles y establecer unos pasos metodológicos a seguir para evaluar un sistema de control industrial, finalmente se resumen estos pasos en un gráfico que representa la metodología propuesta.

En la etapa de análisis documental se investigan fuentes bibliográficas, libros, revistas especializadas, noticias, blogs de opinión, e información en internet referente a los sistemas de control industrial SCADA y su seguridad. Con lo anterior, se pretende identificar aspectos básicos relacionados a los sistemas de control industrial y su seguridad, identificar técnicas para la recolección de información referente a activos de seguridad en los sistemas de control industrial, listar amenazas y vulnerabilidades comunes a estos sistemas, y las técnicas para encontrarlas y documentarlas apropiadamente. También se analizarán los diferentes tipos de controles que apliquen a los sistemas de control industrial con el fin de realizar un listado que permita determinar junto con todo lo anterior el estado de la seguridad del sistema.

3. ACTUALIDAD DE SISTEMAS DE CONTROL INDUSTRIAL Y METODOLOGÍAS DE EVALUACIÓN

Asegurar los sistemas de control industrial es una prioridad para garantizar la disponibilidad, confiabilidad, integridad, estabilidad y buen funcionamiento de los procesos industriales, teniendo en cuenta los riesgos para el medio ambiente, la salud y la vida de las personas involucradas en la producción, entrega y consumo del producto o servicio asociado al sistema (ICS); así como para evitar pérdidas financieras a las compañías o impactos negativos en la economía de una nación.

Debido al alto riesgo que representa el funcionamiento de un sistema de control industrial débil o comprometido, los gobiernos han empezado a crear organizaciones, marcos regulatorios, políticas y metodologías para proteger sus infraestructuras industriales de amenazas y ataques que puedan afectar la ciberseguridad, puesto que en muchos casos estas infraestructuras son consideradas como críticas por su aporte a la economía y la seguridad nacional.

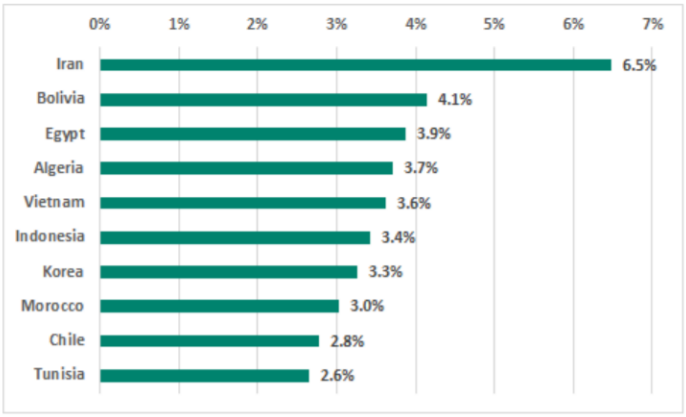
Organismos como el NIST y NERC en Estados Unidos, la ANSSI en Francia, e INCIBE en España, se encargan de normalizar y expedir guías de buenas prácticas de seguridad para los sistemas de control industrial, algunos incluso tienen a su cargo grupos especializados, conocidos como equipos de respuesta ante emergencias informáticas (CERT, Computer Emergency Response Team) para dar respuesta a los diferentes ataques y amenazas a la seguridad de los sistemas de control industrial. Estas acciones gubernamentales en Norte América y Europa han permitido que haya mayor conciencia por parte de los profesionales, proveedores y las compañías propietarias de sistemas de control industrial para asumir la seguridad de estos con mayor seriedad.

3.1 ACTUALIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Desde el año 2017, dos veces al año, Kaspersky Lab ICS CERT publica un reporte en el que se analizan los ataques a los sistemas de control industrial a los equipos que tienen instalados sus productos alrededor del mundo, el reporte es un informe sobre el panorama de las amenazas a los sistemas de control industrial. Según el informe, para el año 2019, el ransomware sigue siendo el ataque que mayor afectación produce a los sistemas de control; los países en los cuales se detectaron

más ataques a su infraestructura fueron, en primer lugar, Irán, seguido de Bolivia y Egipto en el tercer lugar (Figura 8)

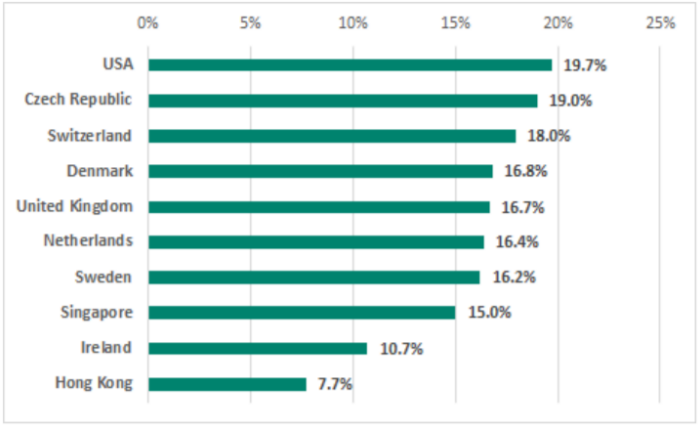
Figura 8. Países con mayores ataques de ransomware a sus ICS.



Fuente: KASPERSKY LAB. Kaspersky.com. Threat landscape for industrial automation systems. [Consultado el 4 de diciembre de 2019]. Disponible en: https://ics-cert.kaspersky.com/media/H1_2019_kaspersky_ICS_REPORT_EN.pdf

Así mismo, de acuerdo con el reporte, los países o territorios con menos ataques de seguridad a sus sistemas de control fueron, Hong Kong, Irlanda y Singapur (figura 9).

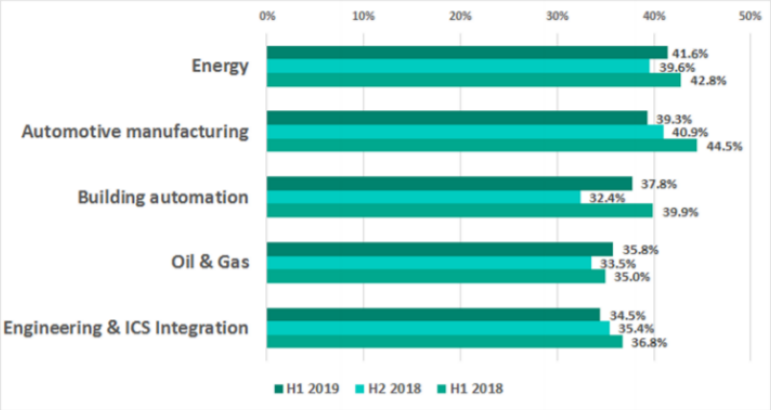
Figura 9. Países con menos ataques a sus ICS.



Fuente: Ibíd., p. 20.

Según el reporte de Kaspersky las industrias con mayores ataques a sus sistemas de control industrial fueron las relacionadas con energía, fabricación de automóviles, automatización de edificios, petróleo y gas, entre otras (figura 10)

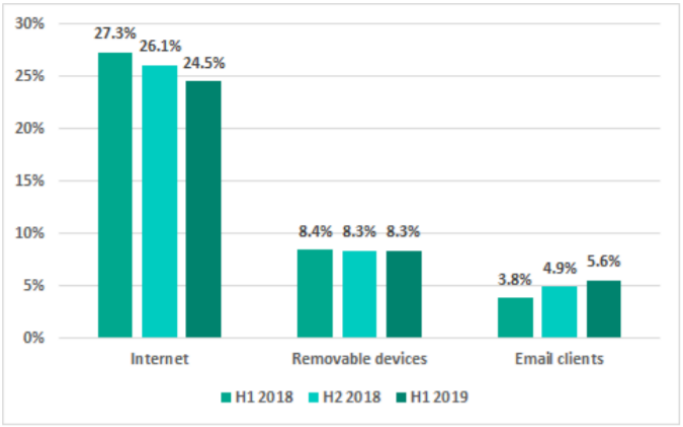
Figura 10. Empresas víctimas de ataques a sus sistemas de control industrial.



Fuente: Ibíd., p. 15.

Finalmente, Kaspersky reporta en su informe que las tres principales fuentes de amenaza a los sistemas de control industrial siguen siendo en primer lugar, Internet, en segundo lugar, los dispositivos removibles, y en tercer lugar los correos electrónicos.

Figura 11. Porcentaje de ataques desde diferentes fuentes de amenaza.

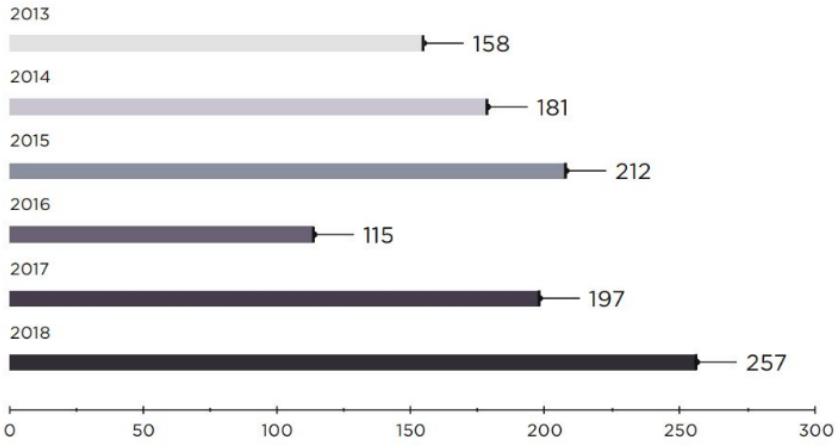


Fuente: Ibíd., p. 25.

En cuanto al estudio de las vulnerabilidades en los sistemas de control industrial, los datos pueden no ser muy alentadores debido a que estas han aumentado, lo que puede significar que los profesionales de seguridad del sector han desarrollado más habilidades para evaluar las vulnerabilidades y esto da como resultado que cada día más vulnerabilidades sean evidenciadas, o que los sistemas de control han heredado un gran número de vulnerabilidades de los sistemas TI debido a la convergencia de los dos sistemas, o que los fabricantes están haciendo caso omiso a las medidas de seguridad que se aconsejan por parte de las organizaciones reguladoras, en la actualidad no hay un estudio que entregue claridad frente al tema.

Según Positive Technologies las vulnerabilidades en los productos de los principales proveedores de equipos de automatización y control industrial vienen en aumento (Figura 12) encontrando en 2018 alrededor de 257 vulnerabilidades, 60 más comparadas con el año 2017 y 99 más que en 2013 cuando iniciaron la medición.

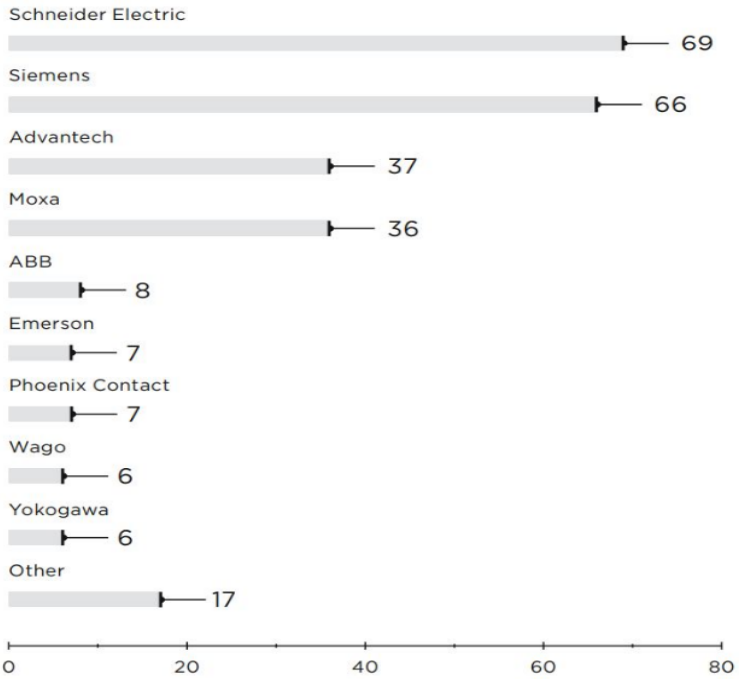
Figura 12. Vulnerabilidades encontradas en ICS desde 2013 hasta 2018.



Fuente: POSITIVE TECHNOLOGIES. Ptsecurity.com [imagen]. ICS vulnerabilities: 2018 in review. [Consultado: 7 de mayo de 2019]. Disponible en: https://www.ptsecurity.com/ww-en/analytics/ics-vulnerabilities-2019/

En el estudio se evidenció que los proveedores que presentan mayor número de vulnerabilidades en sus productos fueron Schneider Electric y Siemens, esto se explica teniendo en cuenta que estos proveedores tienen un amplio portafolio de productos que abarca gran parte de los sistemas de control industrial del mundo.

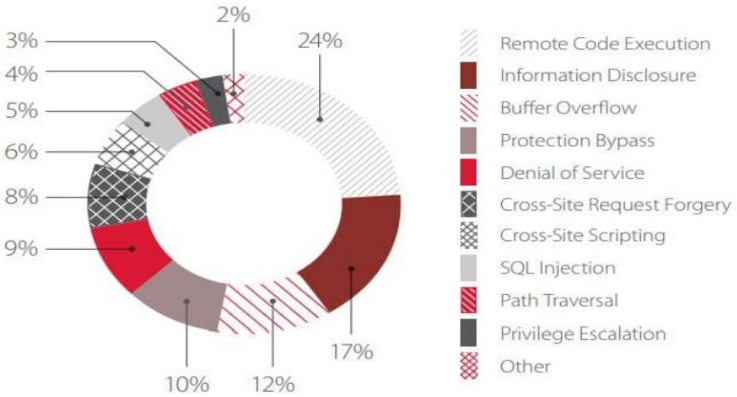
Figura 13. Vulnerabilidades por proveedor de equipos.



Fuente: Ibíd., p. 4.

En 2017 las vulnerabilidades que más se presentaron fueron las relacionadas con ejecución remota de código, divulgación de información y desbordamiento de búfer.

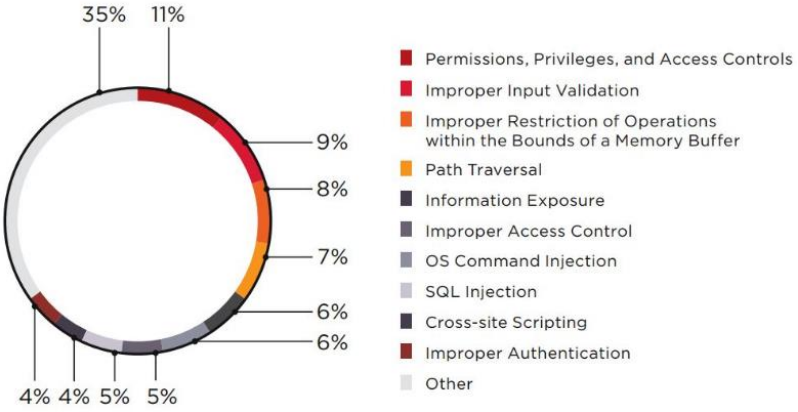
Figura 14. Tipos de vulnerabilidades en ICS en 2017.



Fuente: POSITIVE TECHNOLOGIES. Ptsecurity.com. ICS Security: 2017 in review. [Consultado: 13 de enero 2019]. Disponible en: https://www.ptsecurity.com/ww-en/analytics/ics-security-2017/

En 2018 las vulnerabilidades más encontradas estuvieron relacionadas con permisos, privilegios y controles de acceso; entradas inválidas y operaciones con el búfer de memoria.

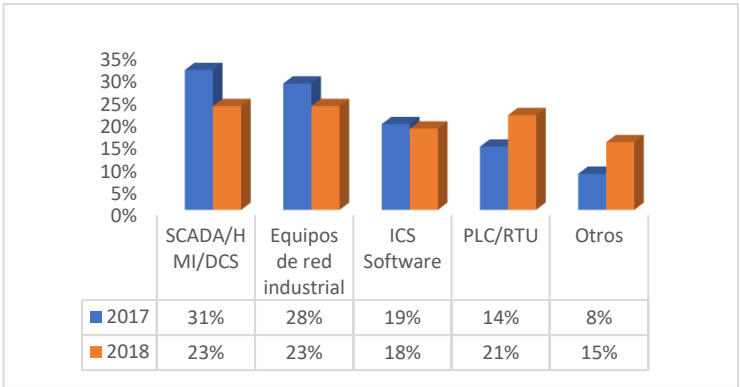
Figura 15. Tipos de vulnerabilidades en ICS en 2018.



Fuente: KASPERSKY, Op. cit., p. 5.

Se evidenció que en 2018 las principales vulnerabilidades siguen encontrándose en los equipos de redes, los SCADA/HMI/DCS, y en el software de ICS, pero que estas han disminuido con respecto al año 2017. También se observó un aumento considerable en las vulnerabilidades en dispositivos PLC y RTU y en otros equipos, lo cual puede indicar que no se están haciendo esfuerzos por proteger estos dispositivos que por lo general se instalan en ubicaciones remotas.

Figura 16. Vulnerabilidades en componentes ICS en 2017 y 2018.

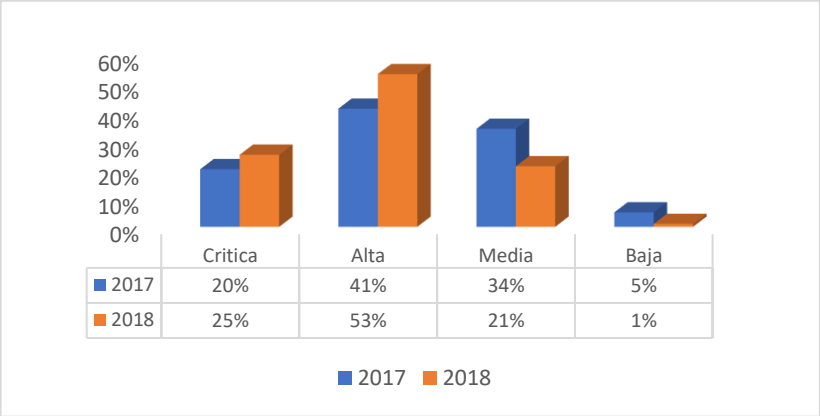


	SCADA/HMI/DCS	Equipos de red industrial	ICS Software	PLC/RTU	Otros
2017	31%	28%	19%	14%	8%
2018	23%	23%	18%	21%	15%

La severidad de las vulnerabilidades encontradas fue evaluada de acuerdo con el sistema de puntuación de vulnerabilidad común CVSS versión 3, encontrando en el 2017 un 20% de vulnerabilidades críticas y un 41% de vulnerabilidades altas, un 34% de vulnerabilidades de nivel medio y 5% de vulnerabilidades de nivel bajo. En 2018 las vulnerabilidades críticas aumentaron llegando a ser de 25% y las altas pasaron a ser el 53%, las de nivel medio bajaron un 13% y las vulnerabilidades de nivel bajo son sólo del 1%.

Teniendo en cuenta los datos se puede inferir que las vulnerabilidades en 2018 comparadas con el año anterior disminuyeron en algunos dispositivos importantes como los SCADA y equipos de red, pero aumentaron su criticidad.

Figura 17. Criticidad de las vulnerabilidades en ICS en 2017 y 2018.



Este estudio que Positive Technologies realiza anualmente sirve de alerta para pensar que es indispensable proteger los sistemas de control industrial que se encuentran en las fábricas y en las infraestructuras críticas y en este proyecto se pretende aportar un grano de arena a ese objetivo, porque a pesar de que el gobierno colombiano ha dado avances en la protección de su infraestructura y ha creado algunas herramientas como el CONPES 3854 y los CERT como colCERT estás no son suficientes para enfrentar las diferentes amenazas a la seguridad informática que enfrentan los sistemas de control hoy en día y se requiere de marcos de trabajo que permitan a las organizaciones públicas y privadas, a las instituciones y los profesionales determinar el estado de la seguridad de la información de su sistema y que tan vulnerable es éste a los ataques que se pueden encontrar.

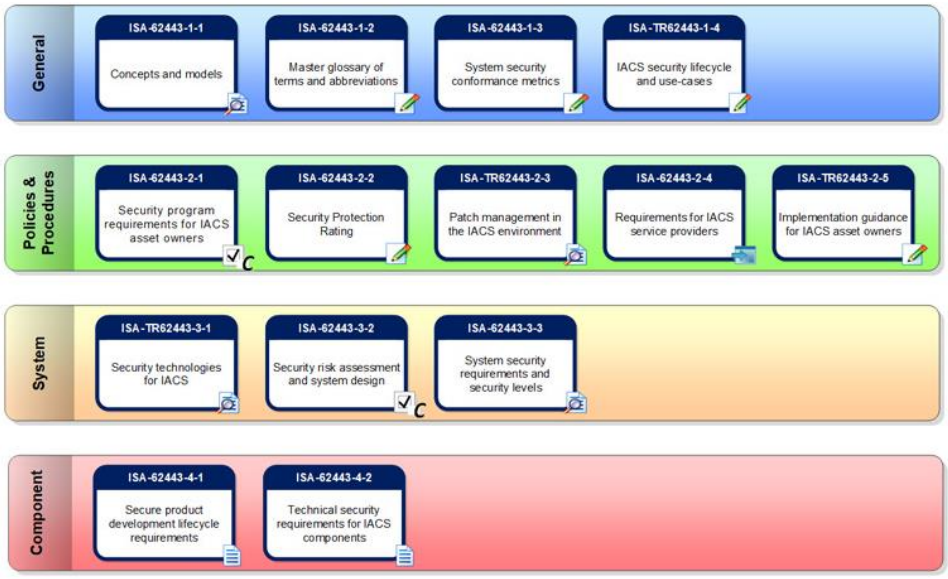
3.2 ACTUALIDAD DE LAS METODOLOGÍAS DE EVALUACIÓN

En la actualidad, aunque existen diferentes marcos de trabajo, documentos y guías de buenas prácticas para asegurar los sistemas de control industrial, se puede decir que no existe una metodología general para la evaluación de seguridad de los ICS, a diferencia de las tecnologías de la información que cuentan con diferentes metodologías de evaluación. A continuación, se esbozan algunos marcos de trabajo y metodologías que soportan los sistemas de control industrial.

3.2.1 IEC 62443.

La norma IEC 62443 tiene como base la norma ISA99 y es un conjunto de 13 documentos y guías en los que se establecen una serie de recomendaciones y mejores prácticas con el fin de mejorar la seguridad de los sistemas de control industrial frente a las diferentes amenazas a las que estos se enfrentan. Estos documentos se clasifican en 4 grupos: general, políticas y procedimientos, sistema y componentes, estos documentos a su vez se dividen en 5 informes técnicos, 1 informe de especificaciones técnicas y 7 de guías.

Figura 18. Documentos de la serie IEC 62443



Fuente: ISA. isa.org. ISA99, Industrial Automation and Control Systems Security. [Consultado: 18 de diciembre 2019]. Disponible en: https://www.isa.org/isa99/

De los 13 documentos que conforman la serie IEC 62443 seis se encuentran publicados, tres de ellos bajo revisión; cinco están en desarrollo y dos han sido aprobados con comentarios.

La norma IEC 62443 no es en sí misma una metodología de evaluación de seguridad

de sistemas de control industrial, es más bien un marco de trabajo que brinda guías y recomendaciones para la implementación segura de sistemas de control industrial y evaluar el desempeño durante esta tarea.

3.2.2 NERC CIP 002-009

La norma NERC-CIP 002-009 de la Corporación Norteamericana de Confiabilidad Eléctrica (NERC, del inglés North American Electrical Reability Corporation) está compuesta por una serie de documentos y guías en los que se realizan recomendaciones y se establecen controles de obligatorio cumplimiento para la valoración de la seguridad de los activos más importantes en la operación del sistema eléctrico. En la serie se definen los requisitos de confiabilidad para planificar y operar un sistema de generación de energía eléctrica usando un enfoque basado en resultados y enfocado en el rendimiento y la gestión adecuada del riesgo.

La serie de documentos de la norma NERC-CIP 002-009 no constituye como tal una metodología para la evaluación de sistemas de control industrial, sino más bien es un estándar para la implementación y operación segura de un sistema de generación de energía eléctrica, teniendo por objeto garantizar la ciberseguridad del sistema, identificando, reconociendo los diferentes roles de la operación, la criticidad y vulnerabilidad de los activos necesarios en la administración de la confiabilidad de la red y los riesgos a los que estos se enfrentan.

3.2.3 NIST SP800-82

El National Institute of Standars and Technology del departamento de comercio de los Estados Unidos publicó en mayo de 2015 la segunda versión de este documento, en el cual se establecen una serie de pautas para asegurar los sistemas de control industrial. En el documento se revisan topologías y arquitecturas de red

típicas de los sistemas de control, se identifican amenazas y vulnerabilidades conocidas de los ICS, y se proporcionan contramedidas para mitigar los riesgos asociados a los ICS.

A pesar de ser un documento bastante completo en cuanto a la seguridad de los sistemas de control industrial, no constituye una metodología para la evaluación de seguridad de los ICS, es más bien un soporte documental para las evaluaciones de seguridad de los ICS aportando pautas para cumplir con los requisitos de seguridad de los ICS.

3.2.5 NESCOR

A diferencia de las anteriores, NESCOR es una guía de pruebas de penetración con enfoque en el sector eléctrico y las SmartGrid de la National Electric Sector Cybersecurity Organization Resource. El documento proporciona una guía para la realización de pruebas de penetración en los sistemas SmartGrid.

NESCOR aborda la prueba de penetración con una revisión de la arquitectura del sistema de control industrial, luego procede a clasificar el sistema objetivo en cuatro grupos y realizar test de penetración a cada grupo, estos grupos son: sistemas operativos de servidor, aplicaciones de servidor, comunicaciones de red y dispositivos embebidos, con los resultados de las pruebas se realiza un análisis de extremo a extremo con el fin de encontrar brechas de seguridad que pudieron ser pasadas por alto. Finalmente, se procede a la interpretación de resultados, reporte y recomendaciones.

4. PROBLEMAS DE SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL

Los sistemas de control industrial son sistemas complejos que dependen de muchos componentes y tecnologías diferentes para monitorear y controlar procesos físicos, como la generación de energía, la explotación petrolera, o la fabricación de materias primas, diferenciándose de los sistemas de tecnologías de la información (TI) tradicionales cuyo objetivo principal es el control y administración de datos, además de esto también se diferencian en las prioridades de seguridad y los riesgos que enfrentan, algunos de estos riesgos son significativos para la salud, las vidas humanas, y pueden generar daños graves al medio ambiente, así como pérdidas de producción e impactos negativos a la economía de una nación.

En la actualidad, los sistemas de control industrial modernos están integrados en la operación de las compañías e interactúan con las tecnologías de la información compartiendo comunicaciones e intercambiando datos, esto se debe principalmente al bajo costo de los dispositivos IP y la creciente adopción de las soluciones de TI para la conectividad corporativa. Esta convergencia de las tecnologías de la información (TI) con las tecnologías operativas (TO) de los sistemas de control industrial plantea nuevos desafíos de seguridad para las compañías, los gobiernos y los profesionales del sector, ya que compartir una arquitectura de red extiende el dominio del ICS y abre la puerta a nuevas amenazas y vulnerabilidades que antes no afectaban el sistema debido a su aislamiento.

Las estrategias de seguridad en los dominios de TI tienden a centrarse en la protección de los datos manteniendo su confidencialidad, integridad y disponibilidad. En los sistemas de control industrial la seguridad no se centra en los datos, sino en la continuidad de los procesos industriales, es por ello que la disponibilidad es un objetivo principal de la estrategia de seguridad

4.1 FUENTES DE AMENAZA

Las fuentes de amenaza son aquellas que involuntariamente o deliberadamente son el origen de las amenazas a los sistemas de control industrial. Se considera a las personas como la principal fuente de amenaza de los ICS, seguidas de los desastres industriales y los desastres naturales.

Algunas fuentes de amenaza conocidas son:

- Ingenieros de control de procesos.
- Operadores.
- Proveedores.
- Personal de apoyo logístico.
- Antiguos empleados descontentos.
- Clientes
- Usuarios.
- Competencia desleal.
- Atacantes internos
- Hackers.
- Hacktivistas.
- Organizaciones criminales.
- Organizaciones de inteligencia extranjeras de naciones enemigas.
- Actores estatales corruptos.
- Terroristas.
- Desastres industriales.
- Desastres naturales.

4.2 AMENAZAS

Una amenaza de un sistema de control industrial es un evento o causa con el potencial de provocar un incidente no deseado en uno o más equipos, dispositivos o servicios de un ICS, y puede llegar a causar daños a las personas, al sistema, a una organización, a la infraestructura crítica, a los servicios sociales vitales, al medio ambiente o a la sociedad en general.

Las amenazas en los sistemas de control industrial se clasifican según su origen en:

- Intencionales.
- Accidentales.
- Estructurales.
- Ambientales.

4.2.1 Amenazas intencionales.

Son eventos que se relacionan con individuos, grupos, organizaciones, incluso estados que buscan explotar los sistemas de control industrial con el objetivo de afectar negativamente a la organización propietaria del sistema de control industrial.

Tabla 1. Amenazas intencionales.

AMENAZAS INTENCIONALES	
ORIGEN	AMENAZA
Individuo, atacante externo, atacante interno, grupo de atacantes, organización, competidor, proveedor, cliente, nación.	Suplantación de la identidad del usuario
	Acceso no autorizado
	Abuso de privilegios
	Manipulación de la configuración
	Manipulación de los registros
	Difusión de malware
	Redireccionamiento de tráfico
	Alteración de datos
	Interceptación de información
	Repudio
	Modificación de la información
	Destrucción de la información
	Divulgación de la información
	Manipulación del software
	Manipulación del hardware
	Denegación de servicio
	Robo
	Ataque con ransomware
	Ingeniería social

4.2.2 Amenazas accidentales.

Son eventos que se refieren a acciones incorrectas o errores cometidos en la ejecución de sus responsabilidades cotidianas por individuos involucrados en la operación del sistema de control industrial.

Tabla 2. Amenazas accidentales.

AMENAZAS ACCIDENTALES	
ORIGEN	AMENAZA
usuario, usuario con privilegios de administrador	Error de uso
	Errores del administrador
	Errores de monitorización
	Errores de configuración
	Errores en la asignación de responsabilidades
	Difusión de malware accidental
	Errores en el envío de información
	Errores de secuencia
	Escape de información
	Alteración accidental de la información
	Destrucción accidental de la información
	Fuga de información accidental
	Errores en el mantenimiento de hardware
	Errores en la actualización de software
	Pérdida de equipos
	Ausencia de personal

4.2.3 Amenazas estructurales.

Son eventos relacionados con fallos de equipos, ambientes controlados, software degradado, agotamiento de recursos u otros eventos que alteran los parámetros de operación esperados.

Tabla 3. Amenazas estructurales.

AMENAZAS ESTRUCTURALES	
ORIGEN	AMENAZA
Sistema de control industrial, periferia distribuida, RTU, sensores, actuadores, monitores, HDI, controladores, fuentes de alimentación, software, sistemas operativos, redes, hardware.	Falla física
	Falla lógica
	Desastre industrial
	Incendio
	Inundación
	Contaminación
	Fallo de energía
	Condiciones inadecuadas de temperatura
	Falla en las comunicaciones

AMENAZAS ESTRUCTURALES	
ORIGEN	AMENAZA
	Degradación de los equipos
	Agotamiento de recursos por envejecimiento

4.2.4 Amenazas ambientales.

Son eventos de tipo natural que amenazan al sistema de control industrial y que están fuera del alcance de la organización propietaria del sistema.

Tabla 4. Amenazas ambientales.

AMENAZAS AMBIENTALES	
ORIGEN	AMENAZA
Natural, ambiental	Terremoto
	Fenómeno climático
	Contaminación
	Fenómeno de origen volcánico
	Inundación
	Incendio

4.3 VULNERABILIDADES

Una vulnerabilidad es una debilidad en uno o más equipos, sistemas, dispositivos, y/o servicios de un sistema de control industrial, que puede ser aprovechada por una amenaza para provocar un daño potencial en el ICS, llegando incluso a ocasionar pérdidas de vidas humanas, daños al medio ambiente, a servicios sociales vitales, a la infraestructura critica o a la economía de una nación.

Para fines de este documento las vulnerabilidades en los sistemas de control industrial se clasifican en:

- Vulnerabilidades en políticas y procedimientos.
- Vulnerabilidades en la arquitectura y el diseño del ICS.
- Vulnerabilidades de configuración y mantenimiento.
- Vulnerabilidades de índole físico.
- Vulnerabilidades en el software.

- Vulnerabilidades en las comunicaciones y configuraciones de red.

4.3.1 Vulnerabilidades en políticas y procedimientos.

La ausencia de políticas de seguridad o el uso de políticas con una documentación inadecuada y/o desactualizada, la poca preocupación por la capacitación y educación de los usuarios en el cuidado de la ciberseguridad de los ICS, la falta de guías de implementación de equipos, dispositivos y/o servicios del ICS como de mecanismos administrativos para la aplicación de la política de seguridad, la revisión inadecuada de la efectividad de los controles, la falta de un plan de contingencia y políticas de gestión de cambios de configuración, así como de políticas de control de acceso y autenticación, y la inadecuada detección de incidentes, la ausencia de procedimientos de respuesta a incidentes en los ICS y de redundancia para los componentes críticos del proceso son vulnerabilidades que corresponden a fallas en las políticas y los procedimientos.

Tabla 5. Vulnerabilidades en políticas y procedimientos.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Políticas y procedimientos	Política de seguridad inadecuada para el ICS
	No hay un programa formal de capacitación y concientización sobre seguridad de ICS
	Pautas de implementación de equipos ICS ausentes o deficientes
	Falta de mecanismos administrativos para la aplicación de la política de seguridad
	Revisión inadecuada de la efectividad de los controles de seguridad de ICS.
	No hay plan de contingencia específico de ICS
	Falta de política de administración de configuración
	Falta de una política adecuada de control de acceso
	Falta de una política de autenticación adecuada
	Inadecuada detección de incidentes y plan y procedimientos de respuesta a incidentes.
	Falta de redundancia para componentes críticos.

4.3.2 Vulnerabilidades en la arquitectura y el diseño del ICS.

La inadecuada incorporación de seguridad en el diseño y la arquitectura del ICS, la evolución insegura y descontrolada de la arquitectura, la indefinición del perímetro de seguridad, el uso indiscriminado de las redes de control, el uso de servicios que no están dentro del dominio del ICS y la recopilación inadecuada del historial de datos de eventos e incidentes de seguridad, son vulnerabilidades en la arquitectura y el diseño.

Tabla 6. Vulnerabilidades en la arquitectura y el diseño.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Arquitectura y Diseño	Incorporación inadecuada de seguridad en la arquitectura y el diseño.
	Evolución insegura de la arquitectura del ICS
	Sin perímetro de seguridad definido
	Redes de control utilizadas para tráfico diferente al del proceso
	Servicios de red de control que no están dentro de la red de control
	Recopilación inadecuada del historial de datos de eventos e incidentes

4.3.3 Vulnerabilidades de configuración y mantenimiento.

Las vulnerabilidades en la configuración y en el mantenimiento se refieren a debilidades de seguridad en las configuraciones del hardware, el software y los servicios que hacen parte del sistema de control industrial, así como en el control y monitoreo de las actividades de mantenimiento.

Tabla 7. Vulnerabilidades de configuración y mantenimiento.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Configuración y Mantenimiento	El hardware, el firmware y el software no están bajo la administración de configuración.
	El sistema operativo y los parches de software del proveedor pueden no desarrollarse hasta

TIPO DE VULNERABILIDAD	VULNERABILIDAD
	significativamente después de encontrar vulnerabilidades de seguridad
	El sistema operativo y los parches de seguridad de la aplicación no se mantienen o el proveedor declina reparar la vulnerabilidad
	Pruebas inadecuadas de los cambios de seguridad.
	Malos controles de acceso remoto
	Se utilizan configuraciones deficientes
	Las configuraciones críticas no se almacenan ni se respaldan
	Datos desprotegidos en dispositivo portátil
	Las contraseñas de generación, uso y protección no están de acuerdo con la política
	Se aplicaron controles de acceso inadecuados
	Enlace de datos incorrecto
	Protección contra malware no instalada o actualizada
	Protección contra malware implementada sin pruebas suficientes
	Denegación de servicio (DoS)
	Software de detección / prevención de intrusiones no instalado
	Registros no mantenidos

4.3.4 Vulnerabilidades de índole físico.

Son vulnerabilidades relacionadas con el entorno físico y ambiental donde se encuentra el sistema de control industrial. Se refieren por lo general a fallas de interferencia con las radiofrecuencias, existencia de pulsos electromagnéticos irregulares, falta de sistemas de respaldo, falta de controles ambientales, fallos en puertos físicos, falta de mecanismos de seguridad física y de monitorización y control de ingreso a terceros.

Tabla 8. Vulnerabilidades físicas.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Vulnerabilidades físicas	Radiofrecuencia, pulso electromagnético (EMP), descarga estática, caídas de voltaje y picos de voltaje
	Falta de energía de respaldo

TIPO DE VULNERABILIDAD	VULNERABILIDAD
	Pérdida de control ambiental (temperatura, humedad)
	Puertos físicos sin garantía
	Falta de mecanismos de seguridad física en los sistemas de control industrial
	Falta de monitorización de las actividades de los terceros

4.3.5 Vulnerabilidades en el software.

Las vulnerabilidades en el software se refieren a debilidades de ciberseguridad en el software de ICS que tienen que ver con la validación incorrecta de los datos, falta de mecanismos de seguridad, cifrado y autenticación, así como ausencia de actualizaciones y parches de seguridad.

Tabla 9. Vulnerabilidades en el software.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Vulnerabilidades en el software	Validación de datos incorrecta
	Capacidades de seguridad instaladas no habilitadas por defecto
	Autenticación inadecuada, privilegios y control de acceso en software
	Falta de mecanismos de cifrado
	Falta de mecanismos de autenticación
	Software sin actualización ni parches de seguridad

4.3.6 Vulnerabilidades en las comunicaciones y configuraciones de red.

Las vulnerabilidades en las comunicaciones y configuraciones de red se refieren a debilidades de ciberseguridad en las redes de telecomunicaciones que comunican los equipos, dispositivos y servicios de los sistemas de control industrial.

Tabla 10. Vulnerabilidades en las comunicaciones y configuraciones de red.

TIPO DE VULNERABILIDAD	VULNERABILIDAD
Vulnerabilidades en las comunicaciones y configuraciones de red	Controles de flujo de datos no empleados
	Cortafuegos inexistentes o mal configurados
	Cortafuegos y registros de enrutamiento inadecuados
	Los protocolos de comunicación estándar y bien documentados se utilizan en texto sin formato.
	La autenticación de usuarios, datos o dispositivos es deficiente o inexistente
	Uso de protocolos ICS no seguros en toda la industria
	Falta de verificación de integridad para comunicaciones
	Autenticación inadecuada entre clientes inalámbricos y puntos de acceso
	Protección de datos inadecuada entre clientes inalámbricos y puntos de acceso

5. PASOS METODOLÓGICOS DE LA EVALUACIÓN DE SEGURIDAD

En este capítulo se realiza la propuesta metodológica a seguir para realizar la evaluación de seguridad a un sistema de control industrial. La propuesta consta de 5 etapas, la primera etapa consiste en determinar el alcance y los términos de la evaluación, la segunda etapa consiste en recolectar información clave sobre los activos del sistema de control, la tercera etapa consiste en realizar el análisis de vulnerabilidades al sistema de control, la cuarta etapa consiste en realizar una verificación de los controles con los que cuenta el sistema de control, la quinta etapa es la presentación de los resultados a la organización objetivo de la evaluación.

5.1 DEFINICIÓN DEL ALCANCE Y TÉRMINOS DE LA EVALUACIÓN

Para realizar una evaluación de seguridad de un sistema de control industrial, en primer lugar, se recomienda definir las reglas que gobernarán la evaluación, describiendo lo que se desea obtener de la evaluación, el alcance y los limitantes que ésta tendrá, la información acerca de cómo se adelantará la prueba y el equipamiento con el que se va a evaluar, entre otros aspectos de gran interés para el desarrollo de la evaluación de seguridad. Todo esto debe quedar consignado en un documento que firmarán las partes involucradas en la evaluación, esto con el fin de que si alguna de las partes tiene alguna queja o reclamación en relación con la forma en la que se realiza la prueba, siempre pueda recurrir al contrato para verificar que no se vulnera ninguna norma allí establecida.

A continuación, se definirán algunas consideraciones que se recomiendan tener en cuenta en el documento que definirá las reglas que gobernarán la prueba o el contrato de la evaluación

5.1.1 Objetivo de la evaluación

Es muy importante consignar en el documento el objetivo de la evaluación, este es el porqué de la evaluación de seguridad al sistema de control industrial y los resultados que se esperan de ella. Se debe indagar a la organización responsable del sistema de control industrial a evaluar acerca de cuál es el propósito de la evaluación, es importante que este sea específico, medible, alcanzable, realista, y

acotado en el tiempo. El cumplimiento del objetivo de la evaluación marcará la línea sobre la cual se desarrollará la evaluación e indicará el éxito o fracaso de la evaluación.

5.1.2 Alcance de la evaluación

La determinación del alcance es una de las acciones más importantes antes de adelantar la evaluación de seguridad, puesto que, es donde se define específicamente qué es lo que se pretende evaluar con respecto al sistema de control industrial. Es importante concertar el alcance con la organización responsable del sistema de control industrial que será evaluada y éste debe ir estrictamente relacionado con el objetivo de la evaluación y la entidad objeto de evaluación.

5.1.3 Limitaciones de la evaluación

Las limitaciones de la evaluación también deben ir consignadas en el documento y corresponden a la delimitación del alcance hechas por la organización responsable del sistema de control industrial a evaluar. También en las limitaciones se pueden colocar las restricciones a la evaluación de seguridad que se pretende adelantar sobre el sistema de control industrial.

Se recomienda establecer como limitación la no explotación de vulnerabilidades en sistemas de control que realicen procesos muy críticos y de alta disponibilidad, puesto que esto puede ocasionar la parada del sistema ocasionando un gran daño a la organización responsable del sistema de control industrial.

5.1.4 Objeto de evaluación.

El objeto de evaluación es la entidad que será evaluada, en el caso de los sistemas de control industrial puede ser un host, la red, historiadores, HMIs, RTUs, servidores, buses de campo, DCS, o todo el sistema de control industrial SCADA.

5.1.5 Roles y responsabilidades

Se deben establecer los roles y las responsabilidades de todo el personal involucrado en la evaluación de seguridad del sistema de control industrial y estos deben quedar consignados en el documento, en lo posible realizar una tabla con los números de contacto telefónico y a través de correo electrónico.

5.1.6 Ubicación del evaluador

La ubicación del evaluador se refiere a la ubicación desde la que el evaluador realizará la evaluación de seguridad, esta puede ser interna o externa. Si la ubicación es interna es importante garantizar el acceso físico y lógico a los dispositivos que serán objeto de evaluación, definir el tipo de acceso (usuario, administrador), y realizar el acompañamiento para el acceso a locaciones remotas donde se requiera acceso físico. Si la ubicación es externa, el evaluador debe informar las características del sitio desde el que se realizará la evaluación y debe tener información para poder hacer el primer contacto con el sistema de control industrial desde fuera de la organización. La información sobre la ubicación desde la que se realizará la evaluación debe quedar consignada en el contrato.

5.1.7 Tipo de evaluación

Las evaluaciones de seguridad a los sistemas de control industrial pueden ser de tres tipos: caja blanca (Whitebox), caja gris (Graybox), y caja negra (Blackbox).

En las evaluaciones de seguridad de tipo caja negra la organización responsable del sistema de control a evaluar no entrega ningún tipo de información al evaluador acerca del objeto de evaluación, pero la organización si tiene conocimiento acerca de las actividades del análisis de seguridad, además de saber cuándo se ejecutará.

En la evaluación de tipo caja gris los analistas de seguridad tienen muy poco conocimiento acerca del objeto de evaluación, pero la organización tiene conocimiento del tipo de test y cuando se realizará.

En la evaluación de tipo caja blanca la organización responsable del sistema de control a evaluar entrega toda la información del objeto de evaluación al evaluador, y ésta conoce en todo momento las actividades que se realizarán sobre el objetivo. Este tipo de evaluación es el más recomendable para los sistemas de control industrial, puesto que se realiza sobre un objeto bien definido y no los expone a las alteraciones en la disponibilidad producto del reconocimiento activo de los hosts.

Es importante que el tipo de evaluación que se va a realizar al sistema de control quede consignado en el documento de contratación de la evaluación, y ahí mismo se describa la información proporcionada por la organización responsable del sistema de control objeto de evaluación.

5.1.8 Equipamiento del evaluador

El equipamiento del evaluador debe quedar descrito en el documento de contratación de la evaluación, este corresponde al hardware y software usado para realizar las diferentes actividades de la evaluación de seguridad al sistema de control industrial. El equipamiento que no esté descrito en esta sección se puede considerar como no autorizado y puede constituir una violación al contrato de la evaluación.

5.1.9 Cronograma de la evaluación

En el cronograma de evaluación se debe consignar un resumen de las actividades a realizar durante la evaluación de seguridad al sistema de control industrial, la hora, fecha y los responsables de cada actividad. También es importante agendar en el cronograma las reuniones periódicas que se deben realizar con el personal responsable de la organización para informar sobre el avance de la evaluación y los problemas que se han encontrado al momento de desarrollar las distintas actividades.

5.1.10 Comunicaciones

Las comunicaciones con la organización son una parte importante de la evaluación de seguridad de un sistema de control industrial, puesto que esa interacción y la forma en la que se realiza puede marcar una diferencia en el sentimiento de satisfacción con respecto a la evaluación de seguridad.

Debido a la criticidad de los sistemas de control industrial, es muy probable que sucedan emergencias durante la evaluación de seguridad, por lo cual, es una práctica muy recomendable tener toda la información de contacto del personal involucrado con el objeto de evaluación, incluyendo proveedores y partes interesadas.

Para la comunicación de información confidencial a la organización se debe establecer un medio de comunicación seguro, y toda la información que viaje sobre él debe ir cifrada siempre.

5.1.11 Manejo de la evidencia

Durante la evaluación de seguridad al sistema de control industrial es importante el recaudo de evidencia que permita probar la existencia de amenazas, fallas y vulnerabilidades encontradas y estas deben estar documentadas en el informe final de la evaluación y deben ser entregadas a la organización utilizando algún tipo de cifrado seguro.

5.1.12 Autorización

La autorización es el documento firmado por los representantes legales de la organización responsable del sistema de control a evaluar y autoriza a los analistas de seguridad para realizar la evaluación de seguridad sobre el objeto de evaluación definido. Este documento es muy importante y se debe tener firmado por las partes antes de iniciar el proceso de evaluación de seguridad al sistema de control industrial, puesto que es garantía para las partes de que la prueba de seguridad se desarrollará conforme fue planificada y contratada.

5.2 RECOLECCIÓN DE INFORMACIÓN

La recolección de información se refiere a la primera etapa del proceso práctico de la evaluación de seguridad sobre el sistema de control industrial. En esta etapa se pretende obtener la mayor cantidad de información posible sobre el sistema de control industrial objeto de evaluación, con el fin de tener una clara imagen del objetivo, conocer su funcionamiento, su diseño, encontrar posibles fallos comunes de implementación, que ocurren de pasar de la etapa de diseño a la de operación.

Con el fin de seguir una metodología clara, se clasifica la recolección de información en dos partes, de acuerdo con su grado de agresividad sobre el objeto de evaluación, estas son, las técnicas de recolección pasivas y activas.

5.2.1 Técnicas de recolección pasivas.

Las técnicas de recolección de información pasivas consisten en examinar de forma pasiva el sistema de control industrial en busca de información que permita descubrir información acerca del objeto de evaluación, como puede ser el proceso que ejecuta, los puertos abiertos, los servicios que se están ejecutando y los posibles fallos de seguridad. En esta fase se revisa información de documentación, registros, reglas, configuraciones, uso del protocolo whois, hacking con buscadores, ingeniería social, e información de fuentes OSINT.

5.2.1.1 Revisión de la documentación. Con la revisión de la documentación sobre el sistema de control industrial se pretende determinar si los aspectos técnicos, las políticas de seguridad y los procedimientos se encuentran actualizados y la documentación es exhaustiva, por lo general, se revisan documentos relacionados con las políticas de seguridad del sistema de control industrial, su arquitectura, los procedimientos de operación, los planes de seguridad, actualización y de respuesta a incidentes.

Lo que se busca con la revisión de la documentación es encontrar fallas, o puntos débiles el sistema de control que no estén documentadas correctamente, cómo procedimientos mal documentados o diseñados, uso de protocolos o sistemas operativos obsoletos, software desactualizado, hardware obsoleto, entre otros.

La revisión de la documentación del sistema de control industrial objetivo es útil para ajustar la evaluación de seguridad. Por ejemplo, si existe documentación acerca de los protocolos utilizados por los equipos en la arquitectura del sistema, esta información se puede usar para configurar las herramientas que evaluarán esos protocolos.

5.2.1.2 Revisión del registro. Los sistemas de control industrial por lo general registran todos los eventos que ocurren en los procesos. La revisión de los registros es útil para verificar que el sistema esté funcionando de acuerdo con las políticas establecidas, y puede también revelar problemas de seguridad como intentos de intrusiones, accesos no autorizados, servicios mal configurados, o procesos que están fallando en el sistema de control industrial. Es muy importante realizar la revisión de todos los registros de los dispositivos y sistemas de los procesos críticos del sistema de control industrial.

5.2.1.3 Revisión de las reglas. La revisión de las reglas es útil para identificar posibles brechas de seguridad y debilidades en los dispositivos de seguridad del sistema de control industrial, como los firewalls, IDS/IPS y las ACLS de los dispositivos de enrutamiento.

Es importante revisar las reglas en los dispositivos de seguridad del sistema de control industrial para asegurarse de que no haya puertos o servicios abiertos que puedan aprovecharse con alguna vulnerabilidad. Las reglas deben estar debidamente documentadas para cada dispositivo.

5.2.1.4 Revisión de las configuraciones. La revisión de la configuración de los diferentes dispositivos de un sistema de control industrial permite identificar vulnerabilidades en las configuraciones de acuerdo con las políticas de seguridad establecidas para el sistema. También se pueden encontrar servicios o puertos que están abiertos innecesariamente, dispositivos configurados con contraseñas por defecto, equipos con información crítica sin cifrado de datos o de comunicaciones. Se recomienda realizar un checklist de las configuraciones de cada dispositivo objeto de evaluación para verificar si cumple con la documentación revisada.

La revisión de la documentación es utilizada para ayudar también a ajustar la evaluación de seguridad sobre el sistema de control industrial. Por ejemplo, en la

revisión de la documentación se pueden encontrar usuarios y contraseñas por defecto que pueden ser probadas en el proceso de evaluación para verificar el acceso a un equipo o dispositivo objeto de evaluación.

5.2.1.5 Utilización del protocolo WHOIS. El protocolo WHOIS es un protocolo TCP que es utilizado para realizar consultas a una base de datos permitiendo determinar el propietario de un nombre de dominio o una IP pública. Con este protocolo es posible encontrar información de contacto del propietario de un dominio público o dirección IP pública de la organización responsable del sistema de control industrial, y se puede recolectar información que puede ser útil en un proceso de ingeniería social, o de suplantación de identidad, si el administrador o responsable del dominio olvida renovar el contrato.

5.2.1.6 Hacking con buscadores. Existen algunos motores de búsqueda diseñados para buscar dispositivos y sistemas de control conectados a Internet. Realizar una búsqueda con estos motores puede resultar importante para verificar que el sistema de control a evaluar no esté indexado y en caso tal de estarlo cuente con las medidas de seguridad y protección correspondientes.

5.2.1.7 Ingeniería social. La ingeniería social consiste en verificar que información confidencial se puede obtener a través de la manipulación de usuarios legítimos del sistema de control industrial. Es útil para determinar si con la información obtenida de los usuarios del sistema de control industrial, (operadores y administradores) es posible acceder con privilegios y realizar alguna actividad que lo comprometa. Se recomienda documentar las técnicas de ingeniería social utilizadas y la información recabada con la actividad.

5.2.1.8 OSINT. Open Source Intelligence es una técnica que consiste en la recopilación de información a partir de fuentes abiertas como la prensa escrita, radio, televisión, informes escritos o cualquier tipo de recurso público disponible. Se recomienda el uso de OSINT con el fin de verificar que información confidencial del sistema de control industrial a evaluar no esté disponible de forma pública. Se deben documentar todos los recursos en los que se encontró información pública acerca del sistema de control y evidenciar el tipo de información que fue hallada.

5.2.2 Técnicas de recolección activas

Las técnicas de recolección de información activas usan herramientas agresivas que buscan puertos y servicios activos en el sistema de control industrial, con el fin de recolectar información acerca del protocolo, servicio, aplicación o sistema operativo que se está ejecutando. También sirve para corroborar la información que fue recolectada de forma pasiva.

La información recolectada con las técnicas activas es útil para ajustar el proceso de análisis de vulnerabilidades sobre el objeto de evaluación y entrega gran cantidad de evidencia para desarrollar el informe de resultados.

5.2.2.1 Descubrimiento de redes. Se usan herramientas que facilitan el descubrimiento de equipos activos en la red del sistema de control industrial, por lo general, se envían peticiones de respuesta usando el protocolo ICMP, para determinar que equipos están activos, que sistemas operativos o aplicaciones están ejecutando, que puertos están abiertos y que servicios están activos. La información recolectada es útil para delimitar el alcance de la evaluación de seguridad, realizar un mapeo de la arquitectura del sistema de control industrial, descubrir dispositivos de seguridad como firewalls o IDS/IPS, o encontrar vulnerabilidades en los sistemas o sus protocolos.

Es importante tener en cuenta que los sistemas de control industrial usan diferentes medios de transmisión para comunicar los dispositivos, por ello el descubrimiento de redes se debe hacer sobre todos los medios posibles como cableado e inalámbrico (WLAN, Bluetooth).

Se recomienda tomar evidencias de todo el proceso para soportar la documentación de los resultados de la evaluación sobre el sistema de control industrial.

5.2.2.2 Sniffing de redes. Es una técnica que consiste en escuchar el tráfico que transita por la red del sistema de control industrial, con el fin de capturarlo para su posterior análisis. Con el Sniffing de redes se pueden encontrar protocolos vulnerables, comunicaciones no cifradas, identificar sistemas operativos, aplicaciones, servicios y puertos abiertos abiertos, así como protocolos no autorizados. También es posible capturar información correspondiente a usuarios y contraseñas de los diferentes dispositivos presentes en el sistema de control industrial.

El Sniffing de redes requiere de conectarse físicamente a un puerto por el que pase todo el tráfico del sistema de control industrial, es por ello, que es importante contar con las autorizaciones correspondientes para acceder a esos equipos e informar a la organización de los posibles riesgos.

Se recomienda realizar capturas del proceso para ser utilizadas como evidencia en el informe de resultados que se entrega a la organización.

5.2.2.3 Banner grabbing. El banner grabbing es una técnica de interacción manual sobre el dispositivo o equipo que se está evaluando en el momento y consiste en verificar el funcionamiento del puerto, servicio, aplicación o sistema que está ejecutándose en el dispositivo de control industrial. Por ejemplo, muchos dispositivos de control industrial actuales poseen servidores web para realizar su configuración, usando la técnica de banner grabbing se puede hacer uso de un navegador web para verificar el acceso a la página que despliega el servidor web del dispositivo evaluado.

Se recomienda realizar captura de la información producto de la interacción con los diferentes dispositivos ya que puede ser usada como evidencia y como material de apoyo para la detección de fallas y vulnerabilidades.

5.3.3 Checklist para activos hallados.

En la tabla de abajo se propone un modelo de lista de chequeo para la identificación de los activos hallados en el proceso de recolección de información, estos activos deben ser los mismos que se encuentran definidos en el alcance de la evaluación. En la lista de chequeo se deben documentar la organización propietaria del sistema de control a evaluar, el nombre del evaluador que identificó el activo, la ubicación del activo, el responsable de ese activo, la fecha y hora en la que se produjo la identificación del activo, las observaciones a que haya lugar, y las características del activo identificado como el nombre, la dirección IP (si aplica), sistema operativo, la acción que realiza, los puertos abiertos y los servicios que está ejecutando.

Se recomienda acompañar esta tabla de la evidencia recolectada para el activo en el informe de resultados de la evaluación del sistema de control industrial.

Tabla 11. Checklist identificación de activos.

CHECKLIST DE IDENTIFICACIÓN DE ACTIVOS						
ORGANIZACIÓN						
EVALUADOR						
UBICACIÓN						
RESPONSABLE						
FECHA				HORA		
OBSERVACIONES						
ID Activo	Nombre del activo	Dirección IP	Sistema operativo	Acción	Puertos	Servicios

5.3 ANÁLISIS DE VULNERABILIDADES

El núcleo de una evaluación de seguridad a un sistema de control industrial es la identificación de las amenazas y las vulnerabilidades que afectan al ICS. En esta etapa se propone al evaluador en primer lugar identificar si las amenazas que fueron expuestas en el capítulo anterior se encuentran presentes en el sistema y luego evaluar las vulnerabilidades segmentando el sistema de control en un dominio de TI y el dominio ICS, posteriormente se deben tomar todas las evidencias correspondientes a las vulnerabilidades, sea que se encuentren presentes o no, con el fin de realizar el informe de resultados. En el informe de resultados es importante reseñar las contramedidas que ayudarían a superar las amenazas o vulnerabilidades que presenta el sistema de control industrial.

En el dominio de TI se encuentran los equipos, dispositivos, servicios y personas que a pesar de hacer parte del sistema de control industrial no hacen parte del proceso productivo, algunos ICS pueden o no tener esa configuración, eso depende de la arquitectura del ICS. En el dominio ICS se encuentran todos los equipos, dispositivos, servicios y personas que forman parte del proceso productivos. Ambos dominios conforman el sistema de control industrial y deben ser analizados en busca de vulnerabilidades.

Una aclaración importante a tener en cuenta es que en esta metodología de evaluación no se proponen pautas para la explotación de vulnerabilidades en un sistema de control industrial, debido a que son sistemas que controlan procesos muy críticos que pueden verse afectados y pueden impactar negativamente las operaciones de la organización. Además, no se aconseja realizar el análisis de vulnerabilidades de manera activa sobre el sistema de control industrial en producción, ya que puede provocar fallos y degradación en el rendimiento del proceso, sin embargo, esto se deja al criterio de la organización objetivo de la evaluación de seguridad.

5.3.1 Vulnerabilidades de los sistemas de control industrial.

Una vulnerabilidad es una debilidad en la seguridad de un sistema de control industrial que puede llegar a comprometer alguno de los objetivos principales de seguridad de la información, integridad, confidencialidad, disponibilidad. Las vulnerabilidades pueden ser encontradas en las políticas y procedimientos, la arquitectura y el diseño, la configuración y el mantenimiento, el software, las comunicaciones y las redes y/o en la planta física.

El análisis de vulnerabilidades es la parte más importante de una evaluación de la seguridad en los sistemas de control industrial, puesto que su resultado es fundamental para cumplir con los objetivos trazados en el contrato de evaluación.

En la evaluación de vulnerabilidades se usa toda la información recaudada en las etapas anteriores donde se determina el alcance y los términos de la evaluación y se recolecta la información del objetivo que se evaluará. Con esa información se procede a realizar el análisis de vulnerabilidades sobre los activos contemplados en el alcance e individualizados en la etapa de recolección de información, luego se toma la evidencia de todo el proceso para documentar el reporte final a entregar.

5.3.1.1 Evaluación de vulnerabilidades pasiva. En la evaluación de vulnerabilidades pasiva se realizan conexiones directas con los objetos de evaluación identificados en la etapa de recolección de información, también se analizan metadatos y se monitoriza el tráfico para identificar comportamientos sospechosos, información confidencial o probar contraseñas por defecto que puedan representar una vulnerabilidad en el sistema de control industrial

5.3.1.2 Evaluación de vulnerabilidades activa. Para la evaluación de vulnerabilidades de forma activa se recomienda realizar pruebas de autenticación, autorización, gestión de sesión, lógica de negocio, e inyección de código sobre los dispositivos que permitan esta opción o tengan algún tipo de aplicación para registrar sesiones de usuario. También se recomienda escanear vulnerabilidades en los diferentes tipos de redes que usan los sistemas de control (buses de campo, redes LAN, wifi, bluetooth), basándose en los puertos y servicios que se encuentran en el entorno del sistema de control industrial. Se deben explorar también vulnerabilidades en dispositivos de seguridad como firewalls e IDS/IPS, verificando si las reglas configuradas funcionan apropiadamente o presentan alguna vulnerabilidad. Se pueden usar con esta técnica escáneres de vulnerabilidades.

Algunos dispositivos de control industrial actuales traen embebido aplicaciones web, es importante realizar análisis de vulnerabilidades web sobre estos dispositivos.

Se recomienda realizar pruebas con los protocolos que usa el sistema de control industrial de forma específica como MODBUS, DNP3, IEC 61850, ICCP, ZigBee, entre otros. También es importante verificar vulnerabilidades que estén registradas en las diferentes listas de vulnerabilidades de seguridad como CVE, OSVDB, o vulnerabilidades publicadas por cada proveedor del producto que se está evaluando.

Escanear todos los dispositivos involucrados en el sistema de control industrial es una obligación para el evaluador y se debe evidenciar esta actividad en el informe de resultados de la evaluación.

5.3.3 Checklist análisis de vulnerabilidades.

En la tabla de abajo se propone una lista de chequeo para el análisis de amenazas y vulnerabilidades en la cual se relacionan datos de la organización evaluada, el evaluador, la ubicación del activo, el responsable del activo, la fecha y hora en la que fue evidenciada la amenaza y la vulnerabilidad, el identificador del activo, el nombre del activo, el proceso que realiza en el sistema de control industrial, las amenazas presentes y las vulnerabilidades halladas.

Tabla 12. Checklist análisis de vulnerabilidades

CHECKLIST DE ANÁLISIS DE AMENAZAS Y VULNERABILIDADES				
ORGANIZACIÓN				
EVALUADOR				
UBICACIÓN				
RESPONSABLE				
FECHA			HORA	
OBSERVACIONES				
ID ACTIVO	NOMBRE DEL ACTIVO	PROCESO	AMENAZAS	VULNERABILIDADES

5.4 VERIFICACIÓN DE LOS CONTROLES IMPLEMENTADOS

En la presente propuesta metodológica para evaluar los sistemas control industrial SCADA se plantea realizar la verificación de los controles actualmente implementados en el sistema evaluado, con el fin de documentarlos y determinar si están siendo efectivos o requieren modificación. Para ello, se relacionan los controles de seguridad más comúnmente encontrados en los sistemas de control industrial y se propone al evaluador una lista de chequeo en la que debe anotar si los controles existen, si existen, pero no son efectivos, si son efectivos, pero no están documentados, o si son efectivos y están documentados.

Lo que se pretende con esta verificación de controles es complementar la información obtenida en la etapa de análisis de vulnerabilidades, con el fin de proponer contramedidas que ayuden a subsanar las brechas de seguridad encontradas durante la evaluación.

Tabla 13. Evaluación de controles implementados.

CHECKLIST CONTROLES DE SEGURIDAD PARA SISTEMAS DE CONTROL INDUSTRIAL SCADA			
ORGANIZACIÓN			
EVALUADOR			
UBICACIÓN			
RESPONSABLE			
FECHA		HORA	
OBSERVACIONES	Calificación del control (1 control no existe, 2 existe, pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)		
CONTROL	SUBCONTROL	OBSERVACIÓN	CALIFICACIÓN
Control de acceso	Control de acceso basado en roles		
	Control de acceso a servidores web		
	Redes de área local virtual (VLAN)		
	Módems de acceso telefónico		
	Control de acceso inalámbrico		
Concientización y entrenamiento	Capacitación del personal en políticas y procedimientos de seguridad		
Auditorías a las políticas y procedimientos	Auditoría a los controles para garantizar el cumplimiento de políticas y procedimientos de seguridad		
Evaluaciones de seguridad	Evaluaciones de seguridad periódicas al sistema de control industrial		
Gestión de la configuración	Control de modificaciones al hardware		
	Control de modificaciones al firmware		
	Control de modificaciones al software		
	Plan de pruebas implementado		
	Documentación de los procesos de configuración		
Planificación de contingencias	Plan de continuidad del negocio implementado		

CHECKLIST CONTROLES DE SEGURIDAD PARA SISTEMAS DE CONTROL INDUSTRIAL SCADA			
ORGANIZACIÓN			
EVALUADOR			
UBICACIÓN			
RESPONSABLE			
FECHA		HORA	
OBSERVACIONES	Calificación del control (1 control no existe, 2 existe, pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)		
CONTROL	SUBCONTROL	OBSERVACIÓN	CALIFICACIÓN
	Plan de recuperación de desastres implementado		
Identificación y autenticación	Autenticación por contraseña		
	Doble autenticación		
	Autenticación con token físico		
	Autenticación con tarjeta inteligente		
	Autenticación biométrica		
Respuesta a incidentes	Plan de respuesta a incidentes implementado		
Mantenimiento	Plan de mantenimiento rutinario al sistema de control industrial		
Protección de medios	Uso de dispostivos firewall		
	Uso de dispositivos IDS/IPS		
	Redes privadas virtuales (VPN)		
	Uso de cifrado de comunicaciones		
Protección de acceso físico	Políticas y procedimiento de acceso físico al sistema de control industrial		
	Monitoreo de acceso físico		
	Registros de acceso		
	Manejo de visitantes		
	Seguridad física en el centro de control		
	Uso de equipos y dispositivos fuera de la red del sistema de control industrial		

CHECKLIST CONTROLES DE SEGURIDAD PARA SISTEMAS DE CONTROL INDUSTRIAL SCADA			
ORGANIZACIÓN			
EVALUADOR			
UBICACIÓN			
RESPONSABLE			
FECHA		HORA	
OBSERVACIONES	Calificación del control (1 control no existe, 2 existe, pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)		
CONTROL	SUBCONTROL	OBSERVACIÓN	CALIFICACIÓN
	Seguridad del cableado		
Planificación de la seguridad	Plan de seguridad implementado		
Seguridad del personal	Políticas y procedimientos frente a errores del personal		
	Políticas y procedimientos frente a robos o fraudes		
Integridad de la información	Detección de virus y código malicioso		
	Detección y prevención de intrusiones		
	Gestión de parches		

5.5 PRESENTACIÓN DE LOS RESULTADOS DE LA EVALUACIÓN

El producto final de una evaluación de seguridad a un sistema de control industrial es el informe de resultados de la evaluación, es el documento donde se informa a la organización solicitante el resultado de la evaluación y cómo se llevó a cabo, adjuntando las evidencias recolectadas durante el proceso.

A continuación, se relacionan algunas secciones que se recomienda lleve el informe de resultados de la evaluación.

5.5.1 Objetivo de la evaluación de seguridad.

Es importante relacionar el objetivo de la evaluación de seguridad debido a que este es un factor fundamental para definir el éxito de la evaluación.

5.5.2 Tiempo total de la evaluación.

Se debe indicar el tiempo total que duró la evaluación y las fechas y horarios en las que se realizaron las distintas actividades con el fin de que la organización solicitante revise si se cumplieron sus expectativas.

5.5.3 Alcance y limitaciones de la prueba.

Es importante incluir el alcance y las limitaciones de la prueba para asegurar que en todo momento la prueba cumplió con las especificaciones iniciales de la organización solicitante.

5.5.4 Objetos de evaluación

Relacionar todos los objetos evaluados en la auditoría de seguridad del sistema de control industrial.

5.5.5 Descripción de las amenazas y vulnerabilidades encontradas

Descripción de las amenazas y vulnerabilidades encontradas en el sistema de control industrial, adjuntando las evidencias recolectadas durante la evaluación.

5.5.6 Descripción de los controles hallados.

Descripción de los controles hallados durante la verificación de los controles de seguridad del sistema de control industrial.

5.6.7 Recomendaciones

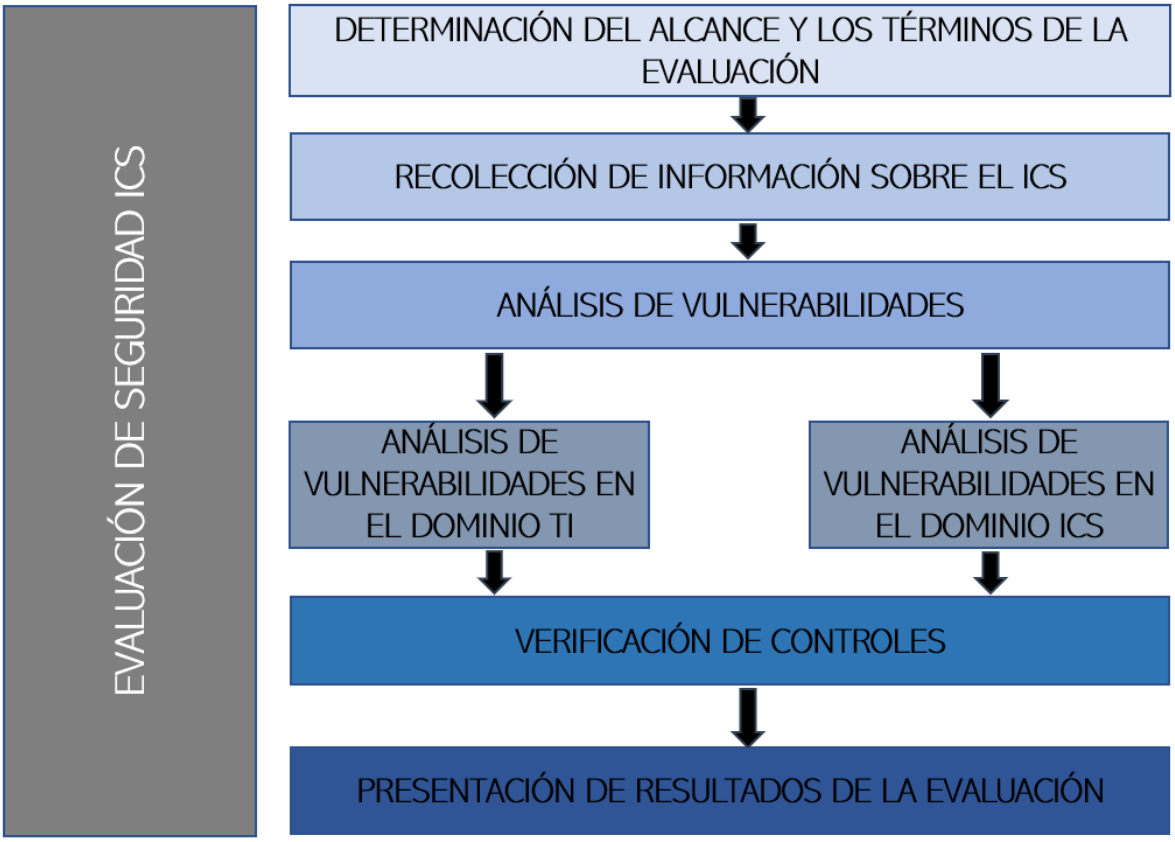
Es importante garantizar realizar las recomendaciones encaminadas a corregir las distintas amenazas y vulnerabilidades encontradas durante la evaluación del sistema de control industrial.

6. REPRESENTACIÓN GRÁFICA DE LA METODOLOGÍA DE EVALUACIÓN

La metodología de evaluación de la ciberseguridad de los sistemas de control industrial que se propone en este trabajo de grado consta de 5 etapas, donde cada etapa entrega un insumo a la etapa siguiente que la nueva etapa procesa para producir un resultado. En la primera etapa se establece el procedimiento a seguir para determinar el objetivo de la evaluación, el alcance, las limitaciones, el objeto de evaluación, los roles y responsabilidades que tendrán los interesados, la ubicación del evaluador, el tipo de evaluación, las herramientas que se van a usar, el cronograma de la evaluación, la forma como se realizarán las comunicaciones con el equipo, el manejo de la evidencia y la autorización del cliente para iniciar la evaluación; esta etapa produce el entregable para la siguiente etapa, la etapa de recolección de información, basados en el alcance y el objeto de la evaluación se procede a recolectar información sobre el sistema de control objeto de la evaluación, usando técnicas de recolección pasivas y activas según se haya pactado con el cliente, esta etapa produce un entregable para la etapa de análisis de vulnerabilidades, en la cual el evaluador realiza un análisis de vulnerabilidades segmentando el sistema de control industrial en dos dominios, el dominio TI, donde se encuentran todos los equipos, dispositivos, servicios y personal que no forma parte del proceso industrial, y el dominio ICS donde se analizan las vulnerabilidades de todos los equipos, dispositivos, servicios y personal que forma parte activa del proceso industrial, este proceso desarrolla un entregable que se usa en la siguiente como complemento para verificar los controles implementados, con esta información se produce un entregable para la siguiente etapa, en la cual se realiza el informe de resultados de la evaluación y que contiene el objetivo de la evaluación de seguridad, el tiempo que tomó la evaluación, el alcance y las limitaciones pactadas, los activos objeto de la evaluación, las amenazas y vulnerabilidades encontradas, los controles hallados y las contramedidas y recomendaciones que se realizan al propietario del sistema.

En la figura 19 se puede observar una representación gráfica, modular y por etapas de la metodología para la evaluación de la ciberseguridad de los sistemas de control industrial que se propone en este trabajo de grado.

Figura 19. Representación gráfica de la metodología de evaluación propuesta.



CONCLUSIONES

Con la investigación, recolección y análisis de la información relacionada con los sistemas de control industrial se observó que en la actualidad no hay una metodología de evaluación de ciberseguridad que englobe los ICS a un nivel general, a pesar de que se encontraron marcos de trabajo enfocados en la implementación segura de los ICS y una metodología de pruebas de penetración dirigida a los sistemas de generación de energía eléctrica y SmartGrid (NESCOR).

Durante el desarrollo del trabajo de grado se encuentra que a pesar de la amplia adopción de dispositivos TI en los sistemas de control industrial, los ICS tienen varias características que los diferencian de la postura de seguridad de los sistemas TI, mientras para estos lo importante es la confidencialidad, integridad y disponibilidad de los datos, para los ICS lo importante es la disponibilidad y seguridad del proceso industrial, esto hace que cosas como la integridad y la confidencialidad pasen a un segundo plano cuando de evaluar la seguridad de los ICS se trata.

En el proceso de identificación de las amenazas y vulnerabilidades en los sistemas de control industrial se observa que, al llegar a materializarse alguna vulnerabilidad en un ICS, y dependiendo de su impacto, las consecuencias físicas, ambientales, en vidas humanas pueden ser muy importantes y pueden llegar a provocar un gran impacto en la seguridad y la economía de una nación.

Se encuentra que a pesar de que la convergencia de tecnologías de la información y tecnología operativa en los sistemas de control industrial brinda a las empresas una mayor integración y visibilidad de los activos críticos, la logística y los procesos operativos, existen diferencias significativas entre una evaluación de ciberseguridad en ICS y un sistema TI, por ello se aconseja en la metodología de evaluación cuando se analizan las vulnerabilidades, aprovechar la información recolectada sobre el objetivo para segmentar sistema de control industrial en dos dominios, el dominio ICS y el dominio TI.

El desarrollo de la metodología de evaluación de ciberseguridad en los sistemas de control que se desarrolla por etapas produce entregables que se usan como insumo

de la siguiente etapa del proceso, estos resultados de cada etapa se convierten en entregables parciales que se pueden ir entregando a los interesados para mostrar el avance de la evaluación de ciberseguridad del ICS.

La metodología de evaluación de ciberseguridad propuesta en este trabajo de grado pretende ser un documento de apoyo a las organizaciones y profesionales relacionados con la ciberseguridad de los sistemas de control industrial en el mundo y su beneficio real es la disminución del riesgo debido al descubrimiento y corrección de las vulnerabilidades, por lo que este beneficio depende de las capacidades técnicas y financieras de la organización propietaria del ICS objeto de evaluación para mitigar las vulnerabilidades identificadas.

RECOMENDACIONES

Antes de realizar la evaluación de seguridad se aconseja realizar una planeación bien estructurada y en conjunto con todos los involucrados en el sistema de control industrial con el fin de afectar en lo más mínimo los procesos críticos que se realizan por parte del ICS y firmar un documento que evidencie el alcance y los términos en los que se desarrollará la evaluación de seguridad.

Se recomienda al evaluador no superar el alcance pactado con la organización propietaria del sistema de control a evaluar sin autorización de esta, puesto que esto puede tener serias consecuencias penales.

La recolección de información referente a los activos de los sistemas de control industrial debe realizarse teniendo en cuenta el entregable de la primera etapa, en el cual se indica el objetivo de la evaluación, su alcance, las limitaciones y el objeto a evaluar, así como las herramientas que se utilizarán y el tipo de evaluación a desarrollar. Realizar acciones por fuera de lo pactado puede significar enfrentar multas o consecuencias penales por incumplimiento del contrato y pueden afectar el rendimiento del sistema de control industrial.

Se recomienda segmentar el sistema de control de acuerdo con los dominios de TI y de ICS, esto con el fin de realizar un análisis enfocado en la postura de seguridad de cada entorno.

No se aconseja realizar un análisis de vulnerabilidades activo sobre un sistema de control industrial en producción por se pueden producir degradaciones del rendimiento del proceso productivo que pueden producir comportamientos erráticos del ICS y pueden llegar incluso a parar la producción

No se aconseja la explotación de las vulnerabilidades en los sistemas de control industrial, esto debido a que son sistemas que manejan procesos muy críticos que no se pueden afectar en su disponibilidad ni productividad. Si es necesario explotar alguna vulnerabilidad, es importante respaldar la configuración del sistema y contar

en todo momento con la autorización escrita del propietario del sistema de control industrial.

Es importante evidenciar todas las actividades que se realicen sobre el sistema de control industrial, al igual que las respuestas que se obtengan de este, con el fin de plasmar esta información en el reporte de resultados que se entrega a los directivos, responsables administrativos y técnicos.

BIBLIOGRAFÍA

ACKERMANN, Pascal. Industrial Cybersecurity. Packt Publishing, 2017, pp. 23-65.

ANDREW, Wilson. CREST Industrial Control Systems Technical Security Assurance Position Paper. [En línea]. {16 de diciembre 2019}. Disponible en: https://www.crest-approved.org/wp-content/uploads/CREST-Industrial-Control-Systems-Technical-Security-Assurance-Position-Paper.pdf

BALCELLS SENDRA, Josep. Autómatas programables. Barcelona: Marcombo, 1997.

BARCELÓ, Martha. HERZOG, Pete. OSSTMM 3: The Open Source Security Testing Methodology Manual. {En línea}. {3 de junio de 2018}. Disponible en: http://www.isecom.org/mirror/OSSTMM.3.pdf

BÉCUE, Adrien. CUPPENS-BOULAHIA, Nora. Security Of Industrial Control Systems And Cyber Physical Systems. Cham: Springer, 2017.

BODUNGEN, Clint. SINGER, Bryan. SHBEEB, Aaron. Hacking Exposed, Industrial Control Systems. New York: McGraw-Hill Education, 2017.

BROTHERSTON, Lee. BERLIN, Amanda. Defensive Security Handbook. Sebastopol: O'Reilly Media, 2017. pp. 13-34.

BSI. STUDY A PENETRATION TESTING MODEL. {En línea}. {10 de mayo de 2018}. Disponible en: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile

CASTILLO, Javier. Estableciendo Zonas y Conductos Según el Estándar ISA99/IEC6443. Madrid: Centro De Ciberseguridad Industrial. 2018, PP. 27-36

CASTRO GIL, Manuel Alonso. Comunicaciones industriales. Madrid: UNED, 2012. pp. 103-158.

CENTRO CRIPTOLÓGICO NACIONAL. CCN-STIC-480 SEGURIDAD EN SISTEMAS SCADA. 2010. pp18-20

CHENG, Peng. CHEN, Jiming. Cyber Security For Industrial Control Systems. New York: CRC Press, 2016. pp. 57-95.

COBB, Stephen. TENDENCIAS EN CIBERSEGURIDAD 2018: EL COSTO DE NUESTRO MUNDO CONECTADO. {En línea}. {10 de mayo de 2018}. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf

COLBERT, Edward. KOTT, Alexander. Cyber-Security Of SCADA And Other Industrial Control Systems. Berlin: Springer, 2016.

COLPRENSA BOGOTÁ. (2015). Más de 74% de pequeñas y medianas empresas están conectadas a Internet. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.vanguardia.com/mundo/tecnologia/323706-mas-de-74-de-pequenas-y-medianas-empresas-estan-conectadas-a-internet

CPNI. Cyber Security Assessments Of Industrial Control Systems. [En línea]. {16 de diciembre 2019}. Disponible en: https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/CPNI-Guia-SCI.pdf

DIOGENES, Yuri. OZKAYA, Erdal. Cybersecurity - Attack And Defense Strategies. Birmingham: Packt Publishing, 2018 pp. 76-117.

FORSHAW, James. Attacking Network Protocols: A Hacker's Guide To Capture, Analysis, And Exploitation. San Francisco: No Starch Press, 2018.

GINTER, Andrew. SCADA Security: What's Broken and How To Fix. Calgary: Abterra Technologies, 2018. pp. 15-47.

GÓMEZ VIEITES, Álvaro. Auditoría De Seguridad Informática. Bogotá: Ediciones De La U, 2013.

GÓMEZ, Luis, and Pedro Pablo FERNÁNDEZ. Cómo Implantar Un SGSI Según ISO/IEC 27001. Bogotá: Alfaomega, 2018. pp. 57-132.

GONZÁLEZ PÉREZ, Pablo. ALONSO CEBRIÁN, José María. Metasploit Para Pentesters. Madrid: Zeroxword Computing, 2016, pp. 13-62.

GONZÁLEZ PÉREZ, Pablo. SÁNCHEZ GARCÉS, German. Pentesting Con Kali. Madrid: Zeroxword, 2013.

GUERRERO, Vicente. YUSTE, Ramón L. MARTÍNEZ, Luis. Comunicaciones industriales. Barcelona: Marcombo, 2016.

ICONTEC. NORMA TÉCNICA COLOMBIANA NTC 5613. {En línea}. {10 de febrero 2018}. Disponible en: http://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC5613.pdf

ICONTEC. NORMA TÉCNICA COLOMBIANA NTC 5613. {En línea}. {10 de febrero 2018}. Disponible en: http://www.politecnicojic.edu.co/images/downloads/biblioteca/guias/NTC4490.pdf

INCIBE. IEC 62443: Evolución de la ISA 99. INCIBE-CERT [En línea]. {16 de diciembre 2019}. Disponible en: https://www.incibe-cert.es/blog/iec62443-evolucion-isa99

KAPOOR, Nilesh. SCADA Penetration Testing: Do I need to be prepared?. [En línea]. {16 de diciembre 2019}. Disponible en: https://research.aurainfosec.io/scada-penetration-testing/

KNAPP, Eric. LANGILL, Joel Thomas. Industrial Network Security. Waltham: Syngress, 2015.

KNAPP, Eric. SAMANI, Raj. Applied Cyber Security And The Smart Grid. Waltham: Syngress, 2013. pp. 52-55, 101-122.

LANGNER, Ralph. Robust Control System Networks: How to Achieve Reliable Control After Stuxnet. New York: Momentum Press, 2012.

MACAULAY, Tyson. SINGER, Bryan. Cybersecurity For Industrial Control Systems. Boca Raton: CRC Press, 2012.

NEIL, Ian. Comptia Security+ Certification Guide. Birmingham: Packt Publishing, 2018. pp. 45-65

PÉREZ SAN-JOSÉ, Pablo. Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA). 2012. pp 17-30.

PICÓ GARCÍA, José. PÉREZ CONDE, David. Hacking Y Seguridad En Comunicaciones Móviles GSM-GPRS-UMTS-LTE. Madrid: Zeroxword Computing, 2014.

RADVANOVSKY, Robert. BRODSKY, Jacob. Handbook Of SCADA/Control Systems Security, Second Edition. 2da Ed. Boca Raton: CRC Press, 2016. pp. 209-229.

RICCETTI, Simone. Industrial Control Systems Security: To Test or Not to Test?. [En línea]. {16 de diciembre 2019}. Disponible en:

https://securityintelligence.com/posts/industrial-control-systems-security-to-test-or-not-to-test/

RODRÍGUEZ PENÍN, Aquilino. Sistemas SCADA. 2da. Edición. Barcelona: Marcombo 2007. pp. 65 -76, 133-136.

RUIZ CANALES, Antonio. MOLINA MARTÍNEZ, José Miguel. Automatización y telecontrol de sistemas de riego. Barcelona: Marcombo, 2010. pp. 382-390.

SCARFONE, Karen. SOUPPAYA, Murugiah. CODY, Amanda. Technical Guide to Information Security Testing and Assessment. Washington: NIST, 2008.

SEARLE, Justin. Nescor: Guide to Penetration Testing for Electric Utilities. {En línea}. {10 de octubre de 2018}. Disponible en: http://smartgrid.epri.com/doc/NESCORGuidetoPenetrationTestingforElectricUtilities-v3-Final.pdf

SOTO, Carlos. (SCADA, el peligro asecha a los sistemas de infraestructura crítica. {En línea}. {10 de mayo de 2018}. Disponible en: http://www.securitic.com.mx/reportaje-especial/2373-scada-el-peligro-asecha-a-los-sistemas-de-infraestructura-critica

STOUFFER, Keith. PILLITTERI Victoria. LIGHTMAN, Suzanne. Guide to Industrial Control Systems (ICS) Security. 2da. Edición. Washington: NIST, 2015.

TORO LÓPEZ, Francisco J. Gestión De Proyectos Con Enfoque PMI. 3rd ed. Bogotá: Ecoe Ediciones, 2015. pp. 51-110.

UNAD. ACUERDO 0029 DEL 13 DE DICIEMBRE DE 2013. Reglamento estudiantil. Bogotá. 2013. p. 27-28

WEISS, Joseph. Protecting Industrial Control Systems From Electronic Threats. New York: Momentum Press, 2010. pp. 7-52.

WRIGHT, Joshua. CACHE, Johnny. Hacking Exposed Wireless. 3rd ed. New York: Mcgraw-Hill Education, 2015.

RESUMEN ANÁLITICO ESPECIALIZADO (RAE)

Tema	Seguridad informática
Título	Diseño de una metodología para la evaluación de la ciberseguridad de los sistemas de control industrial (SCADA).
Autor	Christian Camilo Mendieta Martínez.
Año de la publicación	2020
Palabras Claves	Amenaza, control, DCS, evaluación de seguridad, ICS, metodología, sistema de control industrial, SCADA, técnicas, vulnerabilidad.

Fuentes bibliográficas.

En la realización de la monografía se consultaron alrededor de 47 fuentes bibliográficas relacionadas con la seguridad informática en los sistemas de control, algunas de las fuentes consultadas fueron:

ACKERMANN, Pascal. Industrial Cybersecurity. Packt Publishing, 2017, pp. 23-65.

COLBERT, Edward. KOTT, Alexander. Cyber-Security Of SCADA And Other Industrial Control Systems. Berlin: Springer, 2016.

KNAPP, Eric. LANGILL, Joel Thomas. Industrial Network Security. Waltham: Syngress, 2015.

MACAULAY, Tyson. SINGER, Bryan. Cybersecurity For Industrial Control Systems. Boca Raton: CRC Press, 2012.

WEISS, Joseph. Protecting Industrial Control Systems from Electronic Threats. New York: Momentum Press, 2010. pp. 7-52.

Resumen

La monografía tuvo como objetivo el de presentar un diseño de una metodología que permita realizar la evaluación de la seguridad cibernética de los sistemas de control industrial (ICS/SCADA). El diseño presentado consiste en una metodología de cinco pasos, los cuales entregan lineamientos para la determinación del alcance y los términos de la evaluación de seguridad, la recolección de información sobre el ICS objetivo, el análisis de las vulnerabilidades para los dominios de TI e ICS, la verificación de los controles implementados y la presentación de los resultados de la evaluación.

Descripción del problema

El aumento en la frecuencia y severidad de los ataques a los sistemas de control industrial, sumados a la poca preparación de los profesionales para enfrentar los nuevos desafíos y la falta de metodologías que permitan evaluar la seguridad en los sistemas de control industrial son una amenaza para las infraestructuras críticas, la economía y la seguridad

nacional.

Objetivo General

Diseñar una metodología para la evaluación del estado de la ciberseguridad en los sistemas de control industrial.

Objetivos específicos

- Recolectar información referente a sistemas de control industrial y metodologías de evaluación de seguridad informática.
- Identificar las amenazas, las vulnerabilidades más comunes, los principales ataques y los controles de seguridad a tener en cuenta en los sistemas de control industrial.
- Definir los pasos metodológicos para la evaluación de seguridad en los sistemas de control industrial.
- Presentar el diseño de la metodología de evaluación de seguridad en sistemas de control industrial.

Metodología

Para la realización de la monografía se investigaron diferentes fuentes documentales de diferentes tipos de organizaciones de índole público y privado dedicadas a la seguridad informática y al control industrial. Se analizaron las metodologías encontradas, la información sobre amenazas, vulnerabilidades y controles comunes a los sistemas de control industrial y se establecieron los pasos metodológicos a seguir para evaluar un sistema de control industrial.

Contenido

La metodología de evaluación de la ciberseguridad de los sistemas de control industrial que se propone en este trabajo de grado consta de 5 etapas, donde cada etapa entrega un insumo a la etapa siguiente que la nueva etapa procesa para producir un resultado. En la primera etapa se establece el procedimiento a seguir para determinar el objetivo de la evaluación, el alcance, las limitaciones, el objeto de evaluación, los roles y responsabilidades que tendrán los interesados, la ubicación del evaluador, el tipo de evaluación, las herramientas que se van a usar, el cronograma de la evaluación, la forma como se realizarán las comunicaciones con el equipo, el manejo de la evidencia y la autorización del cliente para iniciar la evaluación; esta etapa produce el entregable para la siguiente etapa, la etapa de recolección de información, basados en el alcance y el objeto de la evaluación se procede a recolectar información sobre el sistema de control objeto de la evaluación, usando técnicas de recolección pasivas y activas según se haya pactado con el cliente, esta etapa produce un entregable para la etapa de análisis de vulnerabilidades, en la cual el evaluador realiza un análisis de vulnerabilidades segmentando el sistema de

control industrial en dos dominios, el dominio TI, donde se encuentran todos los equipos, dispositivos, servicios y personal que no forma parte del proceso industrial, y el dominio ICS donde se analizan las vulnerabilidades de todos los equipos, dispositivos, servicios y personal que forma parte activa del proceso industrial, este proceso desarrolla un entregable que se usa en la siguiente como complemento para verificar los controles implementados, con esta información se produce un entregable para la siguiente etapa, en la cual se realiza el informe de resultados de la evaluación y que contiene el objetivo de la evaluación de seguridad, el tiempo que tomó la evaluación, el alcance y las limitaciones pactadas, los activos objeto de la evaluación, las amenazas y vulnerabilidades encontradas, los controles hallados y las contramedidas y recomendaciones que se realizan al propietario del sistema.

Conclusiones

- Con la investigación, recolección y análisis de la información relacionada con los sistemas de control industrial se observó que en la actualidad no hay una metodología de evaluación de ciberseguridad que englobe los ICS a un nivel general, a pesar de que se encontraron marcos de trabajo enfocados en la implementación segura de los ICS y una metodología de pruebas de penetración dirigida a los sistemas de generación de energía eléctrica y SmartGrid (NESCOR).

- Durante el desarrollo del trabajo de grado se encuentra que a pesar de la amplia adopción de dispositivos TI en los sistemas de control industrial, los ICS tienen varias características que los diferencian de la postura de seguridad de los sistemas TI, mientras para estos lo importante es la confidencialidad, integridad y disponibilidad de los datos, para los ICS lo importante es la disponibilidad y seguridad del proceso industrial, esto hace que cosas como la integridad y la confidencialidad pasen a un segundo plano cuando de evaluar la seguridad de los ICS se trata.

- En el proceso de identificación de las amenazas y vulnerabilidades en los sistemas de control industrial se observa que, al llegar a materializarse alguna vulnerabilidad en un ICS, y dependiendo de su impacto, las consecuencias físicas, ambientales, en vidas humanas pueden ser muy importantes y pueden llegar a provocar un gran impacto en la seguridad y la economía de una nación.

- Se encuentra que a pesar de que la convergencia de tecnologías de la información y tecnología operativa en los sistemas de control industrial brinda a las empresas una mayor integración y visibilidad de los activos críticos, la logística y los procesos operativos, existen diferencias significativas entre una evaluación de ciberseguridad en ICS y un sistema TI, por ello se aconseja en la metodología de evaluación cuando se analizan las vulnerabilidades, aprovechar la información recolectada sobre el objetivo para segmentar sistema de control industrial en dos dominios, el dominio ICS y el dominio TI.

Recomendaciones

- Antes de realizar la evaluación de seguridad se aconseja realizar una planeación bien estructurada y en conjunto con todos los involucrados en el sistema de control industrial con el fin de afectar en lo más mínimo los procesos críticos que se realizan por parte del ICS y firmar un documento que evidencie el alcance y los términos en los que se desarrollará la evaluación de seguridad.

- Se recomienda al evaluador no superar el alcance pactado con la organización propietaria del sistema de control a evaluar sin autorización de esta, puesto que esto puede tener serias consecuencias penales.

- La recolección de información referente a los activos de los sistemas de control industrial debe realizarse teniendo en cuenta el entregable de la primera etapa, en el cual se indica el objetivo de la evaluación, su alcance, las limitaciones y el objeto a evaluar, así como las herramientas que se utilizarán y el tipo de evaluación a desarrollar. Realizar acciones por fuera de lo pactado puede significar enfrentar multas o consecuencias penales por incumplimiento del contrato y pueden afectar el rendimiento del sistema de control industrial.

- Se recomienda segmentar el sistema de control de acuerdo con los dominios de TI y de ICS, esto con el fin de realizar un análisis enfocado en la postura de seguridad de cada entorno.

- No se aconseja realizar un análisis de vulnerabilidades activo sobre un sistema de control industrial en producción por se pueden producir degradaciones del rendimiento del proceso productivo que pueden producir comportamientos erráticos del ICS y pueden llegar incluso a parar la producción

- No se aconseja la explotación de las vulnerabilidades en los sistemas de control industrial, esto debido a que son sistemas que manejan procesos muy críticos que no se pueden afectar en su disponibilidad ni productividad. Si es necesario explotar alguna vulnerabilidad, es importante respaldar la configuración del sistema y contar en todo momento con la autorización escrita del propietario del sistema de control industrial.

- Es importante evidenciar todas las actividades que se realicen sobre el sistema de control industrial, al igual que las respuestas que se obtengan de este, con el fin de plasmar esta información en el reporte de resultados que se entrega a los directivos, responsables administrativos y técnicos