UAI

Universidad Abierta Interamericana

Programa de Ciberseguridad Orientado a I.IoT

Alumno: Hernán Costante

Tutor Técnico: Lic. Jorge Kamlofsky

Profesora de Trabajo Final: Dra. Marcela Samela

Trabajo Final de Carrera presentado para obtener el título de Licenciatura en Gestión de Tecnología informática

(Marzo, 2022)

Resumen

En el presente trabajo se realizó una investigación sobre los aspectos de ciberseguridad de la Industria 4.0, de la Tecnología Operacional y de Internet de las Cosas Industriales. El alcance de la misma abarcó: el crecimiento, la evolución, los riesgos y las amenazas que se encuentran presentes en los últimos años y en la actualidad, como también las contramedidas de ciberseguridad propuestas en investigaciones de otros autores.

A continuación se abordaron los problemas de ciberseguridad causados por la convergencia entre las Tecnologías de la Información y Operacional, que si bien es un aspecto ya presente hace años, se ha profundizado notablemente al introducir en ella los dispositivos conocidos como I.IoT.

Por último se propuso un Programa de Ciberseguridad orientado a I.IoT para el abordaje de esta disciplina de forma sistémica y holística. A través de este programa, diseñado en etapas, una organización puede aplicar las contramedidas previamente identificadas y establecer procesos evolutivos de mejora continua. El mismo incluye aspectos técnicos y de gestión para la reducción de los riesgos y la contención de las amenazas que presentan la convergencia entre las Tecnologías de la Información y Operacional con el arribo de I.IoT.

Palabras clave: ciberseguridad, internet de las cosas industriales, tecnología operacional, industria 4.0

Abstract

In this final degree project, an investigation was carried out on the cybersecurity aspects of Industry 4.0, Operational Technology and the Internet of Industrial Things. Its scope covered: growth, evolution, risks and threats that are present in recent years and today, as well as cybersecurity countermeasures proposed in research by other authors.

Later, in this research, the cybersecurity problems caused by the convergence between Information and Operational Technologies were addressed, which, although it is an aspect that has been present for years, has been considerably deepened by the introduction of devices known as I.IoT.

Finally, a Cybersecurity Program oriented to I.IoT was proposed to approach this discipline in a systematic and holistic way. Through this program, designed in stages, an organization can apply previously identified countermeasures and establish evolutionary processes for continuous improvement. It includes technical and management aspects for the reduction of risks and the containment of threats presented by the convergence between Information and Operational Technologies with the arrival of I.IoT.

Keywords: cyber security, industrial internet of things, operational technology, industry 4.0

Dedicatoria

A mi querida esposa Elisa y a mi hija Felicitas que sacrificaron valioso tiempo en familia y por su apoyo incondicional para poder lograr mis objetivos y sueños. Ellas son el combustible de mi pasión.

A mi mamá Liliana por enseñarme el valor del esfuerzo, a nunca rendirme, a que no importa las circunstancias o los obstáculos que la vida nos presente, y que siempre se puede salir adelante.

A los docentes que invirtieron incontables horas y largas cursadas nocturnas en mi formación como profesional durante mi carrera de grado en la Universidad Abierta Interamericana.

Reconocimientos

Al Licenciado Jorge Kamlofsky por haberme aceptado en su equipo de investigación, por su tutoría, guía y asesoramiento durante la aventura de realizar un trabajo final de carrera.

A la titular de cátedra de Trabajo Final de Carrera Doctora Marcela Samela, por su sapiencia y paciencia para enseñarnos los fundamentos teóricos para realizar este trabajo y por su apoyo para lograr finalizarlo.

A los docentes de la Universidad Abierta Interamericana que aportaron los granos de arena que establecieron los cimientos de los conocimientos utilizados en este trabajo de investigación.

A mis compañeros del grupo de investigación Federico Devatanian Ocampo, Facundo Bernardi, Leonardo Scussolin y Dario Zatti, con quienes hemos tenido interminables debates e intercambios de ideas para poder resolver todos los problemas con los que nos hemos encontrado.

A los compañeros Oscar Romero y Federico Romero que aportaron un gran valor con su experiencia vivida sobre la aprobación de un trabajo final de carrera, un proceso desconocido para mi y para muchos otros alumnos.

A mi familia y amigos, a los cuales les he suspendido o postergado gran cantidad de planes en pos de cursar materias, rendir exámenes y trabajar en este documento.

Índice General

Resumen 1

Abstract 2

Dedicatoria 3

Reconocimientos 4

Índice General 5

Índice de Figuras 8

Índice de Tablas 9

Capítulo 1 - Introducción 10

- **Presentación del problema** 10
- **Hipótesis** 11
- **Objetivo de este Trabajo** 11
- **Objetivos Particulares** 11
- **Enfoque Metodológico** 12
- **Contribuciones Principales** 12
- **Estructura General del Trabajo** 13

Capítulo 2 - Marco Teórico 14

- **Historia de los Sistemas Industriales** 14
  - **Automatización Industrial de la Tercer Era (Industria 3.0)** 16
  - **Cuarta Revolución Industrial (Industria 4.0)** 17
  - **Blockchain (Industria 4.0)** 18
  - **Inteligencia Artificial (Industria 4.0)** 19
  - **Realidad Aumentada y Virtual (Industria 4.0)** 21
  - **Impresión 3D (Industria 4.0)** 22
  - **5G (Industria 4.0)** 23
  - **Internet of Things - IoT (Industria 4.0)** 24
- **Tecnología Operacional (OT)** 26
  - **Convergencia IT-OT** 27
  - **Sistemas de Control Industrial (ICS)** 28

Control de Supervisión y Adquisición de Datos (SCADA) 28
Sistema de Control Distribuido (DCS) 29
Interfaz Hombre-Máquina (HMI) 30
Controlador Lógico Programable (PLC) 30
Comunicaciones entre los Sistemas de Control Industrial (ICS) 30
Industrial Internet of Things (I.IoT) 32
Ciberseguridad 32
Confidencialidad, integridad y disponibilidad 32
Ciberseguridad 35
Ciberseguridad en OT 37
Estándar de ciberseguridad OT IEC 62443 / ISA 99 38
Marco de ciberseguridad de NIST (NIST CSF) 39
Ciberseguridad en la convergencia IT y OT 39
Ciberataques a I.IoT y sus contramedidas 47
Marco de trabajo de Seguridad de I.IoT (Industry IoT Consortium) 57
Modelo de Madurez de Seguridad de I.IoT (Industry IoT Consortium) 59
Capítulo 3 - Desarrollo Técnico 62
Introducción 62
Programa de Ciberseguridad orientado a I.IoT 62
Gobierno de la Ciberseguridad 63
Estrategia y Gobierno de la Ciberseguridad 63
Modelado de Amenazas y Evaluación de Riesgos 66
Cadena de Suministro y Gestión de Dependencias Externas 69
Habilitación de la Ciberseguridad 73
Gestión de Identidades y Accesos 73
Gestión de Activos 75
Protección de Datos 77
Endurecimiento de la Ciberseguridad 79
Gestión de las Vulnerabilidades y Parches 80

Concientización Situacional 82

Respuesta a Eventos e Incidentes, Continuidad de las Operaciones 86

Capítulo 4 - Conclusiones 90

Capítulo 5 - Líneas Futuras de Investigación 91

Acrónimos 92

Referencias 94

Índice de Figuras

Figura 1: Dominios y subdominios del Programa de Ciberseguridad orientado a I.IoT 11

Figura 2: Las cuatro etapas de la Revolución Industrial 16

Figura 3: Ejemplo de un pantalla de video mixta una implementación industrial de realidad aumentada 22

Figura 4: ¿Cómo 5G es diferente? 23

Figura 5: Tecnologías IoT 25

Figura 6: Convergencia IT/OT 27

Figura 7: ¿Que es un Sistema de Control Industrial? 28

Figura 8: Ataque MITM: secuestro de la comunicación IEC 61850-90-5 38

Figura 9: Las ciberamenazas que pueden derribar infraestructuras críticas Convergencia accidental 40

Figura 10: Las ciberamenazas que pueden derribar infraestructuras críticas: Sin visibilidad de las redes OT 41

Figura 11: Las ciberamenazas que pueden derribar infraestructuras críticas: Equipos obsoletos 42

Figura 12: Las ciberamenazas que pueden derribar infraestructuras críticas: Controladores inseguros 43

Figura 13: Las ciberamenazas que pueden derribar infraestructuras críticas: Empleados descontentos y negligentes 44

Figura 14: Arquitectura de red segura recomendada 46

Figura 15: Arquitectura en capas de I.IoT y posibles ataques 48

Figura 16: Taxonomía de Ataques de Ciberseguridad en I.IoT 56

Figura 17: Bloques de construcción funcionales del marco de seguridad 58

Figura 18: Proceso de Modelo de Madurez de Seguridad 61

Figura 19: Ciclo de Mejora de Modelo de Madurez de Seguridad 61

Índice de Tablas

***Tabla 1*: Los cuatro principios de diseño fundamentales de la Industria 4.0 17**

***Tabla 2*: Los protocolos de los sistemas de control industrial más conocidos 31**

***Tabla 3*: Categorías de la Ciberseguridad 35**

***Tabla 4*: Ciberataques a I.IoT y sus contramedidas 50**

***Tabla 5*: Gestión del Programa de Ciberseguridad 64**

***Tabla 6*: Gestión del Cumplimiento 65**

***Tabla 7*: Modelado de Amenazas 67**

***Tabla 8*: Actitud de Riesgo 68**

***Tabla 9*: Gestión de la Cadena de Suministro de Productos 69**

***Tabla 10*: Gestión de los Servicios y Dependencias de Terceros 71**

***Tabla 11*: Establecer y Gestionar Identidades 73**

***Tabla 12*: Control de Acceso 74**

***Tabla 13*: Gestión de Activos, Cambios y Configuraciones 75**

***Tabla 14*: Protección Física 77**

***Tabla 15*: Modelo de Ciberseguridad y Política de Protección de Datos 78**

***Tabla 16*: Implementación de los Controles de Protección de Datos 79**

***Tabla 17*: Evaluación de Vulnerabilidades 80**

***Tabla 18*: Gestión de Actualizaciones de Seguridad 81**

***Tabla 19*: Monitoreo de Seguridad 83**

***Tabla 20*: Concientización de la Situación e Intercambio de Información 84**

***Tabla 21*: Plan de Detección de Eventos y Respuesta ante Incidentes 86**

***Tabla 22*: Remediación, recuperación y Continuidad de Operaciones 88**

Capítulo 1 - Introducción

1.1 Presentación del problema

La industria de los dispositivos conocidos como Internet de las Cosas Industriales (I.IoT, del inglés Industrial Internet of Things), se encuentra en desarrollo desde hace ya cinco años[1] y está en pleno crecimiento. Según Gartner, en su análisis de mercado donde presenta el nivel de madurez de la industria en aspectos de negocios, estima que el 15% de las industrias ya cuentan con esta tecnología implementada en el año 2019 y se proyecta un crecimiento del 30% para el año 2030 (Gartner, 2019). Es decir, se estima un crecimiento del mercado de un 100% en apenas cuatro años, donde habrá cerca de 27 mil millones de dispositivos I.IoT conectados, con negocios estimados de USD 310 mil millones de dólares (T4, 2020).

Un crecimiento de tal magnitud trae consigo una gran cantidad de desafíos. En los entornos industriales la tecnología utilizada se encontraba aislada de otros sistemas informáticos y aún más de Internet. Ahora los dispositivos I.IoT incrementan en el ecosistema de la Industria 4.0 y la Tecnología Operacional (OT, del inglés Operational Technology) la superficie disponible para ataques informáticos, aumentando también los riesgos a los que las mismas se exponen.

En este contexto, estos sistemas se encuentran expuestos a Internet por primera vez en años, o tal vez décadas. Dado que la probabilidad de que alguien pueda encontrarlos en Internet es muy grande, pudiendo aprovechar sus debilidades, es necesario llevar adelante evaluaciones y estimaciones de ciberseguridad y riesgos informáticos con el fin de identificar las posibles amenazas y aplicar contramedidas. Esta tarea no es sencilla sin un marco de referencia.

Esto nos lleva a la siguiente pregunta: ¿Cómo es posible establecer un Programa de Ciberseguridad orientado a I.IoT? El cual cubra no sólo aspectos técnicos como contramedidas a implementar, sino también aspectos de gestión, procesos y operaciones. Un programa que esté diseñado para proteger a la infraestructura OT, reduciendo los riesgos y la probabilidad de que un ataque informático sea exitoso, y que puede ser sostenible en el tiempo.

En este trabajo se pretende establecer dicho programa basado en la investigación llevada a cabo.

[1] La idea de I.IoT fue concebida en 2016 (Desjardins, Jeff (2018) Timeline: The History of the Industrial Internet of Things.)

1.2 Hipótesis

Lo que se busca demostrar es que, mediante la implementación de un programa de ciberseguridad, que incorpore el tratamiento de los riesgos y amenazas de I.IoT y la convergencia de entornos IT y OT, es posible disminuir de forma progresiva el riesgo de ciberseguridad y proteger de sus principales amenazas a las organizaciones que adopten estas tecnologías.

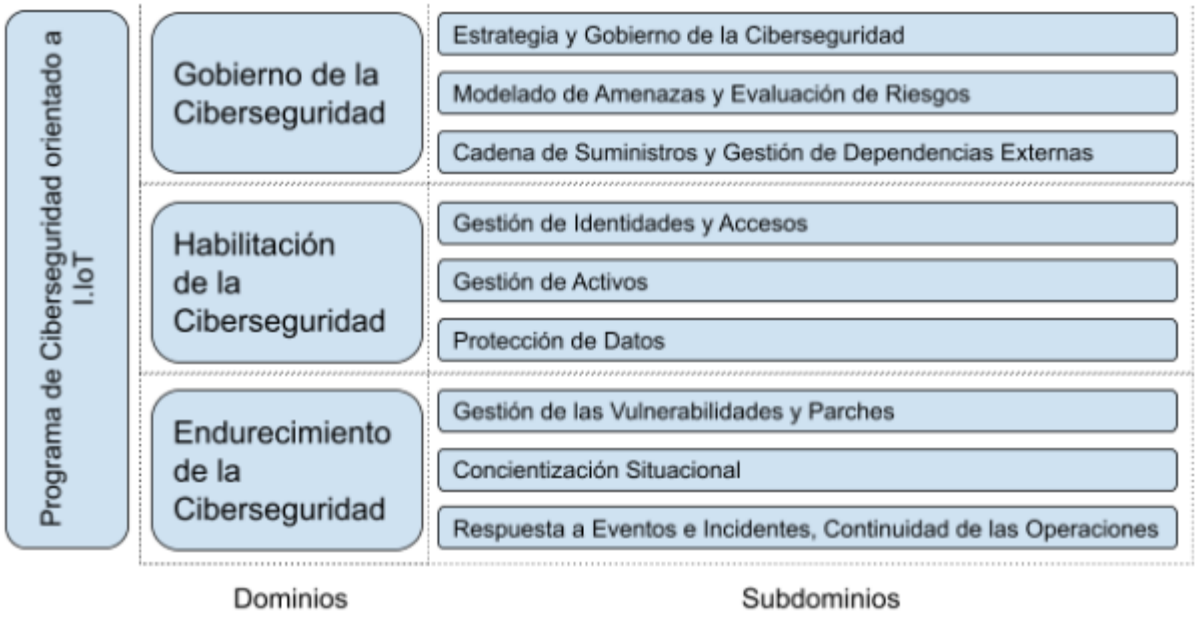
1.3 Objetivo de este Trabajo

El objetivo general de este trabajo es desarrollar un programa de ciberseguridad orientado a I.IoT que cubra aspectos generales y particulares de gestión de la ciberseguridad, modelado de amenazas, análisis de riesgos, gestión de accesos y protección de los datos, entre otros. La finalidad de este es lograr una reducción de riesgos y con capacidad de ser adaptado a las diferentes organizaciones.

Este programa está organizado en tres dominios, cada uno de ellos dividido en tres subdominios. En la Figura 1 se puede observar dicha organización.

Figura 1

Dominios y subdominios del Programa de Ciberseguridad orientado a I.IoT



Finalmente, los subdominios estarán compuestos por dos procesos definidos en cuatro etapas cada uno, con el objetivo de ir evolucionando en el tiempo.

1.4 Objetivos Particulares

Para poder lograr el objetivo general se plantean los siguientes objetivos particulares:

- Identificar las principales amenazas y riesgos de la industria I.IoT, OT y la convergencia IT-OT
- Identificar cuales son las contramedidas de ciberseguridad recomendadas por la industria I.IoT y OT.
- Identificar cuales son las herramientas y marcos de trabajo de ciberseguridad utilizados actualmente en las industrias I.IoT y OT.
- Establecer cuáles son los aspectos claves de un programa de ciberseguridad aplicable a I.IoT.

1.5 Enfoque Metodológico

El enfoque metodológico utilizado durante la investigación de este trabajo es del tipo cualitativo. Se comenzó realizando la lectura y análisis de los aspectos relacionados a Internet de las Cosas Industriales, como ser: la historia de los sistemas industriales, la tecnología clave de la industria 4.0 e internet de las cosas industriales, considerando también aspectos, estándares y marcos de trabajo de ciberseguridad.

A medida que se realizó la investigación, se fue profundizando en estos aspectos y se fue logrando el entendimiento del contexto y la tecnología aplicada, logrando comprender las conclusiones de las investigaciones de otros autores sobre las amenazas y riesgos de la tecnología I.IoT y la convergencia IT-OT.

Luego se observaron y analizaron las cualidades de los hallazgos de los otros investigadores, poniéndolos en el contexto de las amenazas y riesgos de los últimos años y, finalmente, se los contrastó con los estándares y marcos de trabajo de ciberseguridad. Con toda esta información y datos recolectados se sacaron conclusiones y se determinó cual era el enfoque más apropiado para lograr el objetivo de esta investigación.

Finalmente se realizó el desarrollo técnico, el cual consistió en un programa en etapas de ciberseguridad para internet de las cosas industriales, con la intención de lograr una verificación empírica sobre de la hipótesis.

1.6 Contribuciones Principales

Esta investigación tiene como fin poder contribuir y ayudar a cualquier organización en la creación de la base de un programa de ciberseguridad aplicable a I.IoT, el cual puedan adoptar o adaptar a su actual programa, en caso de disponer de uno.

Este trabajo de investigación aporta al proyecto "Ciberseguridad en Redes Industriales" radicado en el CAETI[2] y dirigido por Jorge Kamlofsky.

1.7 Estructura General del Trabajo

El presente trabajo cuenta con 5 capítulos en los que se desarrollan los diferentes conceptos y análisis, el desarrollo técnico, las conclusiones, líneas futuras de investigación y, finalmente, los acrónimos y referencias.

- **Capítulo 1: Introducción.** En este capítulo se desarrollan los fundamentos que sientan las bases para el desarrollo del trabajo final de carrera, se propone la hipótesis y se plantean los objetivos.
- **Capítulo 2: Marco Teórico.** En este capítulo se propone una explicación conceptual de los términos en los que se basa el tema, los describe, compara y propone técnicas que se ejecutan a lo largo del trabajo, incluyendo otros trabajos de investigación relacionados.
- **Capítulo 3: Desarrollo Técnico.** En este capítulo se elabora la propuesta del Programa de Ciberseguridad orientado a I.IoT, en sus diferentes dominios, subdominios y procesos, que son las medidas para la reducción de riesgos con la capacidad de mantener o mejorar su implementación en el tiempo.
- **Capítulo 4: Conclusiones.** En este capítulo se detallan las conclusiones y sugerencias, basadas en la investigación elaborada en el Capítulo 2 y en el desarrollo técnico del Capítulo 3.
- **Capítulo 5: Líneas Futuras de Investigación.** Este capítulo describe las posibles líneas de investigación que pudieran continuar el trabajo de investigación presentado.
- **Acrónimos:** Lista ordenada alfabéticamente de acrónimos utilizados a lo largo de todo el trabajo con su abreviación.
- **Referencias:** Listado ordenado alfabéticamente de referencias y bibliografías utilizadas a lo largo de todo el trabajo.

[2] CAETI: Centro de Altos Estudios en Tecnología Informática. http://caeti.uai.edu.ar/

Capítulo 2 - Marco Teórico

2.1 Historia de los Sistemas Industriales

La necesidad de producir bienes al menor costo posible (buscando la eficiencia de los recursos) se remonta a los inicios de la humanidad. Es importante remarcar que cada producto fabricado, ya sea por un individuo o un grupo de ellos, puede ser identificado con un proceso de fabricación fundamental. Durante mucho tiempo el ser humano ha logrado comenzar a dominar estos procesos para fabricar objetos para su propio uso, o con fines comerciales, en talleres muy elementales utilizando instrumentos rudimentarios (Gomes da Costa et al., 2021, p. 61).

En Inglaterra, durante el siglo XVIII, más exactamente durante las década de 1760 sucedió el primer cambio importante en este ámbito. Se comenzó con los primeros procesos industrializados con máquinas para la fabricación de ciertos elementos reemplazando las confecciones artesanales o puramente manuales dando inicio a la Primera Revolución Industrial, lo que hoy se denomina Industria 1.0. Luego esto comenzó a extenderse a los Estados Unidos a finales del siglo y produjo el paso de las economías de estos países, las cuales se basaban en los aspectos agrarios y artesanales, o unas economías con mayor industrialización y procesos llevados a cabo por máquinas. Las industrias que mayor impacto tuvieron fueron las relacionadas a la minería, textil, vidrio y la agroindustria (Gomes da Costa et al., 2021, p. 61).

Varias industrias se vieron afectadas por la drástica reducción del costo de los materiales y del tiempo de producción. En el caso de la industria textil, previo a este periodo, la fabricación se realizaba mayormente en las casas de los trabajadores y los comerciantes facilitaban los equipos y la materia prima necesarios. Bajo este esquema los trabajadores eran los que definían los horarios de trabajo, lo que hacía complejo el control y regulación. Inventos como la máquina de vapor, la rueda de hilar y la rueda de agua cambiaron la cara de la manufactura y marcaron el camino hacia una innovación que está presente en nuestros días (Gomes da Costa et al., 2021, p. 62).

La demanda era mayor que la oferta, provocando fuerte presión sobre la clase trabajadora más baja. Hasta 1833, casi no existían estándares para los trabajadores, lo que significaba largas jornadas y condiciones de trabajo peligrosas, especialmente para los niños. Esto condujo a la Ley de Fábricas de 1833, que impuso restricciones a las horas de trabajo de los niños y estableció normas para proteger a los trabajadores (Gomes da Costa et al., 2021, p. 62).

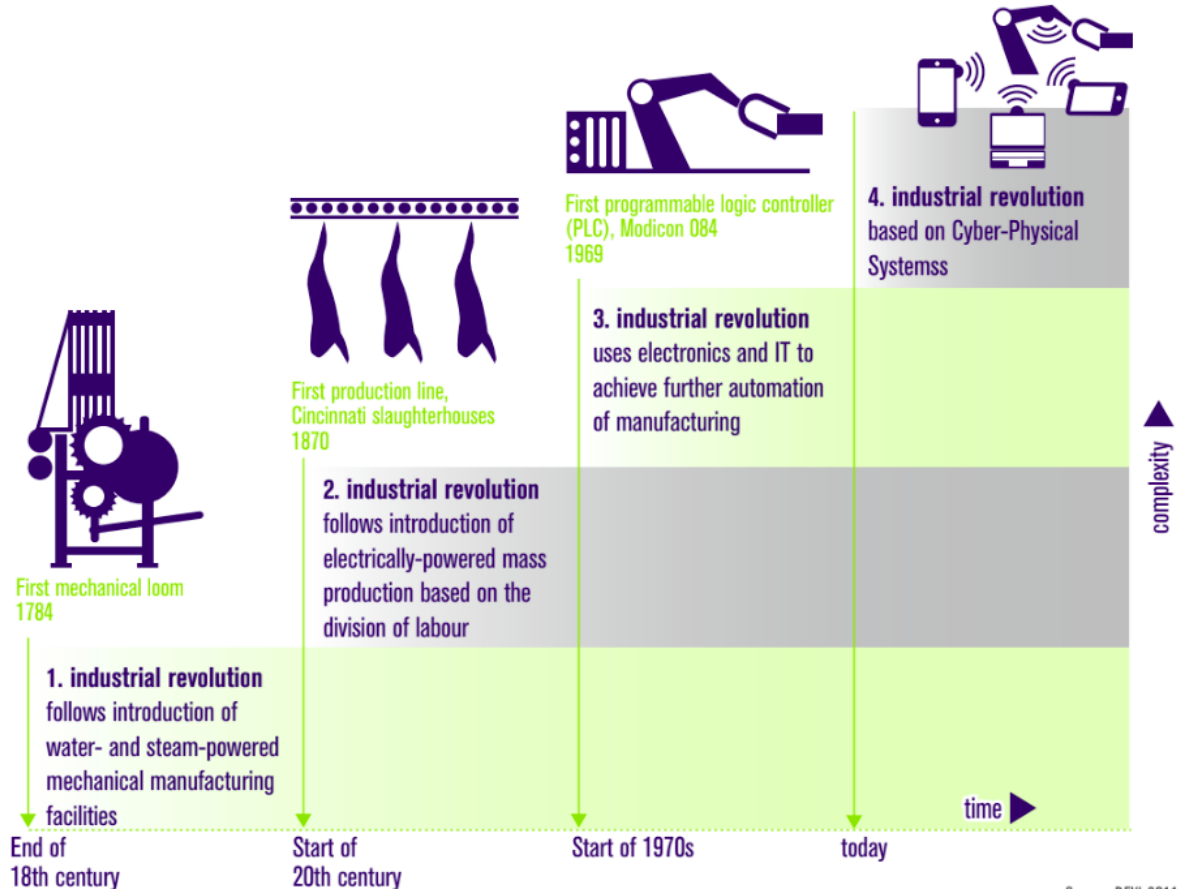
El siguiente cambio en la industrialización fue en el período entre 1871 y 1914, conocido como la Segunda Revolución Industrial (Industria 2.0), como resultado de las extensas red de ferrocarril y de telegrafía, que habilitaron a una más rápida transferencia de personas y comunicación de ideas. La introducción de la electricidad permitió a las fábricas desarrollar líneas de producción modernas. De hecho, la primera línea de montaje fue patentada en 1901 por Ransom E. Olds, productor de automóviles Oldsmobile. Su método permitió a su empresa producir veinte unidades por día, lo que finalmente aumentó su producción en un 500% en un año. Como efecto, Oldsmobile estaba creando más vehículos, permitiendo una disminución drástica de los precios al mismo tiempo. El método utilizado por Olds terminó sirviendo de modelo a Henry Ford, que creó su propio sistema. A Ford se le atribuye ahora el mérito de ser el verdadero padre de la línea de montaje y de la fabricación en masa de automóviles (Gomes da Costa et al., 2021, p. 62).

Si bien esta segunda revolución generó muchos beneficios por el crecimiento económico y una mayor productividad por la introducción de las máquinas, su contracara se presenta en el gran desempleo de los trabajadores que no pudieron reconvertirse a las nuevas formas de trabajo (Gomes da Costa et al., 2021, p. 62).

Como se puede observar en la Figura 2, luego de la Primera y Segunda Revolución Industrial siguió la Tercera y Cuarta, que es donde nos encontramos actualmente y es es donde se ubica en el tiempo este trabajo.

Figura 2

Las cuatro etapas de la Revolución Industrial (Wahlster et al., 2021)



2.1.1 Automatización Industrial de la Tercer Era (Industria 3.0)

La Tercera Revolución Industrial (Industria 3.0), que también es conocida como la Revolución Digital, comenzó en los años 70 del siglo XX a través de una incipiente automatización mediante el uso de computadoras y controladores lógicos programables (PLC, del inglés Programmable Logical Controller) (Gomes da Costa et al., 2021, p. 63).

El punto central de esta fase es la producción en masa y el uso generalizado de lógica digital, transistores semiconductor-metal-óxido (MOS, del inglés metal-oxide-semiconductor), chips de circuitos integrados y sus tecnologías derivadas, incluidas computadoras, microprocesadores, teléfonos celulares digitales e Internet. Estas innovaciones tecnológicas han transformado los métodos tradicionales de producción y negocios. Básicamente, se puede decir que esta revolución convirtió a la tecnología que había sido analógica en un formato digital (Gomes da Costa et al., 2021, p. 63).

Es importante mencionar que la Industria 3.0 todavía está presente: la mayoría de las fábricas se encuentran en este nivel de evolución.

2.1.2 Cuarta Revolución Industrial (Industria 4.0)

La Cuarta Revolución Industrial, conocida como Industria 4.0 (Kagermann et al., 2013), es una unión entre activos físicos y tecnologías digitales avanzadas como: Internet de las Cosas (IoT, del inglés Internet of Things), Inteligencia Artificial (AI, del inglés Artificial Intelligence), robots, drones, vehículos autónomos, impresión en tres dimensiones (3D, del inglés 3 Dimensions), computación en la nube y otros, que están interconectados, teniendo la posibilidad de comunicarse, analizar y actuar. Las organizaciones que adoptan la Industria 4.0 son más flexibles, receptivas e inteligentes y, por lo tanto, están más preparadas para tomar decisiones basadas en datos (Gomes da Costa et al., 2021, p. 64).

El origen de esta Cuarta Revolución Industrial, tuvo como centro geográfico la ciudad de Hannover en Alemania, donde en dicha ciudad, en una importante feria que lleva el mismo nombre, en el año 2011. Esto marcó el inicio de un proyecto de alta-tecnología del gobierno de ese país que presentó la Industria 4.0 como un concepto de digitalización de las fábricas (Gomes da Costa et al., 2021, p. 64).

El concepto de Industria 4.0 tiene cuatro principios de diseño fundamentales (Gomes da Costa et al., 2021, p. 64) y se muestran en la Tabla 1.

Tabla 1

Los cuatro principios de diseño fundamentales de la Industria 4.0

Principio	Descripción
Interconexión	Es la capacidad de los sensores, los dispositivos, las máquinas y las personas para conectarse y comunicarse entre sí a través de Internet: IoT o IoP (del inglés Internet of People).
Transparencia de la información	Es la transparencia que ofrece la Industrial 4.0 a los operadores. Información completa para la toma de decisiones.
Asistencia técnica	Es la facilidad tecnológica de los sistemas para ayudar a los humanos en la toma de decisiones, la resolución de problemas y la capacidad de ayudar a los humanos con tareas difíciles o inseguras.
Decisiones descentralizadas	Es la capacidad de los sistemas ciber físicos para tomar decisiones por sí mismos y realizar sus tareas de la manera más autónoma

Principio	Descripción
	posible.

Notas. (Gomes da Costa et al., 2021, p. 64)

Desde 2011, el enfoque de las empresas de tecnología fue incluir las tecnologías más nuevas en sus productos y llevar los principios de la Industria 4.0 a la producción real. Esto también es posible gracias a una evolución de tecnologías sin precedentes, fáciles de adoptar e integrar, lo que reduce el tiempo de creación y lanzamiento de nuevos productos (Gomes da Costa et al., 2021, p. 64).

2.1.3 Blockchain (Industria 4.0)

Blockchain se puede definir como un directorio descentralizado y distribuido que impulsa contratos inteligentes y brinda la oportunidad de ayudar en la trazabilidad, la gestión de registros, la automatización de la cadena de suministro, las aplicaciones de pago y otras transacciones comerciales. Blockchain proporciona un registro casi en tiempo real replicado entre una red de socios comerciales y que no es modificable (Javaid et al., 2021, p. 3).

Las aplicaciones de la tecnología Blockchain están surgiendo en todos los sectores de la sociedad y la industria. Por ejemplo, en el sector financiero, Blockchain puede simplificar los procesos comerciales mientras crea registros seguros y confiables de acuerdos y transacciones. Se ha formado un consorcio global de más de 80 miembros institucionales para desarrollar pruebas de conceptos y prototipos de sistemas financieros que están alterando el sector financiero mediante la ejecución automática de transacciones financieras en tiempo real. Además, en el caso de las cadenas de suministro de alimentos, por ejemplo, un ecosistema habilitado por Blockchain puede facilitar un servicio de extremo a extremo que alivia las interrupciones en la ocurrencia de productos fraudulentos en la cadena de suministro. Al integrar la gestión de la cadena de suministro con un sistema de IoT que admite una comunicación automatizada de máquina a máquina, puede tener lugar una transferencia de valor óptima y segura a lo largo de todo el proceso (Subic et al., 2018).

Para tener éxito en la próxima era industrial, las empresas de fabricación deben definir y dar forma a sus principales impulsores de valor habilitados por las tecnologías digitales. La Industria 4.0 impulsa la eficiencia operativa a través de fábricas inteligentes y cadenas de suministro inteligentes, así como también aumenta las oportunidades a través de la innovación

y las soluciones a medida para aumentar el valor para el cliente. En última instancia, conduce a modelos comerciales y ofertas de servicios completamente nuevos habilitados a través de la digitalización (Subic et al., 2018).

Se está volviendo evidente que Blockchain tiene el potencial de ser más impactante al combinar sistemas cibernéticos y físicos a través de la integración con plataformas tecnológicas de la Industria 4.0, como IoT, robótica, impresión 3D, realidad aumentada y sensores inteligentes. Se están diseñando modelos industriales y comerciales basados en estos servicios de extremo a extremo que están completamente interconectados y son seguros mediante la tecnología Blockchain (Subic et al., 2018).

Según la Universidad Tecnológica de Swinburne (Austria), que colocó a la Industria 4.0 en el centro de su estrategia, la cual llaman “Swinburne Factory of the Future”, y a la cual Siemens ha subvencionado con 135 millones de dólares para la digitalización industrial, tendrá como corazón de la estrategia a la tecnología Blockchain. Esta representa una plataforma de capacidad tecnológica que potencialmente admite todas las aplicaciones de la industria. Las áreas incluyen la cadena de suministro y el comercio en las industrias manufacturera, alimentaria, farmacéutica, sanitaria y creativa. "Distribuyendo la confianza" (del inglés “Distributing Trust”) entre los participantes, Blockchain impulsará modelos comerciales de fabricación completamente nuevos. Las características disruptivas de Blockchain ya se han experimentado y probado en el sector financiero, donde la actividad de los corredores está siendo desafiada por plataformas que pueden verificar la información de forma rápida y segura sin la participación manual. Más allá de los servicios financieros y después de los servicios profesionales (como la propiedad y los servicios legales), Blockchain representa una plataforma de capacidad tecnológica que admite potencialmente todas las aplicaciones de la industria (Subic et al., 2018).

2.1.4 Inteligencia Artificial (Industria 4.0)

La Inteligencia Artificial (AI, del inglés Artificial Intelligence) es una de las tecnologías impulsoras de la Industria 4.0. Según la Comisión Europea, la AI se refiere a “sistemas que muestran un comportamiento inteligente al analizar su entorno y tomar acciones (con cierto grado de autonomía) para lograr objetivos específicos” (European Commission, 2018). Su aplicación en el sector industrial ha dado lugar al concepto de “fabricación inteligente” (Yao et al., 2017, p. 751-760), que, junto con otras tecnologías emergentes de la Industria 4.0, permite operaciones más flexibles y eficientes en la fábrica inteligente. Para lograr una buena

implementación de esta tecnología, también se propone para el marco de AI Industrial, una estructura, metodología y ecosistema claros (Lee et al., 2018, p. 20-23).

Por ejemplo, en la industria de la construcción naval ya existen algunas aplicaciones en términos de diseño de buques para optimizar el rendimiento general (Abramowski, 2013, p. 101-112). Las aplicaciones de la AI están relacionadas principalmente con el desarrollo de otras tecnologías, actuando como habilitador para impulsar el potencial de cada una de las otras tecnologías habilitadoras clave (Gomez et al., 2016). Esto se muestra en la interacción entre la AI y el efecto particular que despliega.

La utilización de la inteligencia artificial está mejorando la forma en que las empresas aplican inteligencia y esto significa una mejora sustancial para la economía alrededor del mundo. En un estudio de IBM titulado "La Carrera Mundial por la AI" (IBM, 2020), se menciona que en España el 82% de las empresas ya está haciendo uso de la inteligencia artificial. Esta tecnología está permitiendo hacer que sus modelos de producción tengan escalabilidad sin detrimento de la calidad en los procesos, algo clave en la competitividad de los mercados.

Las técnicas de inteligencia artificial como el aprendizaje automático (ML, del inglés Machine Learning) y el aprendizaje profundo (DL, del inglés Deep Learning), si se implementan bien, producen efectos muy positivos en el retorno de la inversión (ROI, del inglés Return of Investment) de las organizaciones que lo hacen. El ML mejora enormemente la calidad del producto al generar predictibilidad en los sistemas de mantenimiento de los procesos de producción, reemplazando las inspecciones visuales con robots o cobots (robots colaborativos) que ejecutan controles de calidad de manera infinitamente más precisa y eficiente.

Además, con el aprendizaje automático se pueden crear algoritmos sofisticados que permiten la "fabricación inteligente"; los datos recopilados durante la producción se analizan y los cambios se adaptan automáticamente. El aprendizaje profundo, que es una subdivisión que ha evolucionado a partir del aprendizaje automático, permite crear redes neuronales que que a su vez pueden generar el aprendizaje no supervisado, posicionando la autonomía de estos métodos aún más lejos. Los beneficios clave de estas técnicas de AI son:

- Optimización de producción
- Integración de la cadena de suministro
- Adaptación de la empresa al mercado
- Mejor desarrollo de productos

Sin embargo, la complejidad del uso de la AI en la Cuarta Revolución Industrial implica la colaboración de los fabricantes con los especialistas para lograr las mejores soluciones y que estas puedan adaptarse a las industrias. La construcción de esto tiene costos muy altos y requiere un conocimiento profundo tanto interna como técnicamente (Gomez et al., 2016).

2.1.5 Realidad Aumentada y Virtual (Industria 4.0)

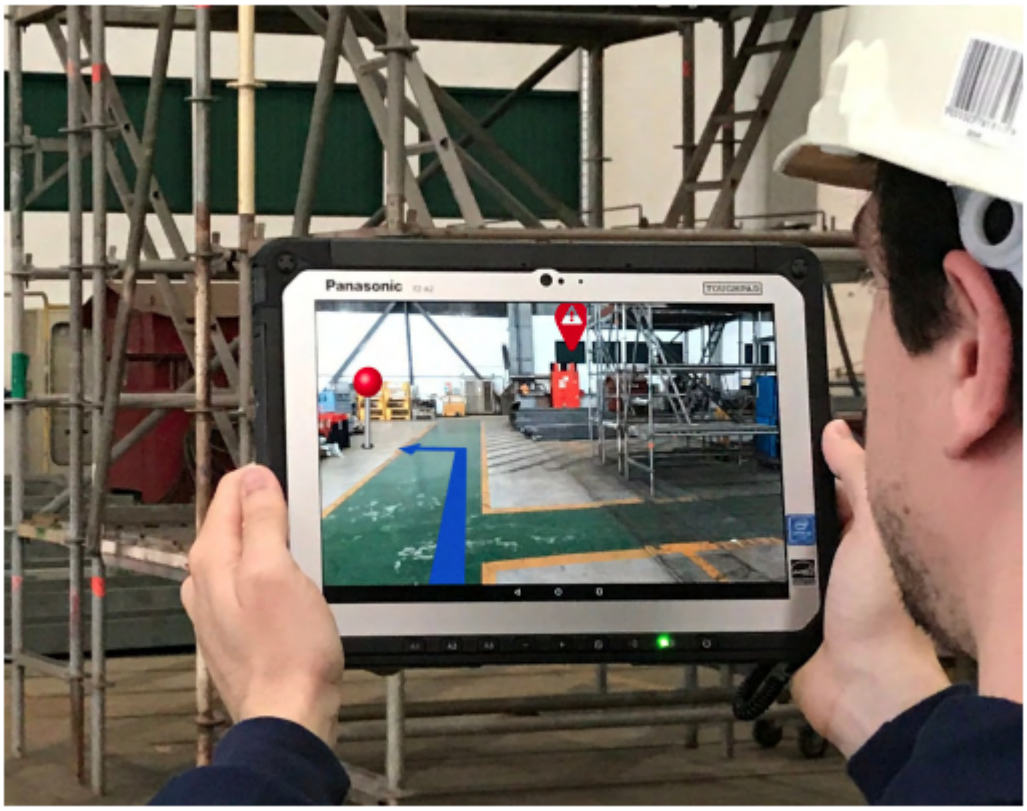
La realidad virtual y aumentada (VAR, del inglés Virtual and Augmented Reality) podría englobarse dentro de las tecnologías de modelado y simulación. Sin embargo, como esta tecnología implica la inmersión humana parcial o completa, además de perseguir un objetivo diferente, el VAR se ha tratado por separado (Mourtzis et al., 2014, p. 213-229).

Por un lado, la realidad virtual implica una inmersión total del ser humano dentro de un mundo virtual utilizando un dispositivo especial conectado con una simulación. En este mundo virtual, el usuario puede interactuar con elementos virtuales para capacitar y mejorar significativamente el conocimiento del operador. También tiene aplicaciones en la prueba de productos y la validación de productos complejos (Roldán et al., 2019, p. 305-316).

Por otro lado, la realidad aumentada converge el mundo real con el virtual a través de un dispositivo, agregando datos del sistema virtual (o gemelo digital), exactamente donde se necesitan. Esta tecnología es útil no solo en los procesos de fabricación sino también en las tareas de mantenimiento. Como se puede observar en la Figura 3 el uso de esta tecnología también ofrece capacidades que pueden ser aplicadas para el aseguramiento del control de calidad, la ubicación de productos y herramientas, gestión de almacenes y soporte para la visualización de áreas ocultas (Fraga-Lamas et al., 2018, p. 1-18), entre otras.

Figura 3

Ejemplo de un pantalla de video mixta una implementación industrial de realidad aumentada (Fraga-Lamas et al., 2018)



2.1.6 Impresión 3D (Industria 4.0)

La impresión 3D es un nuevo proceso de fabricación que también se conoce como fabricación aditiva. Consiste en la fabricación de una pieza añadiendo material capa a capa. Esta tecnología está recibiendo mucha atención en la actualidad y se espera que se convierta en una gran revolución en diferentes sectores industriales. Por ejemplo, en la industria de la construcción naval, hay estudios recientes en los que se utiliza una tecnología de fabricación aditiva basada en polímeros (Moreno Nieto et al., 2018, p. 79-85). Esta tecnología se está utilizando para fabricar piezas grandes no estructurales, lo que reduce los tiempos y costos de fabricación.

Por otro lado, también se está investigando la tecnología de fabricación aditiva por arco de alambre (WAAM, del inglés Wire Arc Additive Manufacturing). En este caso, el polímero es reemplazado por una masa fundida de alambre de metal debido al calor producido por un arco eléctrico (Knezović & Topić, 2018). Esta tecnología tiene el potencial de reemplazar los componentes de los recipientes que aún deben estar hechos de metal, reduciendo los costos de

fabricación. Esta suposición conduce al inevitable rediseño del barco para evaluar qué partes pueden cambiar su tecnología de fabricación. Por lo tanto, está claro que esta tecnología aún necesita otros cambios para tener el impacto que se supone que debe tener.

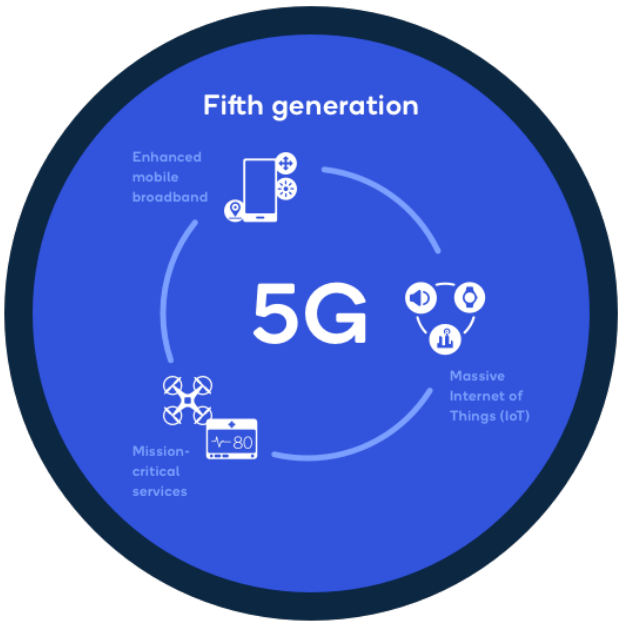
2.1.7 5G (Industria 4.0)

La tecnología de telecomunicaciones de quinta generación (5G, del inglés 5th Generation) es la próxima generación de banda ancha móvil, posterior a la cuarta generación (4G, del inglés 4th Generation). En desarrollo durante casi 10 años, se ha anunciado como el verdadero facilitador de Internet de las cosas, inteligencia artificial, Industria 4.0 y otros. Y la revolución ya ha comenzado dado que países como Estados Unidos, China, Corea del Sur y Reino Unido ya tienen 5G disponible en extensas áreas.

Como se puede observar en la Figura 4, la tecnología 5G utiliza frecuencias de radio más altas para alcanzar velocidades hasta 1.000 veces más rápidas que su predecesor, 4G. Descargar una película de dos horas habría tardado 26 horas en 3G y 6 minutos en 4G, sólo tomará 3.6 segundos en 5G (Iscrupe, 2020). Otra gran diferencia es la cantidad de dispositivos que admite 5G. Las redes 4G actuales admiten alrededor de 4.000 dispositivos por kilómetro cuadrado. En comparación, 5G puede admitir hasta 1 millón (The Medical Futurist, 2019).

Figura 4

¿Cómo 5G es diferente? (Qualcomm, 2021)



Pero quizás la diferencia más significativa con 5G tiene que ver con algo conocido como latencia: el tiempo que lleva obtener una respuesta de la información enviada. Con sus tiempos de latencia significativamente más bajos, la tecnología 5G ayudará a ofrecer redes móviles que nos permitan hacer cosas completamente nuevas, no solo mejorar lo que ya estamos haciendo. Las posibilidades incluyen robots de fábrica avanzados, automóviles autónomos y otras tareas que exigen una respuesta rápida, todas áreas en las que las redes 4G tienen problemas o no pueden funcionar adecuadamente.

La cuarta revolución industrial, Industria 4.0, fue impulsada por una combinación de tecnologías emergentes, como el aprendizaje automático y los dispositivos conectados a IoT. Muchos fabricantes ya están implementando soluciones de Internet de las Cosas para monitorear activos en sus fábricas, mejorar sus salas de control y aumentar su funcionalidad analítica mediante la instalación de sistemas de mantenimiento predictivo. Un estudio estima que el 35% de los fabricantes estadounidenses ya están utilizando datos de sensores inteligentes dentro de sus implementaciones (Ross, 2019).

En la fabricación, a menudo se utilizan numerosas máquinas de uso intensivo de datos en las proximidades. Es por eso que la conectividad 5G es clave. En un mercado que depende de aplicaciones de máquinas con uso intensivo de datos, se requieren velocidades más altas y baja latencia, como la que ofrece 5G, para el uso efectivo de robots automáticos, dispositivos portátiles y cascos de realidad virtual (VR, del inglés Virtual Reality), dando forma al futuro de las fábricas inteligentes. Y lo que es más importante, 5G permite que esto suceda a una escala sin precedentes (Ross, 2019).

2.1.8 Internet of Things - IoT (Industria 4.0)

El concepto de IoT se refiere a la conectividad de cada dispositivo, de forma directa, dentro de una red que es capaz de generar datos a partir de sensores o dispositivos electrónicos integrados, que luego se envían a la nube a través de un sistema de transmisión (Costa et al., 2019, p. 977-994). Como cada "cosa" genera datos, la conexión entre IoT y el análisis de grandes volúmenes de datos (del inglés Big Data) es muy evidente. Esta tecnología también incluye el concepto de sistemas ciber físicos, siendo la puerta de entrada para fusionar el mundo real con el mundo virtual, trayendo objetos físicos a la red.

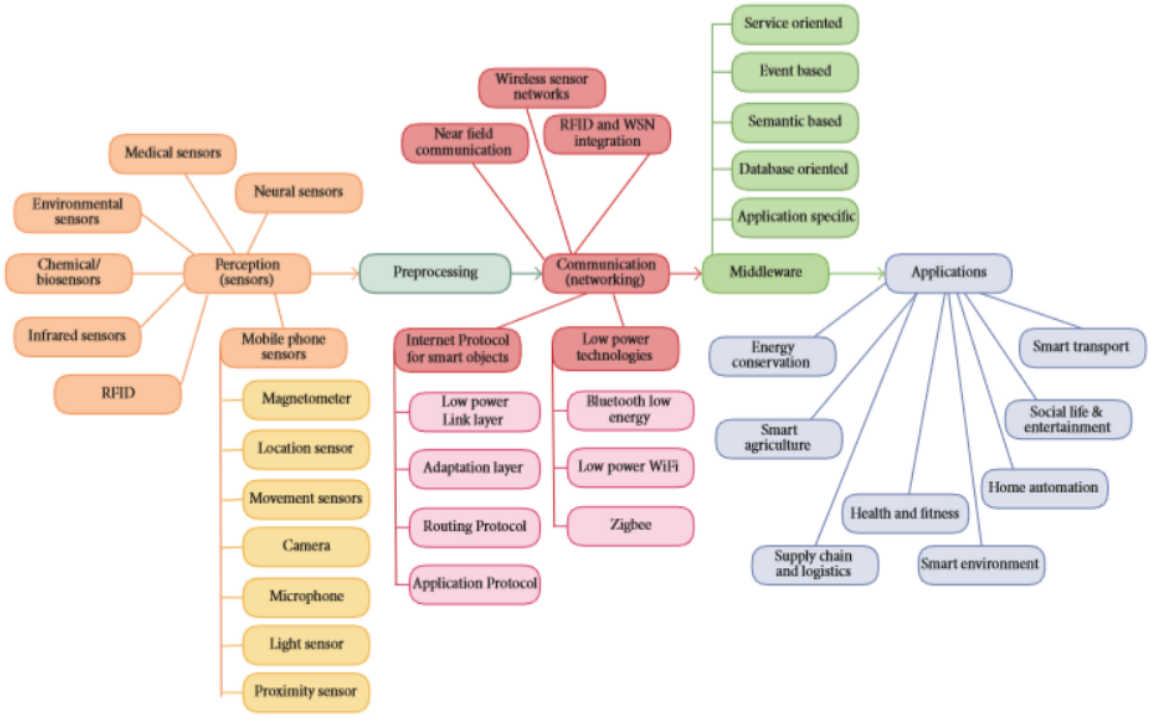
En el sector industrial, la aplicación del IoT se conoce como Internet de las cosas Industriales (I.IoT), y tiene implicaciones y principios particulares que deben cumplirse (ur Rehman et al., 2019, p. 247-259). Estos principios incluyen, entre otros, interoperabilidad, comunicación inalámbrica, descentralización, retroalimentación en tiempo real y

ciberseguridad en todo el sistema para evitar la intromisión de terceros, que puede poner en riesgo todos los datos. De esta forma, la tecnología de ciberseguridad adquiere un papel importante en la protección del entorno industrial.

También se ha llevado a cabo una investigación sobre las implicaciones que esta tecnología puede manejar en proyectos complejos de ingeniería, como las obras de construcción. Esta investigación concluye que es posible crear un "sitio de construcción digital", en el que el IoT juega un papel estratégico ya que se está utilizando en aplicaciones específicas de gran demanda y donde puede ser un generador de valor agregado por sus capacidades. Estas son: de cooperación, comunicación, identificación, medición, actuación, localización, procesamiento de información embebida y las interfaces de usuario. Logrando establecer un sitio de construcción inteligente llamado "smart shipyard" (Lopes de Miranda et al., 2017, p. 567-576). En la Figura 5 se puede observar un diagrama con las tecnologías IoT clasificadas por sus capas arquitectónicas de sensores y aplicaciones.

Figura 5

Tecnologías IoT (Farias Filho, 2012)



2.2 Tecnología Operacional (OT)

La tecnología operacional (OT, del inglés Operational Technology) es una categoría de sistemas de computación y comunicación para administrar, monitorear y controlar operaciones industriales con un enfoque en los dispositivos y procesos físicos (o ciber físicos) que utilizan.

La tecnología OT monitorea y gestiona activos de procesos industriales, equipos industriales o de fabricación. OT existe hace mucho más tiempo que en el ámbito de Tecnología de la información (IT, del inglés Information Technology), más específicamente desde que comenzamos a usar maquinaria y equipos que funcionan con electricidad en fábricas, edificios, sistemas de transporte, la industria de servicios públicos, etc. Sin embargo, el término es más reciente. Esencialmente, OT es el hardware y software que mantiene en funcionamiento cosas, por ejemplo, fábricas, plantas de energía, equipos de instalaciones, etc (Coolfire Solutions, 2019).

A diferencia del mundo de IT, OT es especialmente particular en el aspecto que tanto el hardware como el software están, desde su concepción, diseñados para la ejecución de tareas específicas. Estas tareas pueden ser el control de la temperatura, controlar el movimiento de piezas mecánicas, desencadenar apagados de forma urgente, etc. Comúnmente esto se realiza mediante sistemas cómo: sistemas de control industrial (ICS, del inglés Industrial Control System) y control de supervisión y adquisición de datos (SCADA, del inglés Supervisory Control And Data Acquisition) (i-SCOOP, 2021).

Algo importante para mencionar sobre la tecnología OT es que de forma general fue necesaria la supervisión por parte de las personas. Esto ha sido de esta forma hasta el último periodo, donde se introdujeron los avances de la Industria 4.0, como I.IoT. Antes de esto si era necesario realizar algún cambio, como ser el valor de la temperatura de un horno, o el comportamiento de una máquina, la forma de hacerlo era mediante un cambio físico en el lugar, ya sea activando un pulsador, una palanca o manipulando manualmente algún tipo de control físico (i-SCOOP, 2021).

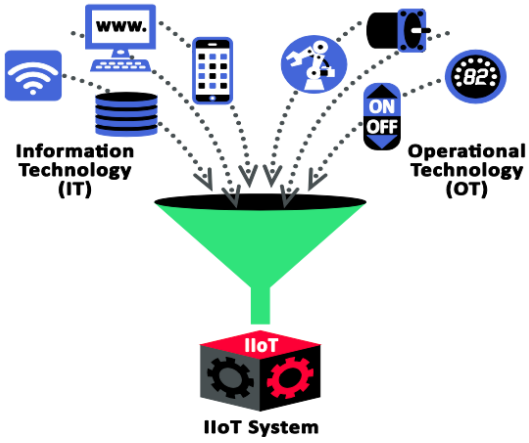
Una evolución importante en OT fue la capacidad de monitorear y controlar dispositivos físicos de forma remota. La inclusión de tecnologías basadas en IT como el big data y el aprendizaje automático (ML) en OT, junto con las evoluciones en la comunicación máquina a máquina (M2M, del inglés Machine to Machine) e Internet de las cosas (IoT), permiten amplias innovaciones con respecto a la gestión de la física, dispositivos en procesos industriales, entre otros en diagnóstico y mantenimiento (diagnóstico remoto, mantenimiento predictivo) e I.IoT (Trend Micro, 2019).

2.2.1 Convergencia IT-OT

Mientras que IT y OT históricamente han constituido aspectos separados de las organizaciones modernas, un fenómeno conocido como convergencia IT-OT está cambiando eso. Debido a que la tecnología I.IoT toma activos que normalmente no están conectados a Internet, como la maquinaria de la línea de ensamblaje, y los pone en línea en Internet, las empresas ahora tienen la oportunidad de ser más eficientes al aplicar la inteligencia de IT a los activos físicos de los sistemas OT. La Figura 6 representa la convergencia IT-OT que estamos mencionando (Coolfire Solutions, 2019).

Figura 6

Convergencia IT/OT (Industrial Internet Consortium, 2016)



Por ejemplo, los controles de temperatura tradicionales vinculados a los sistemas OT generalmente informan las lecturas a través de una lectura de circuito cerrado, lo que permite a los empleados, que se encuentran físicamente allí, ver si los ajustes fueron necesarios en su extremo. Sin embargo, con la tecnología I.IoT, esos sensores de temperatura se pueden conectar a las redes de IT, lo que les permite comunicarse en tiempo real con otros activos en las instalaciones para optimizar los niveles de temperatura automáticamente para obtener el máximo rendimiento (Coolfire Solutions, 2019).

Lo que anteriormente separaba a IT y OT ahora se están desdibujando. Los responsables de la toma de decisiones empresariales deben considerar las implicaciones de ciberseguridad, el cumplimiento y la integración de datos de la convergencia IT-OT. Es muy claro que este cambio brindará una oportunidad casi exponencial para las empresas con la previsión y el conocimiento para que funcione (i-SCOOP, 2019).

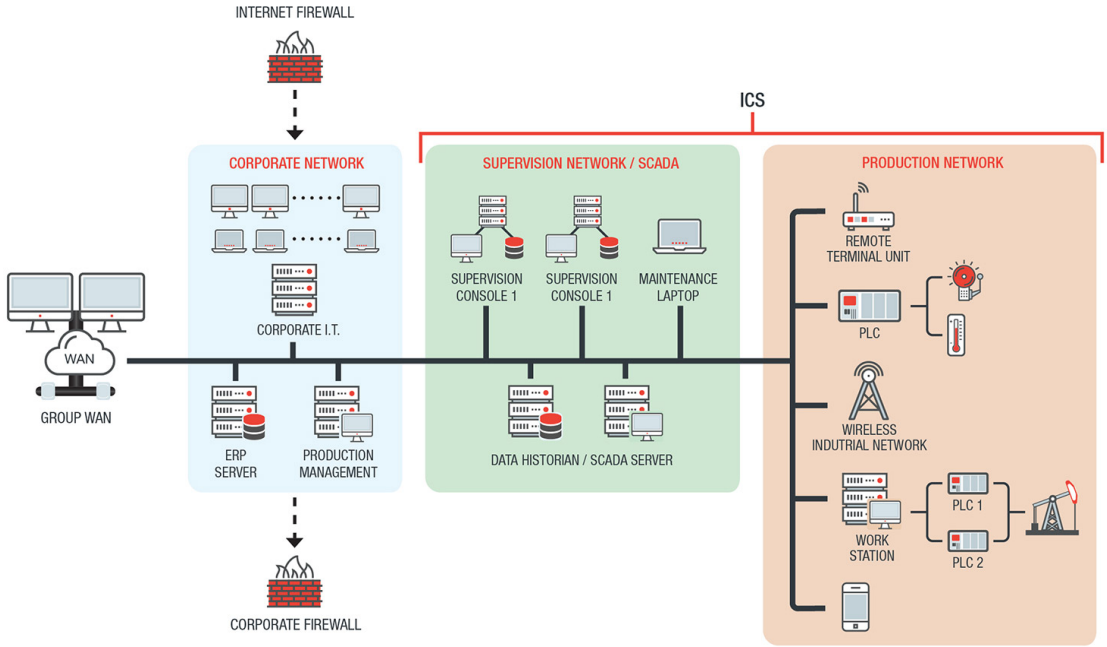
2.2.2 Sistemas de Control Industrial (ICS)

Sistema de control industrial (ICS, del inglés Industrial Control System) es un término colectivo que se utiliza para describir diferentes tipos de sistemas de control e instrumentación asociada, que incluye los dispositivos, sistemas, redes y controles utilizados para operar y / o automatizar procesos industriales. Dependiendo de la industria, cada ICS funciona de manera diferente y está diseñado para administrar las tareas de manera electrónica de manera eficiente. Hoy en día, los dispositivos y protocolos utilizados en un ICS se utilizan en casi todos los sectores industriales e infraestructura crítica, como las industrias de fabricación, transporte, energía y tratamiento de agua (Trend Micro, 2019).

Existen varios tipos de ICS, los más comunes son los sistemas de control de supervisión y adquisición de datos (SCADA) y los sistemas de control distribuido (DCS, del inglés Distributed Control System). Las operaciones locales a menudo están controladas por los llamados dispositivos de campo que reciben comandos de supervisión de estaciones remotas (Trend Micro, 2019). La Figura 7 representa lo que sería un sistema de control industrial tipo.

Figura 7

Qué es un Sistema de Control Industrial? (Trend Micro, 2019)



2.2.3 Control de Supervisión y Adquisición de Datos (SCADA)

Si bien SCADA no es un sistema que pueda proporcionar un control total, sus capacidades se centran en proporcionar control a nivel de supervisión. Los sistemas SCADA

están compuestos por dispositivos generalmente controladores lógicos programables (PLC, del inglés Programmable Logical Controller) u otros módulos de hardware comerciales que se distribuyen en varias ubicaciones. Los sistemas SCADA pueden adquirir y transmitir datos, y están integrados con una interfaz hombre-máquina (HMI, del inglés Human-Machine Interface) que proporciona supervisión y control centralizados para numerosas entradas y salidas de procesos (Trend Micro, 2019).

El propósito principal de usar SCADA es el monitoreo y control de sitios de campo a larga distancia a través de un sistema de control centralizado. En lugar de que los trabajadores tengan que viajar largas distancias para realizar tareas o recopilar datos, un sistema SCADA puede automatizar esta tarea. Los dispositivos de campo controlan las operaciones locales, como la apertura o el cierre de válvulas y disyuntores, la recopilación de datos de los sistemas de sensores y la supervisión del entorno local para detectar condiciones de alarma (Trend Micro, 2019).

Los sistemas SCADA se usan generalmente en industrias que involucran monitoreo y control de tuberías, centros de tratamiento y distribución de agua y transmisión y distribución de energía eléctrica (Trend Micro, 2019).

2.2.4 Sistema de Control Distribuido (DCS)

El Sistema de Control Distribuido (DCS) se utiliza para controlar los sistemas de producción que se encuentran en una ubicación. En un DCS, se envía un punto de ajuste al controlador que es capaz de instruir a las válvulas, o incluso a un actuador, para que operen de tal manera que se mantenga el punto de ajuste deseado. Los datos del campo pueden almacenarse para referencia futura, usarse para un control de proceso simple o incluso usarse para estrategias de control avanzadas con datos de otra parte de la planta (Trend Micro, 2019).

Cada DCS utiliza un bucle de control de supervisión centralizado para gestionar varios controladores o dispositivos locales que forman parte del proceso de producción general. Esto brinda a las industrias la capacidad de acceder rápidamente a los datos de producción y operación, y al utilizar varios dispositivos dentro del proceso de producción, un DCS puede reducir el impacto de una sola falla en el sistema en general (Trend Micro, 2019).

Un DCS también se usa comúnmente en industrias como la fabricación, la generación de energía eléctrica, la fabricación de productos químicos, las refinerías de petróleo y el tratamiento de agua y aguas residuales (Trend Micro, 2019).

2.2.5 Interfaz Hombre-Máquina (HMI)

Una interfaz Hombre Máquina (HMI, del inglés Human-Machine Interface) o aplicación de interfaz gráfica de usuario (GUI, del inglés Graphical User Interface) permite la interacción entre el operador humano y el hardware del controlador. Puede mostrar información de estado y datos históricos recopilados por los dispositivos en el entorno ICS. También se utiliza para monitorear y configurar puntos de ajuste, controlar algoritmos, y ajustar y establecer parámetros en los controladores (Trend Micro, 2019).

2.2.6 Controlador Lógico Programable (PLC)

Este es un tipo de hardware que se utiliza en los sistemas DCS y SCADA como un componente de control de un sistema general. También proporciona una gestión local de los procesos que se ejecutan a través de dispositivos de control de retroalimentación, como sensores y actuadores (Trend Micro, 2019).

En SCADA, un PLC proporciona la misma funcionalidad que las unidades terminales remotas (RTU, del inglés Remote Terminal Unit). En DCS, los PLC se utilizan como controladores locales dentro de un esquema de control de supervisión. Los PLC también se implementan como componentes primarios en configuraciones de sistemas de control más pequeños (Trend Micro, 2019).

2.2.7 Comunicaciones entre los Sistemas de Control Industrial (ICS)

Los dispositivos y módulos de control en los sistemas ICS transmiten información a través de protocolos de comunicación. Hay varios protocolos de comunicación que se utilizan en los entornos ICS. La mayoría de estos protocolos están diseñados para fines específicos, como la automatización de procesos, la automatización de edificios, la automatización de sistemas de energía y muchos más. Estos protocolos también se desarrollaron para garantizar la interoperabilidad entre diferentes fabricantes. Sin embargo, existen algunos protocolos que solo funcionan si los protocolos y el equipo provienen del mismo fabricante (Trend Micro, 2019).

Los protocolos de los sistemas de control industrial más conocidos son los que se describen en la Tabla 2.

Tabla 2

Los protocolos de los sistemas de control industrial más conocidos

Protocolo	Descripción
Bus de campo de proceso (PROFIBUS)	PROFIBUS utiliza comunicaciones RTU a MTU, MTU a MTU y RTU a RTU en el campo. Hay dos variantes disponibles: Profibus DP (periféricos descentralizados), que se usa para operar sensores y actuadores a través de un controlador central, y Profibus PA (automatización de procesos), que se usa para monitorear equipos de medición a través de un sistema de control de procesos.
Protocolo de red distribuida (DNP3)	Este es un protocolo con tres capas que operan en las capas de enlace de datos, aplicación y transporte. Este protocolo es ampliamente utilizado en plantas de tratamiento de agua y / o electricidad y aguas residuales.
Modbus ®	Desde su introducción en 1979, Modbus se considera uno de los protocolos ICS más antiguos. Modbus utiliza comunicaciones en serie con los PLC y ha sido el protocolo de comunicaciones de facto en un entorno ICS. Hay dos tipos de implementaciones de Modbus: Modbus serial, que utiliza el estándar de control de enlace de datos de alto nivel (HDLC) para la transmisión de datos, y Modbus-TCP, que utiliza la pila de protocolos TCP / IP para transmitir datos.
Comunicación de plataforma abierta (OPC)	El OPC es una serie de estándares y especificaciones para comunicaciones industriales. La especificación OPC se basa en tecnologías desarrolladas por Microsoft® para la familia de sistemas operativos Windows® (OLE, COM y DCOM).
Redes de control y automatización de edificios (BACnet)	Este es un protocolo de comunicación diseñado para controlar el control de calefacción, ventilación y aire acondicionado (HVAC); Encendiendo; acceso al edificio; y detección de incendios.
Protocolo industrial	Un CIP es un conjunto de servicios y mensajes de control,

Protocolo	Descripción
común (CIP)	seguridad, sincronización, configuración, información, etc. El CIP se puede integrar en redes Ethernet e Internet, y tiene una serie de adaptaciones que proporcionan intercomunicación e integración para diferentes tipos de redes.
Ethernet para tecnología de automatización de control (EtherCAT)	Protocolo de comunicaciones de código abierto que se utiliza para incorporar Ethernet en entornos industriales. EtherCAT se utiliza en aplicaciones de automatización con ciclos de actualización cortos (≤ 100µs) y con jitter ≤ 1µs.

Nota. (Trend Micro, 2019)

2.2.8 Industrial Internet of Things (I.IoT)

La tecnología I.IoT incorpora el uso de sensores inteligentes para mejorar los procesos industriales y de fabricación. Si bien el término es más reciente, los sensores se han utilizado en fabricación, servicios públicos y otras aplicaciones industriales durante décadas. I.IoT aprovecha la potencia de las máquinas inteligentes y el análisis en tiempo real para aprovechar los datos que las máquinas producen en entornos industriales. I.IoT abarca aplicaciones industriales, que incluyen fabricación, cadena de suministro, robótica, dispositivos médicos y procesos de producción definidos por software. Involucra industrias que van desde la automotriz hasta el petróleo y el gas (Trend Micro, 2019).

El mercado abarca grandes jugadores tradicionales que están creando cada vez más capacidades de integrarse con I.IoT y una larga fila de empresas de nicho y emergentes que ofrecen una amplia gama de soluciones I.IoT. Estas soluciones incluyen el software que permite el análisis de datos y un mejor mantenimiento predictivo, y el hardware que convierte los equipos tradicionales en dispositivos inteligentes conectados y los servicios I.IoT (IIoT World, 2018).

2.3 Ciberseguridad

2.3.1 Confidencialidad, integridad y disponibilidad

La tríada confidencialidad, integridad y disponibilidad se considera el pilar fundamental de la seguridad de la información según el estándar ISO 27001 de la Organización Internacional de Estandarización (International Organization for Standardization, 2013). Cada

control de ciberseguridad y cada vulnerabilidad puede verse medirse con uno o más de estos conceptos clave. Para que un programa de ciberseguridad se considere integral y completo, debe abordar adecuadamente toda la tríada.

La confidencialidad significa que los datos, los objetos y los recursos están protegidos contra la visualización no autorizada y otros accesos. Integridad significa que los datos están protegidos contra cambios no autorizados para garantizar que sean confiables y correctos. Disponibilidad significa que los usuarios autorizados tienen acceso a los sistemas y los recursos que necesitan (Heymsfeld, 2018).

1) Confidencialidad

Las medidas de confidencialidad protegen la información del acceso no autorizado y el uso indebido. La mayoría de los sistemas de información albergan información que tiene cierto grado de sensibilidad. Puede ser información comercial patentada que los competidores podrían utilizar para su beneficio, o información personal sobre los empleados, clientes o clientes de una organización (Heymsfeld, 2018).

La información confidencial a menudo tiene valor y, por lo tanto, los sistemas son objeto de ataques frecuentes a medida que los delincuentes buscan vulnerabilidades para explotar. Los vectores de amenazas incluyen ataques directos, como el robo de contraseñas y la captura de tráfico de red, y más ataques en capas, como la ingeniería social y el phishing. No todas las violaciones de la confidencialidad son intencionales. Algunos tipos de infracciones accidentales comunes incluyen enviar información confidencial por correo electrónico al destinatario incorrecto, publicar datos privados en servidores web públicos y dejar información confidencial en un monitor de computadora desatendido (Heymsfeld, 2018).

Hay muchas contramedidas que implementan las organizaciones para garantizar la confidencialidad. Las contraseñas, las listas de control de acceso y los procedimientos de autenticación utilizan software para controlar el acceso a los recursos. Estos métodos de control de acceso se complementan con el uso de encriptado para proteger la información a la que se puede acceder a pesar de los controles, como los correos electrónicos en tránsito. Las contramedidas de confidencialidad adicionales incluyen soluciones administrativas como políticas y capacitación, así como controles físicos que impiden que las personas accedan a las instalaciones y al equipo (Heymsfeld, 2018).

2) Integridad

Las medidas de integridad protegen la información de modificaciones no autorizadas. Estas medidas brindan garantía de la exactitud e integridad de los datos. La necesidad de proteger la información incluye tanto los datos que se almacenan en los sistemas como los que se transmiten entre sistemas, como el correo electrónico. Para mantener la integridad, no solo es necesario controlar el acceso a nivel del sistema, sino también garantizar que los usuarios del sistema solo puedan alterar la información que están legítimamente autorizados a modificar (Heymsfeld, 2018).

Al igual que con la protección de la confidencialidad, la protección de la integridad de los datos se extiende más allá de las modificaciones intencionales. Las contramedidas de integridad efectivas también deben proteger contra modificaciones no intencionales, como errores del usuario o pérdida de datos como resultado de un mal funcionamiento del sistema (Heymsfeld, 2018).

Hay muchas contramedidas que se pueden implementar para proteger la integridad. El control de acceso y la autenticación rigurosa pueden ayudar a evitar que los usuarios autorizados realicen cambios no autorizados. Las verificaciones hash y las firmas digitales pueden ayudar a garantizar que las transacciones sean auténticas y que los archivos no se hayan modificado ni corrompido. Igualmente importantes para proteger la integridad de los datos son los controles administrativos, como la separación de funciones y la concientización (Heymsfeld, 2018).

3) Disponibilidad

Para que un sistema de información sea útil, debe estar disponible para los usuarios autorizados. Las medidas de disponibilidad protegen el acceso oportuno e ininterrumpido al sistema. Algunas de las amenazas más fundamentales para la disponibilidad no son de naturaleza maliciosa e incluyen fallas de hardware, tiempo de inactividad de software no programado y problemas de ancho de banda de la red. Los ataques malintencionados incluyen varias formas de sabotaje destinadas a causar daño a una organización al denegar a los usuarios el acceso al sistema de información (Heymsfeld, 2018).

La disponibilidad y capacidad de respuesta de un sistema informático es una alta prioridad para muchas empresas. La interrupción del mismo, incluso durante un período breve, puede provocar la pérdida de ingresos, la insatisfacción del cliente y el daño a la reputación. El ataque de denegación de servicio (DoS, del inglés Denial of Service) es un método que los ciberdelincuentes utilizan con frecuencia para interrumpir sistemas informáticos. En un ataque

DoS, los ciberdelincuentes inundan un servidor con solicitudes superfluas, sobrecargando el servidor y degradando el servicio para los usuarios legítimos. A lo largo de los años, los proveedores de servicios han desarrollado sofisticadas contramedidas para detectar y proteger contra los ataques DoS, pero los ciberdelincuentes también continúan ganando en sofisticación y estos ataques siguen siendo una preocupación constante (Heymsfeld, 2018).

Las contramedidas de disponibilidad para proteger la disponibilidad del sistema van tan lejos como las amenazas a la disponibilidad. Los sistemas que tienen un alto requisito de tiempo de actividad continuo deben tener una redundancia de hardware significativa con servidores de respaldo y almacenamiento de datos disponibles de inmediato. Para sistemas empresariales grandes, es común tener sistemas redundantes en ubicaciones físicas separadas. Deben existir herramientas de software para monitorear el rendimiento del sistema y el tráfico de la red. Las contramedidas para protegerse contra los ataques DoS incluyen routers y firewalls de red y de aplicación (Heymsfeld, 2018).

2.3.2 Ciberseguridad

Según la empresa Kaspersky, la cual tiene una gran trayectoria en ciberseguridad, tanto en la investigación como en el desarrollo de productos, define a la misma de la siguiente manera. La ciberseguridad es la disciplina donde se protege de ataques maliciosos la información que es almacenada, procesada o transmitida por sistemas informáticos, que en general están soportados por dispositivos electrónicos como servidores, computadoras, dispositivos de red, dispositivos inteligentes y otros. También se conoce esta disciplina con otros nombres como seguridad de la información o seguridad informática. Estos términos se aplican en una variedad de contextos, desde negocios hasta computación móvil, y se pueden dividir en algunas categorías comunes (Kaspersky, 2021). Estas categorías se pueden observar en la Tabla 3.

Tabla 3

Categorías de la Ciberseguridad

Categoría	Descripción
Ciberseguridad de la Red	"Tiene como objetivo proteger las redes informáticas de posibles intrusos, ya sean atacantes dirigidos, malware o accidentes" (Kaspersky, 2021)

Categoría	Descripción
Ciberseguridad de las Aplicaciones	"Tiene como objetivo que el software desarrollado sea seguro y no contenga vulnerabilidades. Una aplicación comprometida podría proporcionar acceso a los datos sensibles de la compañía y ocasionar pérdidas. La implementación de la ciberseguridad debe comenzarse en la fase de diseño de la aplicación, es decir antes de que se realice implementación" (Kaspersky, 2021)
Seguridad de la Información	"Se centra en proteger la integridad y privacidad de los datos, tanto almacenados como en tránsito" (Kaspersky, 2021)
Ciberseguridad Operativa	"Ésta incluye los procesos y decisiones para manejar y proteger los activos de datos. Los permisos que tienen los usuarios cuando acceden a una red y los procedimientos que determinan cómo y dónde se pueden almacenar o compartir los datos caen bajo este punto" (Kaspersky, 2021)
Recuperación ante Desastres y Continuidad del Negocio	"Ésta define cómo responde una organización a un incidente de ciberseguridad o cualquier otro evento que provoque la pérdida de operaciones o datos. Las políticas de recuperación ante desastres dictan cómo la organización restaura sus operaciones e información para volver a la misma capacidad operativa que tenía antes del evento. La continuidad del negocio es el plan al que recurre la organización mientras intenta operar sin ciertos recursos" (Kaspersky, 2021)

Categoría	Descripción
Educación del Usuario Final	"Ésta aborda el factor de ciberseguridad más impredecible: las personas. Cualquiera puede introducir accidentalmente un virus en un sistema que de otro modo sería seguro si no sigue las buenas prácticas de ciberseguridad. Enseñar a los usuarios a eliminar archivos adjuntos de correo electrónico sospechosos, a no conectar unidades USB no identificadas, y otras lecciones importantes es vital para la ciberseguridad de cualquier organización" (Kaspersky, 2021)

Nota. (Kaspersky, 2021)

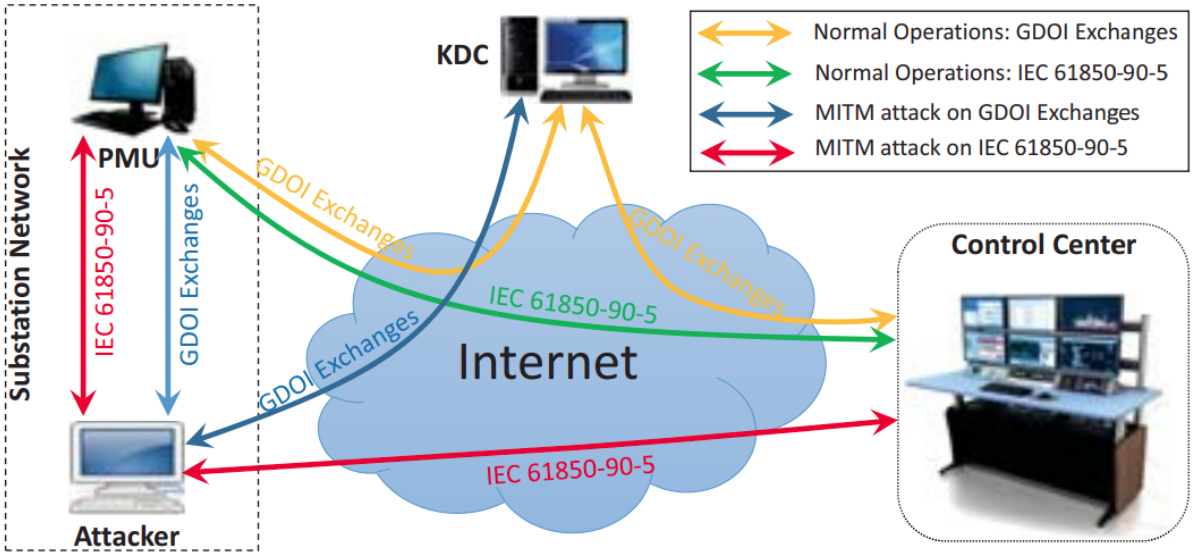
2.3.3 Ciberseguridad en OT

Para mejorar las funciones y la productividad del sistema, cada Sistema de Control Industrial incorpora constantemente nuevas tecnologías y software tanto en IT como en OT. Con la convergencia de IT y OT, se convierten en objetivos más importantes para los ciberdelincuentes. Una de las fallas más comunes de las soluciones de ciberseguridad utilizadas en la infraestructura OT es su incapacidad para proteger los sistemas de control heredados como SCADA. Además de eso, las organizaciones también deben enfrentar el aumento de los desafíos de ciberseguridad en tecnologías nuevas y emergentes, como la computación en la nube, el análisis de big data e Internet de las cosas (IoT). La centralización introduce vulnerabilidades nuevas y desconocidas en el ecosistema ciber físico (Trend Micro, 2016).

Los ataques a los sistemas ICS a menudo son ataques dirigidos que utilizan el punto de entrada de ICS para afianzarse dentro de un sistema que les permitirá moverse lateralmente dentro de la organización. Entre los casos más destacados se encuentran el gusano Stuxnet, que se utilizó para manipular centrifugadoras dentro de instalaciones nucleares en Irán (Shakarian, 2012), y BlackEnergy, que afectó a las instalaciones de generación de energía en Ucrania (Khan et al., 2016) con un ataque de Man in the middle como se puede ver en la Figura 8. A pesar de que la mayoría de los ataques se centran en el robo de datos y / o el espionaje industrial, los dos casos antes mencionados demostraron cómo el malware tuvo un efecto cinético.

Figura 8

Ataque MITM: secuestro de la comunicación IEC 61850-90-5 (Khan et al., 2016)



El documento técnico de Trend Micro titulado Cyber Threats to the Mining Industry (Huq, 2016) explora cómo la industria minera se está convirtiendo cada vez más en un objetivo de las campañas de ciberespionaje. Estas campañas de ciberespionaje están diseñadas para obtener los últimos conocimientos técnicos e inteligencia que ayudarán a algunos grupos de interés a prosperar y mantener una ventaja competitiva.

2.3.4 Estándar de ciberseguridad OT IEC 62443 / ISA 99

El estándar IEC 62443 / ISA 99 es específico de OT. Desarrollado conjuntamente por la Organización Internacional de Estándares y la Sociedad Internacional de Automatización, el marco detalla cuatro niveles destinados a proporcionar ciberseguridad para diferentes tipos o madurez de ataques. Las organizaciones pueden determinar qué nivel de ciberseguridad es el más apropiado en función de sus propios requisitos únicos de cumplimiento o de la cadena de suministro.

Cada nivel de ciberseguridad IEC 62443 / ISA 99 establece un conjunto de requisitos para alcanzar ese nivel. Por ejemplo, hay 37 requisitos para lograr el nivel 1 y 23 adicionales para alcanzar el nivel 2. Estos componentes se parecen mucho a los incluidos en los marcos CIS o NIST, lo que tiene sentido teniendo en cuenta que estos estándares no intentan reinventar la ciberseguridad, solo concentran los esfuerzos.

Debido a que IEC 62443 / ISA 99 está diseñado específicamente para entornos OT, los controles brindan más contexto para los elementos relevantes para la tecnología operativa. Por

ejemplo, el término de la técnica conocida como "zonas y conductos" es un sello distintivo de este estándar. Las "zonas" se pueden considerar como las diferentes partes de una red donde los dispositivos pueden comunicarse entre sí, una característica particularmente relevante en los entornos de OT segmentados. Los "conductos" son entonces las vías de comunicación dentro o entre zonas. IEC 62443 / ISA 99 incluye arquitecturas recomendadas para garantizar comunicaciones seguras dentro de zonas y entre conductos.

2.3.5 Marco de ciberseguridad de NIST (NIST CSF)

El marco de ciberseguridad NIST (NIST CSF, en inglés National Institute of Standards and Technology - Cyber Security Framework) tiene recomendaciones de controles de ciberseguridad muy detalladas, incluidas algunas especialmente ajustadas para sistemas de control industrial junto con una guía emergente para entornos de I.IoT. El CSF es un conjunto de pautas más generales con aproximadamente 120 subcontroles en cinco dimensiones primarias (Ganzer, 2019).

Las cinco funciones del NIST abarcan controles técnicos y de procedimiento, lo que proporciona una base para las evaluaciones de ciberseguridad. En cada una de sus áreas funcionales, el NIST CSF describe subcontroles con pautas detalladas para lograr niveles de madurez específicos.

La madurez en NIST CSF se define mediante el establecimiento de un conjunto de "perfiles". Estos perfiles no son prescriptivos, aunque el NIST ofrece algunos modelos sugeridos. Las organizaciones deben determinar sus propios objetivos y perfiles de madurez, lo que aumenta la flexibilidad del marco.

NIST CSF es el estándar más utilizado en ciberseguridad ICS según SANS. En las encuestas ICS de 2017 y 2019, la mayoria de los encuestados usaban mas NIST CSF que cualquier otro marco, seguido de CIS Top 20, ISO 27000 e IEC 62443 / ISA 99. NIST CSF sigue siendo una alternativa atractiva ya que proporciona orientación direccional y fundamental sin políticas o controles prescriptivos que las organizaciones pueden encontrar demasiado restrictivas para sus entornos de OT únicos (Verve, 2021).

2.3.6 Ciberseguridad en la convergencia IT y OT

Las ciberamenazas pueden comprometer infraestructuras críticas a medida que las industrias integran la automatización e I.IoT en sus entornos de trabajo de tecnología operativa, las plantas y fábricas modernas se han convertido en objetivos de ciberataques.

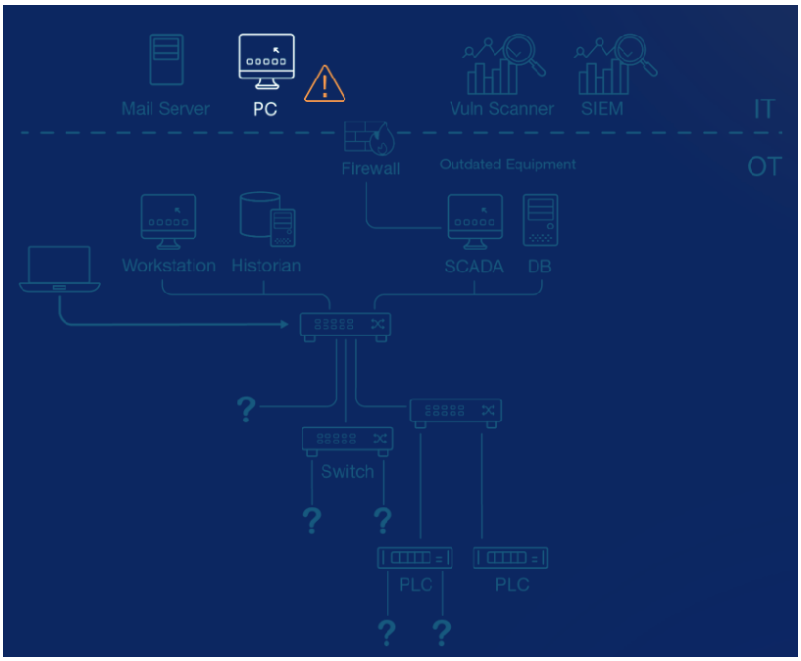
La empresa de ciberseguridad Tenable, la cual posee una basta experiencia en el rubro, que publica artículos de investigación sobre ciberseguridad OT y convergencia IT-OT, y que además posee productos de ciberseguridad para OT, define las siguientes cinco amenazas como las más críticas para prestar atención en 2021 y como un ciberdelincuente puede aprovecharse de ellas (Tenable, 2021):

1) Convergencia accidental (Figura 9)

Dado que los activos de IT comprenden entre el 20% y el 50% de los entornos industriales modernos, el espacio de aire tradicional (separación física entre los dispositivos) ya no es suficiente para proteger la infraestructura OT. Los ciberdelincuentes de hoy pueden hacerlo desde otros lados y los ataques se mueven lateralmente a través de IT a OT, y viceversa.

Figura 9

Las ciberamenazas que pueden derribar infraestructuras críticas: convergencia accidental (Tenable, 2021)



¿Cómo puede aprovechar un ciberdelincuente esta amenaza?

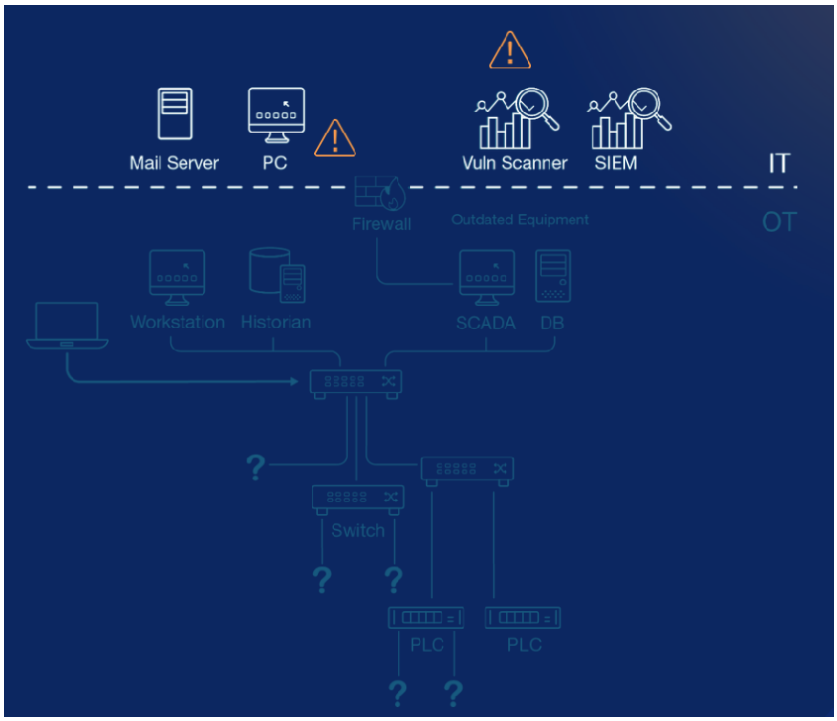
Una sola unidad USB o una computadora portátil infectada es todo lo que se necesita para que un ciberdelincuente obtenga el control de su red industrial. Los ataques OT recientes han explotado vectores previamente desconocidos, que incluyen equipamiento del tipo: acústico, térmico, sin visibilidad en las redes OT, luz, radiofrecuencia, equipo obsoleto, sísmico, medios físicos, controladores inseguros, magnético.

2) Sin visibilidad de las redes OT (Figura 10)

Como no se puede defender lo que no se puede ver, si los activos de OT están separados de los controles de ciberseguridad de IT, pueden crear "puntos ciegos" que ponen en riesgo a la organización. Estas brechas hacen que sea más difícil identificar y remediar las amenazas en todo su entorno de IT y OT.

Figura 10

Las ciberamenazas que pueden derribar infraestructuras críticas: Sin visibilidad de las redes OT (Tenable, 2021)



¿Cómo puede aprovechar un ciberdelincuente esta amenaza?

El malware que se dirige a un entorno de IT puede trasladarse a entornos OT e infectar redes industriales. Esto es lo que sucedió con el malware WannaCry y Petya:

- WannaCry
    - Dispositivos afectados: más de 200.000 dispositivos, incluidas computadoras, escáneres de resonancia magnética, refrigeradores de almacenamiento de sangre y equipos de teatro.
    - Daños: las estimaciones oscilan entre cien y miles de millones de dólares.
    - Industrias afectadas: automotriz, servicios públicos, logística, banca y atención médica.

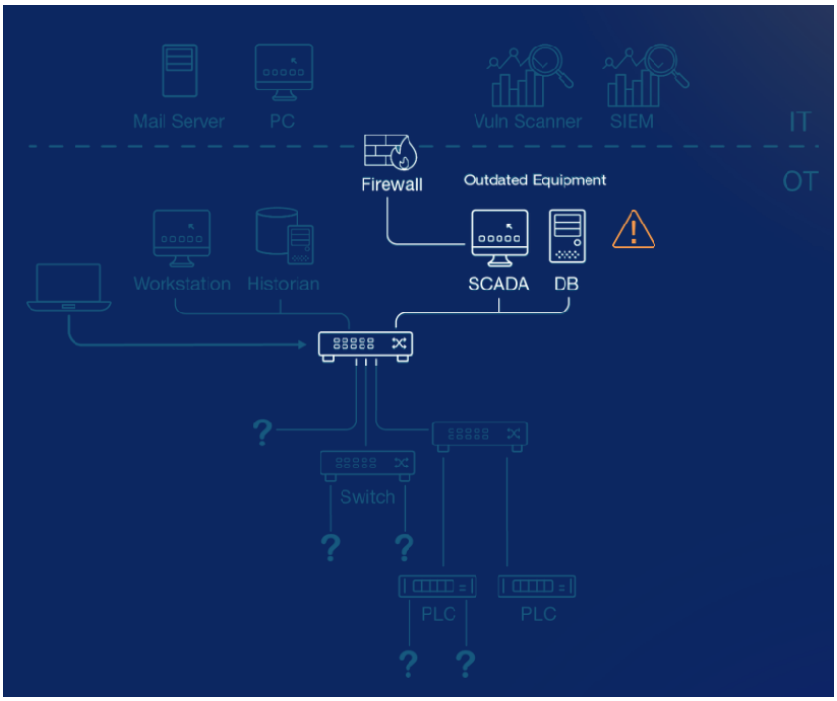
- Petya
    - El enfoque principal de Petya y NotPetya era cifrar archivos y borrar el registro de inicio. Algunos creen que el ejército ruso fue responsable del ataque.
    - Industrias afectadas: logística y farmacéutica

3) Equipos obsoletos (Figura 11)

Si bien quienes gestionan los equipos de trabajo y el equipamiento tecnológico de IT actualizan regularmente la tecnología más antigua, en el caso de OT están acostumbrados a trabajar con sistemas heredados, muchos de los cuales son anteriores a la era de Internet. Partes de la infraestructura de OT no han sido actualizadas desde su instalación, tal vez hace más de diez años o cuando se inauguró una planta.

Figura 11

Las ciberamenazas que pueden derribar infraestructuras críticas: Equipos Obsoletos (Tenable, 2021)



¿Cómo puede aprovechar un ciberdelincuente esta amenaza?

Podrían aprovechar los protocolos de red propietarios, que a menudo carecen de controles de ciberseguridad básicos, como los de autenticación o el cifrado.

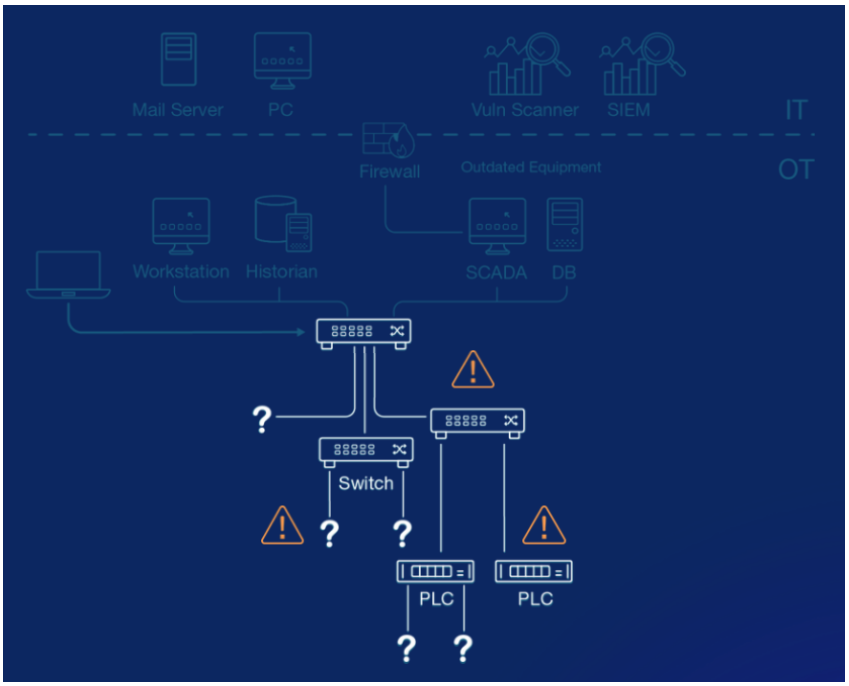
Mientras que el mundo IT se esfuerza por obtener mejor y más reciente hardware y software, con ciclos de vida de 12 a 18 meses, en entornos OT se utilizan sistemas heredados que priorizan la disponibilidad y confiabilidad con ciclos de vida de entre 10 y 15 años.

4) Controladores inseguros (Figura 12)

Los Sistemas de Control Industrial (ICS) se mantienen encendidos por periodos de tiempo muy extensos, por lo cual, debido a su confiabilidad, muchos de estos dispositivos han estado instalados durante años. Son los caballos de batalla de la sociedad moderna de hoy y el punto cero de los ataques dado que también le garantizan persistencia a los atacantes.

Figura 12

Las ciberamenazas que pueden derribar infraestructuras críticas: Controladores Inseguros (Tenable, 2021)



¿Cómo puede aprovechar un ciberdelincuente esta amenaza?

Realizar movimientos laterales es la metodología preferida por los ciberdelincuentes debido a la relativa facilidad con la que se encuentra un eslabón débil en el sistema, aprovecharlo como punto de entrada y luego apropiarse rápidamente de toda la red.

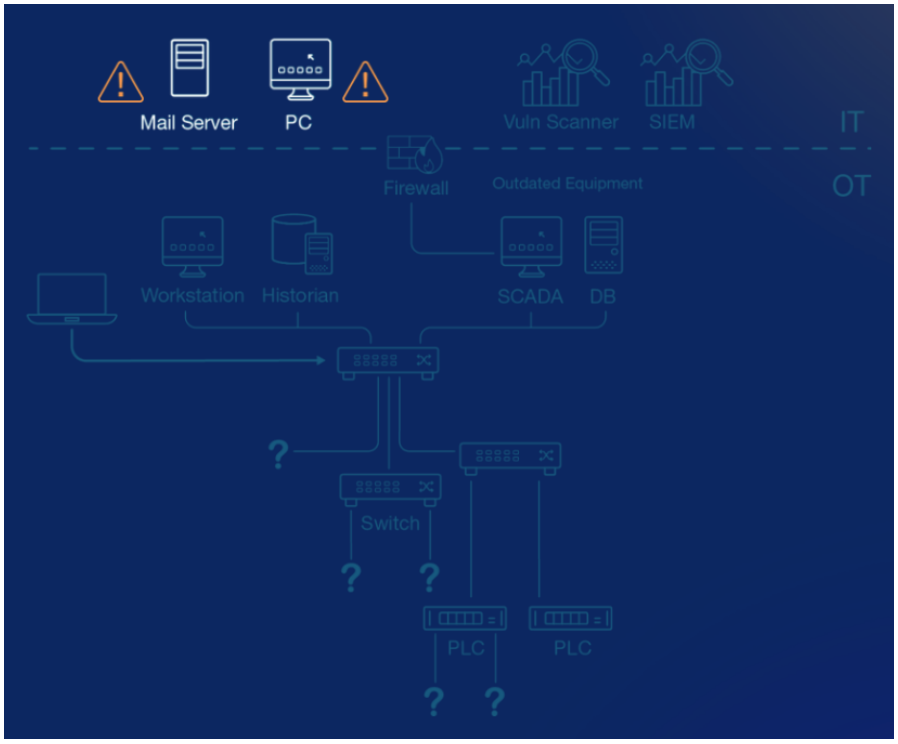
5) Empleados descontentos y negligentes (Figura 13)

No es algo en lo que a las empresas les guste pensar, porque suelen confiar en sus empleados. Pero a veces suceden cosas que escapan de su control, ya sea de forma intencionada

o accidental, ya sea de un informante negligente o de un proveedor externo, o de alguien que tenga la intención de hacer daño, el resultado es el mismo.

Figura 13

Las ciberamenazas que pueden derribar infraestructuras críticas: empleados descontentos y negligentes (Tenable, 2021)



¿Cómo puede aprovechar un atacante esta amenaza?

Un empleado descontento podría robar un código o sabotear una línea de producción, llevando a un resultado catastrófico en la infraestructura OT.

Luego, en el mismo informe, Tenable indica que los siguientes cinco controles son los más importante para poder proteger los ambientes OT de las amenazas mencionadas (Tenable, 2021):

1) Visibilidad de todo el entorno IT y OT

Poder lograr tener identificados y diagnosticados todos los dispositivos de ambos ambientes en su convergencia, posibilita poder lograr identificar el riesgo real de la superficie de ataque en el cual un ataque pueda llevarse a cabo.

2) Identificación de amenazas y mitigación

Poder detectar y generar alertas de las amenazas en ambos entornos, provenientes de fuentes internas o externas, ya sean basados en malware o de naturaleza humana.

3) Seguimiento de activos

Poder lograr descubrir y realizar el seguimiento de todos los activos de forma automática, para lograr tener un inventario de los mismo actualizado sumando visualización de donde se encuentran.

4) Gestión de vulnerabilidades

Poder generar un scoring de riesgo de cada uno de los activos identificados en los entornos, priorizar las vulnerabilidades encontradas y lograr una visualización continua del riesgo actual, particular de los dispositivos y general del entorno.

5) Control de configuraciones

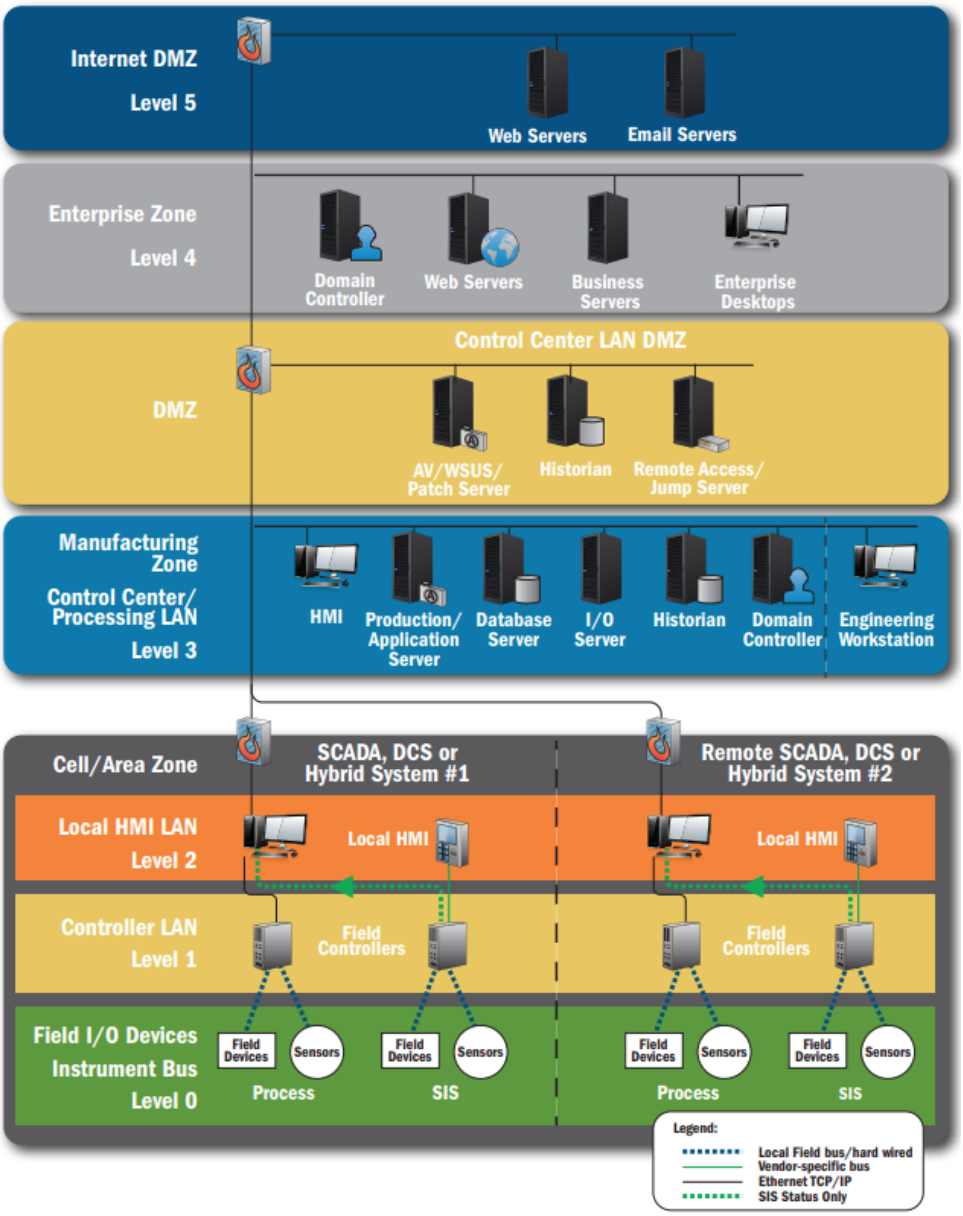
Poder realizar seguimiento y registrar todos los cambios de configuración realizados por un usuario o por un malware, sin importar en qué parte del entorno se realice, ya sea en la red o en algún dispositivo OT. Poder realizar una copia de respaldo del último estado "bueno" conocido para poder utilizarlo en un proceso de recuperación.

Luego el equipo de ICS-CERT (Industrial Control Systems - Cyber Emergency Response Team) de CISA (Cybersecurity & Infrastructure Security Agency) desarrolló un documento cómo realizar una implementación segura para la convergencia de IT y OT. En este documento llamado "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies" (Cybersecurity & Infrastructure Security Agency [CISA], 2016) se describe detalladamente recomendaciones a la hora de definir un programa de ciberseguridad OT basado en varios años de análisis de las principales amenazas identificadas en implementaciones de infraestructuras críticas localizadas en EE.UU.

También en este documento (CISA, 2016), en la sección 2.4 "ICS Network Architectures" describe las mejores prácticas de ciberseguridad a la hora de definir una topología de redes de telecomunicaciones donde se intente lograr la convergencia de IT y OT (Figura 14).

Figura 14

Arquitectura de red segura recomendada (Cybersecurity & Infrastructure Security Agency, 2016)



Luego en la parte final de la sección 2.4.2 “Demilitarized Zones” (DMZ, en castellano zona desmilitarizada) dan precisos detalles sobre la implementación de un Jump host (o Jump boxes) en la zona de DMZ para proveer acceso remoto a la red OT implementado controles de acceso y múltiples factores de autenticación. Según ellos esta es la solución recomendada para la convergencia IT-OT logrando un buen nivel de operatoria y a su vez manteniendo las buenas prácticas de ciberseguridad.

2.3.7 Ciberataques a I.IoT y sus contramedidas

Los recientes ataques a los sistemas ciber físicos suscitan una gran preocupación en materia de ciberseguridad, ya que estos ataques causan enormes pérdidas materiales y pueden provocar también situaciones de riesgo para la vida (Panchal et al., 2019). Por ello es importante poder identificar las amenazas a la ciberseguridad de las industrias que implementan I.IoT, como también los diversos ataques que son posibles en los componentes de la arquitectura de la I.IoT en capas.

Mientras que en el mundo IT la ciberseguridad suele asumir un modelo cliente-servidor, donde la comunicación entre el cliente y el servidor se produce utilizando protocolos bien conocidos como IP (Internet Protocol) TCP (Transmission control Protocol), UDP (User Datagram Protocol) o HTTP (Hypertext Transfer Protocol). Los daños causados por un ataque exitoso suelen implicar dinero o reputación y rara vez implica amenazas a la ciberseguridad (Industrial Internet Consortium, 2016). Sin embargo, los sistemas OT fueron diseñados para operar procesos industriales de forma segura y fiable. Los componentes y subsistemas de OT no se crearon pensando en la ciberseguridad, y para poder lograrlo se aplican medidas de seguridad física y de aislamiento de las redes OT.

Pero estos controles de ciberseguridad no son confiables ya que tienen algunos puntos ciegos que pueden ser utilizados para atacar. Aislar las redes OT puede prevenir un ataque desde una red diferente, pero no puede evitar los ataques dentro de la red. Dentro de una red aislada se puede desplegar eficazmente el malware para comprometer el sistema. Por lo tanto, tenemos que estudiar los posibles ataques en varios niveles de la arquitectura del I.IoT.

En la Figura 15 se puede observar como los autores del trabajo de investigación “Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures” (Panchal et al., 2019) presentan una arquitectura en capas para poder identificar y clasificar los componentes y los posibles ciberataques en cada una de las capas de OT (las primeras tres) e IT (las últimas dos).

Figura 15

Arquitectura en capas de I.IoT y posibles ataques (Panchal et al., 2019)

Layer		Components	Possible Attacks
IT	V	Business Applications, Cloud Computing, Data Analytics, Internet and Mobile Devices	DoS, Side channel attacks, Cloud malware Injection, Authentication Attacks, Man-in-the-Middle, Mobile device attacks
IT	IV	Data Centres, Office Application, Intranet, Mail and Web Services	Phishing, SQL Injections, Malwares, DNS poisoning, Remote code Execution, Brute Force Attacks, Web Application Attacks
DeMilitarized Zone			
OT	III	SCADA Control , HMI, Control Room and Operator Stations	IP spoofing, Data sniffing, Data manipulation, Malwares
OT	II	Distributed Control Systems, PLC's, and Gateways	Replay attack, Man-in-the-Middle attack, Sniffing, Wireless device attacks, Brute force Password guessing
OT	I	Sensors, Motors, Actuators, Transmitters, Embedded Devices	Reverse Engineering, Malware, Injecting crafted packets or input, Eavesdropping, Brute-force search attacks

Todas las capas anteriores tienen alguna vulnerabilidad asociada a los componentes que tienen, estas capas son (Panchal et al., 2019):

- Capa 1: Dispositivos integrados, sensores, actuadores, transmisores y motores funcionan en este nivel para realizar procesos físicos.
- Capa 2: Sistemas de control distribuido (DCS), controladores lógicos programables (PLC) y pasarelas interactúan con los dispositivos de la capa 1.
- Capa 3: SCADA (Control de Supervisión y Adquisición de Datos), dispositivos de Adquisición de Datos e Interfaz Hombre-Máquina (HMI) que utilizan el protocolo de red basado en IP residen en esta capa.
- DMZ: La zona desmilitarizada se utiliza para separar las redes de IT y OT. Los dispositivos críticos que necesitan estar expuestos a la red exterior, como los servidores de aplicaciones y los servidores web, residen en esta capa. Impide el acceso directo a las redes OT mediante herramientas de ciberseguridad como el firewall.

- Capa 4: En esta capa se implementan las aplicaciones de oficina, los servicios de intranet, los servicios web y los servicios de correo. Esta capa es la principal responsable de la planificación empresarial (IT).
- Capa 5: Aplicaciones empresariales, computación en la nube, análisis de datos, Internet y dispositivos móviles en esta capa son responsables de los procesos de análisis y minería de datos para entregar la información a través de Internet e incluso en los dispositivos móviles.

La capa 5 está expuesta a Internet, ya que utilizan servicios también públicos en esta red y proporciona una superficie de ataque para ataques remotos. La tecnología de computación en la nube ha ayudado mucho a almacenar datos de forma remota, realizar análisis y tomar decisiones críticas para el negocio, pero la nube tiene su propio conjunto de vulnerabilidades asociadas con el tipo de nube que se utiliza. La nube pública posee mucho riesgo ya que utiliza servicios de Internet para la comunicación (Papp et al., 2015, p.1). Esta capa también contiene dispositivos móviles que pueden obtener datos de la nube o de Internet cuando los datos que se originan en las industrias se almacenan para el análisis y el procesamiento de los datos. Las capas inferiores utilizan redes de comunicación y servicios internos, que evita los ataques desde las redes públicas. Los dispositivos en OT son dispositivos integrados compuestos por hardware, firmware/OS y aplicación, en los cuales los ataques suelen explotar las vulnerabilidades de los protocolos utilizados por los dispositivos para comunicarse (Papp et al., 2015, p.1).

En la investigación realizada “Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures” (Panchal et al., 2019), se enumeran los ataques relacionados a las capas mencionadas anteriormente y por lo tanto a una implementación de I.IoT como se puede observar en la Tabla 4.

Tabla 4

Ciberataques a I.IoT y sus contramedidas

Ataque	Descripción	Contramedida
Ataque de denegación de servicio (DoS)	Es un ataque realizado en una red para restringir un servidor de servir a su cliente, estos ataques tienen como objetivo el ancho de banda de la red o los servicios. En la nube los ataques de DoS son más dañinos, implica el envío de demandas de hosts inocentes o secuestrados en la red (zombis), y de ahí que también se conoce como Cloud Zombie Attack o Denegación de Servicio Distribuida (DDoS, del inglés Distributed Denial of Service).	Se pueden utilizar firewalls para permitir o denegar el acceso a las solicitudes, la detección de ataques DoS mediante un sistema de detección o prevención de intrusiones (IDS/IPS, del inglés Intrusion Detection System / Intrusion Prevention System) y un mejor sistema de autenticación y autorización pueden ayudar a evitar estos ataques.
Ataques de canal lateral	Para realizar un ataque de canal lateral en la nube se coloca una máquina virtual maliciosa en la nube para atacar la implementación del sistema de algoritmos criptográficos. Por lo general, en la nube I.IoT la seguridad es gestionada por los proveedores de servicios cloud.	Para prevenir ese tipo de ataque es necesario la evaluación de la resistencia de un sistema criptográfico a los ataques de canal lateral, y además es por tanto, importante para el diseño de sistemas seguros.
Inyección de malware en la nube	El atacante inyecta una implementación de servicio malicioso o un gusano en la máquina virtual (VM, del inglés Virtual Machine) en el sistema de la	Realizar una comprobación de la integridad de la instancia de servicio antes de utilizarla para la solicitud entrante puede prevenir este ataque.

Ataque	Descripción	Contramedida
	nube capaz de infectar los objetivos que allí residen.	
Ataques de autenticación	En la actualidad, la mayoría de los servicios en la nube siguen utilizando un nombre de usuario y una contraseña de tipo de autenticación de un solo factor basado en el conocimiento.	El bloqueo de la cuenta, la respuesta retardada y los esquemas de autenticación multifactor pueden evitar este ataque.
Ataque criptográfico Man in the Middle	En este ataque el atacante se coloca entre dos usuarios (MitM, del inglés Man in the Middle) sobre la ruta de comunicación e intercepta o modifica la comunicación entre ellos.	Estos ataques pueden evitarse utilizando contraseñas de un solo uso (OTP, del inglés One Time Password) o utilizando autenticación mutua.
Ataques a dispositivos móviles	Los vectores de ataque a los dispositivos móviles pueden ser el malware, la exfiltración de datos, la manipulación de datos y la pérdida de datos.	Para evitar estos ataques en el dispositivo móvil, asegúrese de que sólo se conceden los permisos necesarios a la aplicación y verifique que ésta no contiene ninguna puerta trasera comprobando las firmas de confianza.
Ataques de phishing	Los ataques de suplantación de identidad se producen cuando los atacantes engañan al usuario para que interactúe con páginas web o correos electrónicos falsos de aspecto original para obtener acceso a sus datos confidenciales	Educar a la gente sobre este tipo de ataque es la mejor manera de defensa contra el phishing.

Ataque	Descripción	Contramedida
Inyección SQL (SQLi)	Es un ataque de inyección en el que el atacante inyecta información maliciosa para obtener datos confidenciales almacenados en la base de datos, eliminar la base de datos y/o evitar la autenticación.	Estos ataques se pueden evitar utilizando consultas parametrizadas y procedimientos almacenados.
Malware	El malware en la capa 4 puede utilizarse para propagarse a la OT, si los sistemas en la IT no están parcheados y no se aplica ninguna política de seguridad. El código malicioso podría entregar una carga útil maliciosa (payload) a los dispositivos de la capa inferior en la red de OT.	El uso de antivirus y firewalls con actualizaciones periódicas puede prevenir ataques de malwares.
Envenenamiento de DNS	Para realizar este ataque el atacante envía una respuesta del servicio de nombres de dominio (DNS, del inglés Domain Name Service) falsificada al servidor DNS para que los datos corruptos se almacenen en la caché del servidor DNS.	Para evitar el envenenamiento se deben limitar las consultas recursivas y comprobar las respuestas de las consultas para que sólo proporcione información sobre el dominio solicitado.
Ejecución remota de código	La ejecución remota de código se produce cuando un atacante explota una vulnerabilidad en el sistema para introducir un malware que puede controlar el sistema objetivo de forma remota.	La aplicación de actualizaciones periódicas, la comprobación de los límites del búfer de datos y las técnicas de prevención de malware pueden ayudar a prevenir la ejecución remota de código.

Ataque	Descripción	Contramedida
Ataques de fuerza bruta	El atacante prueba un conjunto de entradas diferentes hasta encontrar una entrada válida para obtener acceso a los recursos protegidos por alguna información secreta utilizada para identificar a un usuario.	El bloqueo de la cuenta, la respuesta retardada y los esquemas de autenticación multifactor pueden evitar este ataque.
Ataques a aplicaciones web	Este tipo de ataques se producen en las aplicaciones web que se alojan en los servidores web que residen en la zona desmilitarizada y aprovechan vulnerabilidades a nivel aplicación web.	La aplicación o servicio web puede ser protegido de los ataques mediante un firewall de aplicaciones web (WAF, del inglés Web Application Firewall). El WAF intercepta el tráfico que va a una aplicación web y luego aplica filtros para detectar comandos maliciosos, contenido inapropiado y mala sintaxis.
Suplantación de IP	Un atacante se hace pasar por otro dispositivo a propósito modificando la cabecera del paquete con una dirección del protocolo de Internet (IP, del inglés Internet Protocol) falsificada. En las plantas industriales puede ser arriesgado si se utiliza el protocolo industrial Ethernet/IP para la comunicación, que utiliza direcciones IP para identificar los dispositivos.	Establecer mecanismos de control de IP en los switches, routers y firewalls para detectar casos de suplantación de IP, tanto para el tráfico saliente como entrante, y establecer mecanismos robustos de autenticación de los dispositivos.
Ocultación de datos	Es fácil escuchar los datos que pasan por la red industrial, ya que	La mejor manera de defenderse de los ataques de ocultación de datos

Ataque	Descripción	Contramedida
	todos los dispositivos están en la misma subred.	es cifrar todos los datos que pasan por el canal de comunicación. Aunque no es posible cifrar todos los datos debido a la capacidad de cómputo que requiere la encriptación, podemos encriptar los datos sensibles, como las credenciales, que suelen viajar como texto plano cuando se utilizan protocolos industriales.
Manipulación de datos:	La manipulación de los datos es más fácil en las redes industriales, ya que no hay una función de comprobación de la integridad implementada en los protocolos industriales más antiguos, e incluso si se implementa, los datos viajan en texto plano, y un atacante que modifique los datos puede modificar la suma de comprobación de los paquetes.	Asegurar el canal de comunicación y encriptar la comunicación puede ayudar a prevenir este tipo de ataques.
Ataques de repetición	Los ataques de repetición se producen cuando se captura un paquete y se vuelve a enviar posteriormente. Este ataque puede utilizarse para enviar valores erróneos a los sistemas de control. Si se capturan paquetes con valores normales y se reproducen, se puede engañar a los operadores dándoles	Se recomienda enviar marcas de tiempo con los paquetes.

Ataque	Descripción	Contramedida
	valores erróneos.	
Ataques a la red inalámbrica	Son posibles varios ataques a la red inalámbrica. Algunos de ellos son el ataque WEP (Wired Equivalent Privacy), el ataque evil twin, el ataque man-in-the-middle, el DoS, etc.	Muchos de estos ataques pueden ser prevenir utilizando los últimos parches y siguiendo las mejores prácticas como la autenticación adecuada, la búsqueda de puntos de acceso las mejores técnicas de cifrado como WPA2/AES (Wi-Fi Protected Wi-Fi Protected Access with Advanced Encryption Standard) y la implementación implementación del sistema de autenticación 802.1X.
Ingeniería inversa	Mediante un proceso de ingeniería inversa del código fuente del software o firmware utilizado en el dispositivo embebido, un atacante puede obtener información sensible como credenciales codificadas y encontrar errores en el código para planificar un ataque. La ingeniería inversa y la modificación del firmware pueden realizarse para inyectar código malicioso en el dispositivo (Palavicini et al., 2017, p.1).	Evitar las credenciales codificadas y utilizar técnicas de ofuscación de código pueden prevenir la ingeniería inversa.

Notas. (Panchal et al., 2019)

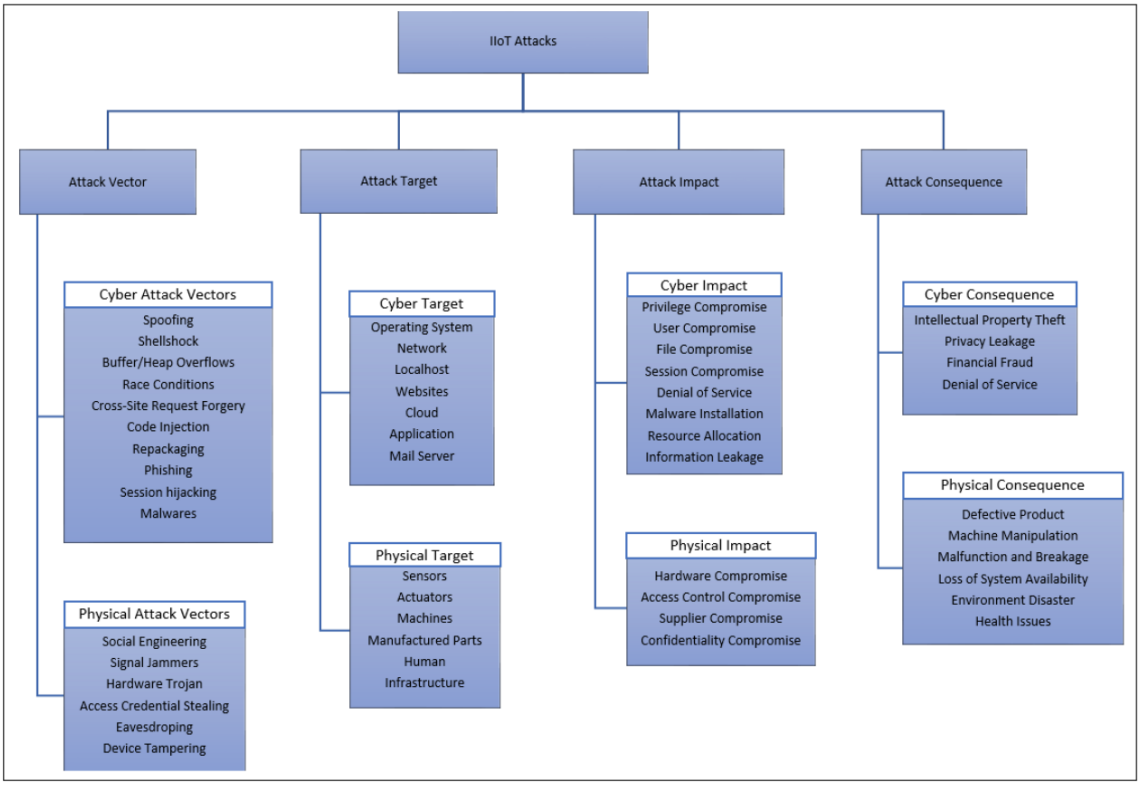
En el mismo documento de investigación “Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures” (Panchal et al., 2019), los autores utilizan

una taxonomía de ataques para I.IoT, la cual ayuda a comprender y clasificar los incidentes de ciberseguridad (Wu & Moon, 2017, p. 367). Chris Simmons, en una investigación anterior junto a Charles Ellis, S. Shiva y Dipankar Dasgupta, desarrolló una taxonomía sobre ciberataques que llama AVOIDIT (Simmons et al., 2009). Esta taxonomía tiene cinco dimensiones: vector de ataque, impacto operativo, defensa, impacto de la información y objetivo. Con ella es posible clasificar fácilmente los ciberataques de IT pero que es incapaz de clasificar los ataques a I.IoT industrial ya que carece de los vectores de ataque físicos que están abiertos en los ataques industriales. Entonces, Mingtao Wo se basó en AVOIDIT y desarrolló una taxonomía con cuatro dimensiones: vector de ataque, impacto de ataque, objetivo de ataque y consecuencia de ataque.

En la Figura 16 se puede observar la modelización de los vectores de ataques a I.IoT en estas cuatro dimensiones que representa cómo el ataque puede llevarse a cabo, qué componentes se afectan, qué podría alcanzar el atacante y las consecuencias del mismo.

Figura 16

Taxonomía de Ataques de Ciberseguridad en IIoT (Panchal et al., 2019)



La taxonomía propuesta puede ser útil para clasificar los ataques a la I.IoT, las cuatro dimensiones pueden distinguir fácilmente los ataques en el entorno de IT y OT, por lo que es

un método adecuado para entender los ataques a I.IoT. Sin embargo, la taxonomía de ataques puede carecer de algunos de los nuevos vectores de ataque que se descubran o desarrollen recientemente y en el futuro. En esta taxonomía los autores han incluido el vector de ataque malware que contiene varios tipos de códigos maliciosos que pueden ser útiles para comprometer la ciberseguridad de cualquier sistema. Hay varios tipos de malwares como virus, troyanos, gusanos, ransomware, rootkits, spywares, etc. Pero sólo los virus y los gusanos se incluyeron en la taxonomía de los ataques transversales a los sistemas de fabricación híbridos IT-OT, por lo que ampliaron la taxonomía para incluir algunos de los vectores de ataque que faltan y que están abiertos en I.IoT.

Según los autores, con esta taxonomía es posible modelar cualquier ataque a una infraestructura industrial utilizando las cuatro dimensiones que revelan la información sobre cómo se realizó el ataque, qué componentes están afectados y qué pudo lograr el atacante. La primera dimensión es el camino o medio por el que un atacante puede acceder a un ordenador o red. Los vectores de ataque se subdividen en ciberataque y ataque físico. Los vectores de ciberataque contienen los puntos de entrada en las redes informáticas en los que no se requiere acceso físico, mientras que los vectores de ataque físico necesitan que el atacante interactúe con el dispositivo o las personas del sector. La segunda dimensión se refiere al objetivo, que es el componente sobre el que se ha planificado el ataque, mientras que la tercera se refiere al impacto del ataque y la cuarta a las consecuencias (Panchal et al., 2019).

2.3.8 Marco de trabajo de Seguridad de I.IoT (Industry IoT Consortium)

El Marco de Seguridad de la Internet Industrial (IISF, del inglés Industrial Internet Security Framework) es un recurso para entender las consideraciones de ciberseguridad de I.IoT, desarrollado por expertos internacionales en la materia del Industry IoT Consortium. El objetivo del IISF es impulsar el consenso en la industria, promover las mejores prácticas de ciberseguridad en I.IoT y acelerar su adopción, explicando cómo combinarla con el negocio de las operaciones industriales. Define los bloques funcionales para abordar los problemas de esta, proporciona orientación para la implementación y técnicas prácticas para la ciberseguridad de I.IoT.

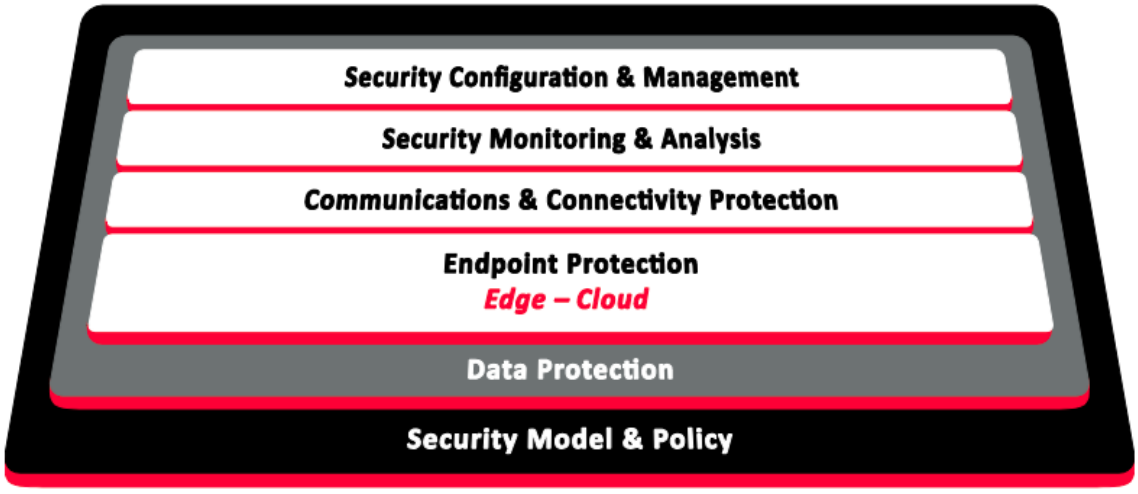
El IISF está escrito para las máximas autoridades de tecnología y ciberseguridad de las organizaciones, como los CTO, CISO y expertos en ciberseguridad. Se puede utilizar el IISF como guía para implementar estas tecnologías disponibles en la actualidad para mejorar la disponibilidad y confiabilidad de su sistema y, por lo tanto, obtener un retorno de la inversión (ROI, del inglés Return of Investment) significativo.

Para los directores ejecutivos y gerentes de negocios, el IISF ofrece un análisis de las preocupaciones industriales relacionadas sobre ciberseguridad, confiabilidad, resiliencia y privacidad. Destaca la necesidad de que todas las organizaciones de todas las industrias aseguren sus sistemas I.IoT e implementen soluciones de ciberseguridad de mejores prácticas de inmediato.

El IISF identifica, explica y posiciona las arquitecturas, los diseños y las tecnologías relacionadas con la ciberseguridad en I.IoT, así como identifica los procedimientos relevantes para estos. Describe sus características, las tecnologías y técnicas que deben aplicarse, los métodos para abordarla y cómo obtener la garantía de que se ha abordado la combinación adecuada de cuestiones para satisfacer las expectativas de las partes interesadas. La publicación del IISF inicia un proceso para crear un amplio consenso en la industria sobre cómo asegurar los sistemas I.IoT. En la Figura 17 se puede observar los bloques fundamentales del IISF.

Figura 17

Bloques de construcción funcionales del marco de seguridad (Industrial Internet Consortium, 2016)



Para la IISF todo proyecto de I.IoT debe implementar la ciberseguridad en su totalidad. Una implementación de forma adecuada en un entorno industrial conlleva muchos niveles de complejidad y se aporta un enfoque de protección integral con el objetivo de minimizar el riesgo.

Los acontecimientos descritos anteriormente en este trabajo, han ilustrado el riesgo de ser atacado desde fuentes inesperadas tanto dentro como fuera del sistema, ya sea de forma intencionada o accidental. Existe una necesidad imperiosa de protegerse contra los errores, las

equivocaciones y las intenciones maliciosas. El Industry IoT Consortium considera que estos riesgos de ciberseguridad industrial representan una gran amenaza para la ciberseguridad mundial.

Al seguir las orientaciones del IISF y asegurar los sistemas I.IoT, las empresas pueden acceder a información valiosa que antes no estaba disponible, lo que conduce a un enfoque más completo y sistemático de la ciberseguridad. La aplicación de esta nueva información mejora la precisión de las decisiones críticas para el negocio, la protección de las operaciones contra el riesgo de daños provocados por violaciones de la ciberseguridad ahorra dinero, tiempo y reputación.

Un ataque exitoso a un sistema de I.IoT tiene el potencial de ser tan grave como los peores accidentes industriales ocurridos hasta la fecha (por ejemplo, Chernobyl y Bhopal), con el resultado de daños al medio ambiente, lesiones o pérdida de vidas humanas. También existe el riesgo de que se produzcan daños secundarios, como: la interrupción o el cese de las operaciones, la destrucción de sistemas, la filtración de datos empresariales y personales sensibles que provoquen la pérdida de la propiedad intelectual, el daño a la reputación de la empresa, la pérdida de clientes, la pérdida económica material, el daño a la marca y la reputación, el daño a las infraestructuras críticas que gestionan la electricidad, el agua, el petróleo y el gas, y el daño irreparable al medio ambiente. Las ventajas de evitar estas circunstancias son evidentes y los ataques a las infraestructuras críticas y a la I.IoT son cada vez más frecuentes y hay que planificar estratégicamente las respuestas adecuadas.

2.3.9 Modelo de Madurez de Seguridad de I.IoT (Industry IoT Consortium)

El objetivo de un Modelo de Madurez de Seguridad (SMM, del inglés Security Maturity Model) es proporcionar un camino para que los proveedores de Internet de las Cosas Industriales (I.IoT) sepan en qué nivel de madurez están y cómo invertir adecuadamente en medidas de ciberseguridad razonables que satisfagan sus necesidades y requisitos. Pretende ayudar a las organizaciones a identificar el enfoque adecuado para la mejora efectiva de estas prácticas cuando sea necesario. Decidir decidir en qué centrar los limitados recursos de ciberseguridad es un reto para la mayoría de las organizaciones, dada la complejidad de un panorama de amenazas en constante cambio.

Dado que una comprensión informada de los riesgos y amenazas a los que se enfrenta una organización es la base para elegir e implementar los controles de ciberseguridad adecuados, el modelo proporciona un marco conceptual para organizar el sinfín de

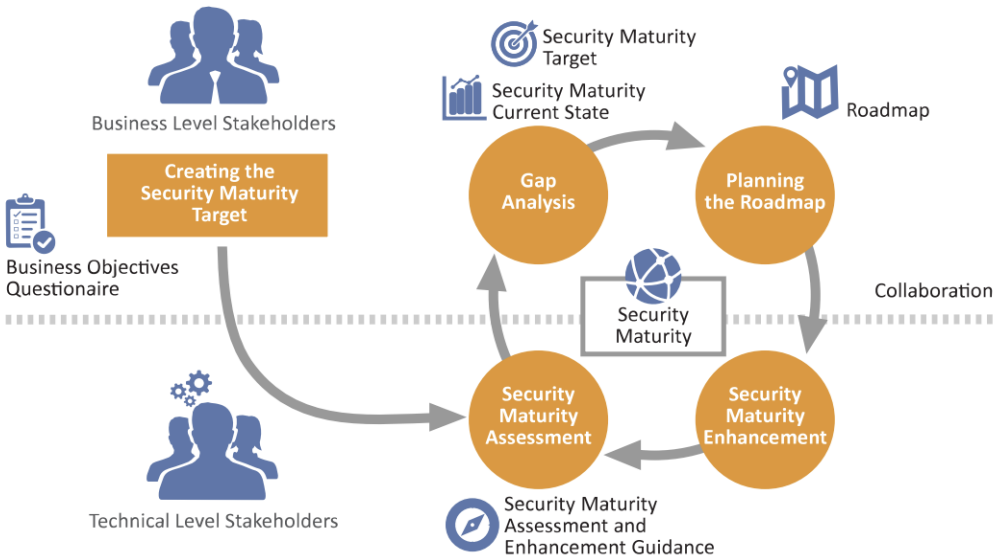
consideraciones. El modelo ayuda a una organización a decidir cuál debería ser su estado de ciberseguridad actual y cuál es su estado objetivo.

No todos los sistemas I.IoT requieren de los mecanismos de protección y los mismos procedimientos para ser considerados suficientemente seguros. La organización determina las prioridades que impulsan el proceso de mejora continua de la ciberseguridad, haciendo posible que los mecanismos y procedimientos se ajusten a los objetivos de la organización sin ir más allá de lo necesario. La aplicación de los mecanismos y procesos de ciberseguridad se considera madura si se espera que sean eficaces para alcanzar esos objetivos. Es la idoneidad de los mecanismos de ciberseguridad para abordar las metas, más que su fortaleza objetiva, lo que determina la madurez. Por lo tanto, la madurez de la ciberseguridad es el grado de confianza en que el estado de ciberseguridad actual satisface todas las necesidades de la organización y todos los requisitos relacionados con la ciberseguridad de la organización. Es decir, la madurez de la ciberseguridad es una medida de la comprensión del nivel general de ciberseguridad actual, incluidas las personas, los procesos y la tecnología, incluida la necesidad, los beneficios y el costo de su soporte. Los factores que contribuyen a sopesar en un análisis de este tipo incluyen las amenazas específicas a los requisitos verticales, de ciberseguridad, regulatorios, éticos y de cumplimiento de la industria de una organización, los riesgos únicos presentes en un entorno y el perfil de amenazas de la organización (Industrial Internet Consortium, 2020).

Como se indica en la Figura 18, parte del primer paso del Proceso de Modelo de Madurez es establecer el contexto de la actividad, definiendo el alcance del sistema en consideración. A esto le sigue la creación de un objetivo o la identificación de un perfil de industria relevante. Después de esto, las organizaciones deben realizar una evaluación para capturar el estado de madurez actual. Se comparan los dos estados y se identifican las brechas para poder establecer una hoja de ruta de mejora. Una vez que se implementan las mejoras, se puede realizar otra evaluación. El ciclo se repite para garantizar que el objetivo de ciberseguridad se mantenga siempre en un panorama de amenazas en constante cambio. Esto incluye, por ejemplo, un mundo donde los ataques que inicialmente son difíciles de montar y requieren una gran habilidad más adelante pueden volverse más fáciles y desplegarse ampliamente debido a la diseminación de conjuntos de herramientas e información.

Figura 18

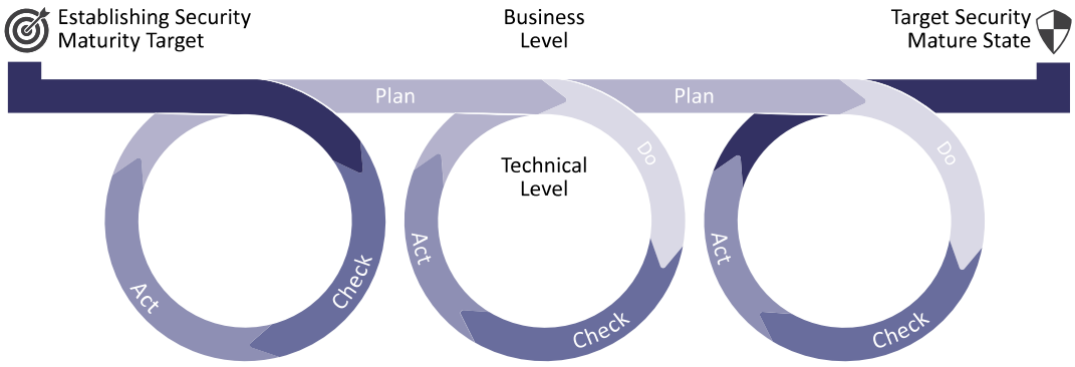
Proceso de Modelo de Madurez de Seguridad (Industrial Internet Consortium, 2020)



Un estado de ciberseguridad persistente solo se puede lograr mediante evaluaciones y mejoras de ciberseguridad continuas, orquestadas a lo largo del tiempo. En consecuencia, como se observa en la Figura 19, el modelo de madurez se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA, del inglés Plan-Do-Check-Act). Este ciclo comienza estableciendo el objetivo de madurez de ciberseguridad para un sistema específico. Luego, comienza un proceso iterativo de alto nivel de mejora de la madurez de la ciberseguridad, como se muestra en la Figura 18. A medida que cambian las amenazas y los enfoques para mitigarlas, las organizaciones deben determinar con qué frecuencia ejecutar el ciclo.

Figura 19

Ciclo de Mejora de Modelo de Madurez de Seguridad (Industrial Internet Consortium, 2020)



Capítulo 3 - Desarrollo Técnico

3.1. Introducción

En el capítulo anterior se recolectó y analizó abundante información de contexto de la Industria 4.0, OT, I.IoT, sobre los ataques a los que se encuentran expuestas estas tecnologías, sus riesgos de ciberseguridad, como también recomendaciones sobre contramedidas que se pueden aplicar. Pero como la gestión de la ciberseguridad no se trata solamente de aplicar medidas eventuales, sino de hacerlo de forma sostenida en el tiempo y de forma priorizada, creando y manteniendo procesos que se integren a la organización, es necesario llevar estas tareas adelante de forma organizada y con una visión más amplia respecto a su gestión.

En este capítulo se desarrollará un programa de ciberseguridad orientado a I.IoT donde se cubrirán aspectos generales y particulares de gestión de la ciberseguridad, modelado de amenazas, análisis de riesgos, gestión de accesos y protección de los datos entre otros. Uno de los objetivos es que se pueda implementar para lograr una reducción de riesgos y que tenga la capacidad de ser adaptado a las diferentes organizaciones para su implementación. Por la naturaleza de la tecnología OT e I.IoT, es clave llevar el nivel de riesgo a un nivel aceptable de ciberseguridad considerando aspectos críticos de una industria altamente automatizada como ser la continuidad de las operaciones y el resguardo de las vidas humanas.

3.2. Programa de Ciberseguridad orientado a I.IoT

Este programa se encuentra basado en el Modelo de Madurez para I.IoT del Industry IoT Consortium, por lo cual está organizado en tres dominios, y cada uno de ellos estará a su vez dividido en tres subdominios. Finalmente cada subdominio está representado por dos procesos. Para cada uno de los procesos se definirán cuatro etapas que van a permitir ir evolucionando en el tiempo, comenzando por las etapas más primitivas y finalizando por las avanzadas.

Esta lista no es exhaustiva, dado que el alcance de la ciberseguridad es muy amplio, por lo que solo se están cubriendo los aspectos que se consideran claves basados en la información obtenida y analizada en el capítulo anterior.

Para cada proceso se definirán las tareas u objetivos a alcanzar en cuatro etapas, de modo que se puedan realizar de forma progresiva a medida que la organización pueda ir avanzando en la ejecución del programa a su propio ritmo. Estas etapas están diseñadas de forma que para cada dominio y subdominio se vayan alcanzando de forma pareja y equilibrada, esto significa que se recomienda comenzar y alcanzar todas, o la mayoría, de las primeras

etapas en conjunto para luego comenzar con las segundas etapas. Las etapas mencionadas para cada uno de los procesos serán representadas en tablas de forma que sea más fácil su organización y comprensión.

En la Figura 1 se puede observar gráficamente cómo se encuentra organizado el programa con sus dominios y subdominios.

Hacerlo de esta manera garantiza cubrir los riesgos de forma abarcativa y desde diferentes perspectivas, evitando sesgos, los cuales suelen producir que una organización se encuentre en un nivel muy maduro de ciberseguridad sólo en algunos dominios. En esta situación podrían materializarse los riesgos en los dominios en los cuales no se han logrado avances o que se encuentren en un nivel muy inferior al resto.

Para la implementación de este programa se recomienda aplicar el mismo proceso del Modelado de Madurez de Seguridad de I.IoT mencionado anteriormente en la sección 2.3.9 y se encuentra ilustrado en las Figura 17 y Figura 18.

A continuación se describen y detallan cada uno de los dominios, subdominios y los procesos del programa propuesto.

3.2.1. Gobierno de la Ciberseguridad

El Gobierno de la Ciberseguridad y sus políticas influyen y dan a conocer todas las decisiones relacionadas con la seguridad, incluido cómo se priorizan los procesos. Este dominio describe a los subdominios directamente relacionados con la gobernanza, incluyendo la estrategia, la modelización de las amenazas y la evaluación de los riesgos y, por último, la gestión de la cadena de suministro y de las dependencias externas. Estos determinan la postura de seguridad de la organización y las políticas relacionadas con otras partes y el entorno externo.

3.2.1.1. Estrategia y Gobierno de la Ciberseguridad

La estrategia y el gobierno de la seguridad apoyan la estrategia de la organización, además de proporcionar seguridad y el cumplimiento de las normas, leyes y obligaciones contractuales. También apoya la protección de la reputación y la gestión de la actividad principal del negocio.

1) Gestión del Programa de Ciberseguridad

La gestión del programa de seguridad es vital para una planificación clara y para la prestación oportuna de las actividades de seguridad, el control sobre el proceso y resultados y una óptima toma de decisiones de decisiones para el cumplimiento de la seguridad.

Tabla 5

Gestión del Programa de Ciberseguridad

Etapa	Tareas
1	Documentar los aspectos relevantes tanto internos como externos para la gestión de la seguridad. Identificar la estructura de la gestión de la seguridad, las medidas que se tomarán, las responsabilidades y los métodos para comunicar esta información al personal. Coordinar y alinear funciones y responsabilidades incluyendo los roles internos y externos con experiencia en dispositivos, redes e infraestructura de I.IoT.
2	Identificar y documentar los sistemas, redes y procesos que deben ser gestionados para abordar los problemas de seguridad. Planificar los recursos para la gestión de la seguridad, la comunicación, formación y sensibilización. Crear centros de competencias para las funciones identificadas. Lograr que las partes interesadas de la empresa apoyen la seguridad e iniciativas de seguridad, entiendan sus funciones y responsabilidades. Lograr que las partes interesadas de OT aporten el punto de vista punto de vista operativo.
3	Alinear el programa de seguridad con las normas apropiadas para cumplir los requisitos reglamentarios y para lograr la coherencia en toda la organización, incluidas las filiales. Incorporar la comprensión de las normas en los programas de gestión, comunicación, formación y concienciación en materia de seguridad. Integrar los equipos en todos los centros de competencia. Realizar un análisis de los riesgos de las infraestructuras críticas y de los sectores específicos (IT y OT) para informar sobre la determinación de la tolerancia al riesgo de la organización. Garantizar que las partes interesadas de terceros (por ejemplo, proveedores, clientes, socios) comprendan sus funciones y responsabilidades.

Etapa	Tareas
4	Lograr el conocimiento de la situación mediante el seguimiento de las amenazas, los requisitos normativos y la evolución de las tecnologías a lo largo del tiempo. Establecer los plazos para las revisiones y actualizaciones periódicas de las medidas, planificar los esfuerzos y los recursos. Llevar a cabo actividades periódicas de formación, concienciación y pruebas. Ampliar los equipos integrados mediante la creación de un centro de excelencia de I.IoT y ajustar los equipos para las fases de prueba de concepto, piloto, escalado del sistema y producción.

2) Gestión del Cumplimiento

La práctica de gestión del cumplimiento es necesaria cuando se exigen requisitos estrictos de cumplimiento de las normas de seguridad de seguridad.

Tabla 6

Gestión del Cumplimiento

Etapa	Tareas
1	Identificar y supervisar los impulsores del cumplimiento general relacionado con la seguridad, incluido el cumplimiento de protocolos, normas y certificaciones. Subcontratar todas o la mayoría de las actividades relativas a mantener el sistema cumpla con las normas de seguridad.
2	Definir un plan para cumplir con los requisitos externos basados en una investigación detallada sobre el régimen de cumplimiento de la organización. Comprobar si las prácticas aplicadas son representativas a los requisitos y si hay desvíos de cumplimiento. Realizar una evaluación de cumplimiento y conformidad utilizando un equipo interno o equipo subcontratado.

Etapa	Tareas
3	Realizar las auditorías de cumplimiento y tener en cuenta las normativas de las autoridades de control para alinear los sistemas, redes, dispositivos de borde, o procesos con la apropiado requisitos. Sistemáticamente, pero independientemente, gestionar el cumplimiento de los requisitos de IT, OT e I.IoT.
4	Mantener actualizado de forma proactiva sobre los próximos cambios en los regímenes de cumplimiento y garantizar la adhesión a esos cambios antes de que entren en vigor. Automatizar y llevar a cabo de forma regular la recopilación, el análisis, el almacenamiento y la recuperación de los datos de auditoría. Mantener centralizados los datos de auditoría actuales e históricos por proyecto y permitir el acceso sólo a las personas autorizadas. Establecer un proceso de evaluación para aquellos requisitos de las autoridades reguladoras que no permitan controles automatizados mediante implementando un esquema similar de obtención y almacenamiento de los datos. Considerar IT, OT e I.IoT en forma conjunta.

3.2.1.2. Modelado de Amenazas y Evaluación de Riesgos

El subdominio de modelización de amenazas y evaluación de riesgos identifica las diferencias en configuraciones, productos, escenarios y tecnologías, y prioriza las contramedidas en consecuencia.

1) Proceso del Modelado de Amenazas

El proceso del modelado de amenazas tiene como objetivo tanto revelar los factores conocidos y específicos que pueden poner en riesgo el funcionamiento de un sistema determinado en riesgo y describir con precisión estos factores.

Tabla 7

Modelado de Amenazas

Etapa	Tareas
1	Recoger la información disponible sobre ciberseguridad, vulnerabilidades e incidentes, y reconocer los que son relevantes como amenazas.
2	Realizar una evaluación de vulnerabilidades para IT, OT e I.IoT y gestionarlas por separado. Utilizar un método generalmente aceptado de medición de evaluación de vulnerabilidades (como el Common Vulnerability Scoring System o CVSS).
3	Describir las amenazas durante el análisis utilizando clasificaciones generalmente aceptadas como CAPEC[3] u OWASP Top10[4]. Utilizar herramientas para describir e identificar las amenazas automáticamente y su posible resolución. Tratar las amenazas específicas de IT, OT e I.IoT. Considerar los resultados del modelado de amenazas y las evaluaciones de riesgos como parte de los procesos formales para abordar y prevenir los problemas identificados.
4	Validar las amenazas de seguridad en función de los objetivos establecidos según las necesidades de la organización. Basar el modelo de amenazas en el conjunto de supuestos de seguridad claramente identificados sobre el entorno del sistema (incluyendo la seguridad física), las restricciones de confianza y el comportamiento de los actores clave. Gestionar las amenazas de IT, OT e I.IoT de forma integrada. Organizar las amenazas particulares y los vectores de ataque como una estructura jerárquica coherente, incluyendo todos los problemas de seguridad identificados.

[3] CAPEC: Common Attack Pattern Enumerations and Classifications. https://capec.mitre.org/

[4] OWASP TOP 10: Open Web Application Security Project. https://owasp.org/www-project-top-ten/

2) Actitud de Riesgo

El proceso de la actitud de riesgo permite a una organización establecer una estrategia para hacer frente a los riesgos de acuerdo con la política de gestión de riesgos, incluyendo las condiciones para la aceptación, la evitación, la evaluación, mitigación y transferencia.

Tabla 8

Actitud de Riesgo

Etapa	Tareas
1	Aplicar una gestión general de riesgos para todos los tipos de riesgos de ciberseguridad, así como para otros tipos de riesgos. Opcionalmente, involucrar a terceros para realizar el análisis de riesgos.
2	Aplicar un enfoque más detallado al análisis de riesgos, evaluación y a las contramedidas concretas. Aplicar múltiples mitigaciones a cada amenaza. Mitigar las consecuencias de un ataque exitoso en cualquiera de los vectores con contramedidas. Considerar los problemas externos e internos que son relevantes para el propósito de la organización y que afectan a su capacidad para lograr los resultados previstos. Considerar los riesgos relacionados con la subcontratación, las terceras partes u otros socios en la cadena de suministro. Considerar los dispositivos en este nivel. Habilitar procedimientos para abordar los riesgos y garantizar que la organización pueda lograr sus resultados previstos; prevenir o reducir los efectos no deseados y lograr una mejora continua. Considerar IT, OT e I.IoT de forma independiente.
3	Abordar IT, OT e I.IoT por separado pero de forma sistemática. Identificar, priorizar y analizar las posibles amenazas de ciberseguridad, vulnerabilidades y consecuencias utilizando métodos aceptados. Utilizar métodos que caracterizan los riesgos cuantitativamente o cualitativamente, y se basan en la estructura como escenario o basado en activos.

Etapa	Tareas
	Hacer que los terceros formen parte del proceso.
4	Establecer un proceso continuo de gestión de riesgos que incluya las decisiones adecuadas en función de los riesgos identificados. Establecer una estrategia de gestión de riesgos e identificar el daño y su probabilidad de amenazas. Integrar IT, OT e I.IoT. Identificar los cursos de acción y respuestas alternativas, evaluarlas y determinar si son coherentes con la tolerancia al riesgo de la organización.

3.2.1.3. Cadena de Suministro y Gestión de Dependencias Externas

El subdominio de cadena de suministro y gestión de dependencias externas tienen como objetivo controlar y minimizar la exposición de un sistema a los ataques de terceros que tienen acceso privilegiado y pueden encubrir los ataques.

1) Gestión de Riesgos de la Cadena de Suministro de Productos

El proceso de gestión de riesgos en la cadena de suministro de productos aborda la necesidad evaluar la confianza en los contratistas o proveedores y comprobar la ausencia de fuentes de amenazas ocultas, garantizando la integridad de la cadena de suministro.

Tabla 9

Gestión de la Cadena de Suministro de Productos

Etapa	Tareas
1	Aplicar medidas comunes para reducir los riesgos que plantean los agentes de la cadena de suministro y terceros. Dichas medidas deben incluir al menos medidas de protección de manipulación durante el envío y almacenamiento, el control de acceso físico del personal que proporciona integración y mantenimiento, limpieza memoria y restablecimiento de fábrica del dispositivo antes de su descarte.

Etapa	Tareas
	Garantizar la autenticidad del proveedor para validar que las falsificaciones o los componentes alternativos no son sustituidos durante el envío del dispositivo. Considerar toda la cadena de suministros, empezando por medidas en el fabricante de los circuitos integrados y todo el camino incluyendo la nube.
2	Mejorar el análisis de ciertas amenazas de la cadena de suministro con el agregado de todas las fuentes de análisis de inteligencia para adaptar estrategias de adquisición, herramientas y métodos. Aplicar métodos para revisión y proteger planes de desarrollo, pruebas y documentación que sean acordes con la función del sistema o componente, su nivel de criticidad y exposición a los ataques. Aplicar las medidas en cada fase de la cadena de suministro y contrato por separado. Identificar las dependencias y las funciones críticas para la prestación de los servicios críticos. Considerar soluciones de aprovisionamiento para componentes independientes.
3	Identificar las cadenas de suministro por procesos. Implementar un conjunto de métodos para abordar el riesgo de la cadena de suministro con respecto a los sistemas informáticos, las redes y sus componentes, y para educar al personal de adquisiciones sobre las amenazas, el riesgo y los controles de seguridad necesarios. Considerar una solución integrada de aprovisionamiento de extremo a extremo. Gestionar las vulnerabilidades y los riesgos de los terceros exigiendo que los aborden. Realizar auditorías aleatorias de los proveedores para verificar su cumplimiento de las obligaciones contractuales.
4	Implementar un proceso estandarizado para abordar el riesgo de la cadena de suministro con respecto a los sistemas de información y los componentes del sistema, y para educar al personal de adquisiciones sobre las amenazas de la cadena de suministro, el riesgo y los controles de seguridad requeridos.

Etapa	Tareas
	Utilizar los procesos de adquisición y compra en una fase temprana del ciclo de vida del desarrollo del sistema para proporcionar un vehículo importante para proteger la cadena de suministro. Garantizar un proceso de verificación exhaustivo que haga que los proveedores se adhieran sistemáticamente a los requisitos de seguridad. Anticipar los riesgos de terceros y crear planes de incidentes para gestionar posibles situaciones y proporcionar redundancia. Establecer requisitos de resiliencia para los servicios críticos de terceros para todos los estados operativos (por ejemplo, operaciones normales, bajo ataque y durante la recuperación).

2) Gestión de los Servicios y Dependencias de Terceros

La práctica de gestión de los servicios y dependencia de terceros aborda la necesidad de evaluar la confianza de los socios y otras terceras partes. La capacidad de tener garantía de la confianza en los terceros requiere comprensión del negocio y de la confianza y de las posibles fuentes ocultas de amenazas.

Tabla 10

Gestión de los Servicios y Dependencias de Terceros

Etapa	Tareas
1	Exigir a todos los agentes externos, incluidos los proveedores de tecnología, los socios, los contratistas y los servicios gestionados, que cumplan con los requisitos de seguridad de acuerdo con los acuerdos establecidos. Tener en cuenta que estos acuerdos pueden realizarse de diversas maneras, esto podría ser muy básico y podría no impedir los abusos que se pueden aprovechar de las debilidades en acuerdos complejos.
2	Establecer los contratos, los acuerdos de intercambio comercial y los SLA (del inglés, Service Level Agreement) que definan los KPI (del inglés, Key Performance Indicator) y los resultados medibles y las respuestas al

Etapa	Tareas
	incumplimiento. Considerar los KPIs y los SLAs para IT, OT e I.IoT de forma independiente. Considerar los requisitos establecidos por las autoridades reguladoras como obligatorios. Proporcionar el cumplimiento de regulaciones de privacidad de los datos personales y requisitos de calidad.
3	Aplicar los acuerdos definidos que van desde un control amplio (contratos), hasta un control muy control limitado (adquirir servicios externos). Asegurar la comprensión clara de qué nivel es aceptable para la organización y apoyar este nivel con medidas a nivel organizacional. Considerar las cadenas de confianza. Tener en cuenta que la gestión de riesgos para el uso de servicios externos se comparte con terceros según los acuerdos empresariales y legales. Rastrear y notificar los incidentes de IT, OT e I.IoT con herramientas por separado. Trasladar los requisitos de calidad y el cumplimiento de regulaciones de las terceras partes.
4	Exigir una evaluación de ciberseguridad que debe ser realizada antes de la adquisición o tercerización para garantizar que no existen riesgos significativos. Considerar la permeabilidad de la confianza, y documentar y supervisar la base de la confianza. Identificar las cadenas de confianza y considerar la confianza de cada parte implicada y su impacto en el nivel de confianza de toda la cadena. Compartir la gestión del riesgo relacionado al uso de servicios de terceros con los terceros según con los acuerdos comerciales, legales y las regulaciones. Codificar el enfoque para que los requisitos y la visión completa del sistema se comprendan bien. Tratar IT, OT e I.IoT en forma conjunta.

3.2.2. Habilitación de la Ciberseguridad

El dominio de habilitación de la seguridad se refiere a la aplicación de los controles y prácticas de seguridad necesarios para crear un sistema operacional, basado en decisiones de gestión relacionadas con la política de seguridad y la necesidad de hacer frente a los riesgos del negocio utilizando los mejores medios disponibles. La política y los controles de seguridad están sujetos a revisiones y evaluaciones periódicas. El dominio de habilitación incluye la gestión de identidades y de acceso, la protección de activos y la protección de datos.

3.2.2.1. Gestión de Identidades y Accesos

El subdominio de gestión de identidades y accesos tiene como objetivo proteger la organización y controlar el uso de los recursos por parte de los usuarios identificados para reducir el riesgo de fuga de información, manipulación, robo o destrucción.

1) Establecer y Gestionar Identidades

El proceso de establecer y mantener las identidades ayuda a identificar y restringir quién puede acceder al sistema y los privilegios que se les otorgaron para acceder a los mismos.

Tabla 11

Establecer y Gestionar Identidades

Etapa	Tareas
1	Asegurar que los dispositivos más importantes en la organización puedan ser identificados y gestionados. Garantizar que aquellos que necesitan acceso puedan acceder a los activos.
2	Identificar los equipos que deben ser autorizados y proporcionar el esquema y los medios técnicos adecuados para su identificación y autentificación. Definir las funciones del personal implicado en los escenarios clave.
3	Implementar un inventario automatizado de sistemas, dispositivos e identidades. Integrar los esquemas de autenticación incluyendo múltiples factores de autenticación cuando sea apropiado.
4	Implementar una gestión de identidades unificada y automatizada que incluya todo el ciclo de vida de la identidad.

	Implementar la prueba de identidad de acuerdo con la normativa o los requisitos del sistema pertinentes. Utilizar un sistema con capacidad amplia para identificar personas, sistemas y cosas. Proporcionar llaves físicas de seguridad y un sistema PKI como fuente de confianza cuando sea necesario.

2) Control de Acceso

La implementación del proceso de control de acceso permite a una organización limitar acceso a los recursos sólo a las identidades que lo requieren y sólo al nivel específico necesario para cumplir con las necesidades de la organización.

Tabla 12

Control de Acceso

Etapa	Tareas
1	Implementar un control de acceso genérico basado en mecanismos de propósito común soportados por las aplicaciones, los servicios, los sistemas operativos y los dispositivos de red. Garantizar que estos mecanismos de propósito común proporcionen una segregación adecuada de los agentes externos e internos y limiten el acceso a los agentes externos.
2	Describir los objetivos de control de acceso para tanto para los agentes externos como para los agentes internos con sus respectivos casos de uso. Verificar que la política de control de acceso esté alineada con estos objetivos. Para minimizar la exposición y el riesgo, la base de sistemas informáticos de confianza debe ser lo más pequeña posible.
3	Asegurar que la política de control de acceso es adecuada tanto para los componentes de IT como para los componentes de OT. Definir los puntos de referencia sobre los cuales supervisar y controlar los acceso e implementar los controles requeridos.

Etapa	Tareas
	Someter a los usuarios privilegiados a una auditoría de accesos.
4	Definir e implementar prácticas de gestión y ciclo de vida de acceso que aborden el acceso a los sistemas de IT y OT, incluyendo el desaprovisionamiento una vez que los usuarios ya no requieren acceso. Garantizar la coherencia del control de acceso en todos los sistemas de la organización. Llevar a cabo de forma periódica pruebas de control de acceso.

3.2.2.2. Gestión de Activos

El subdominio de gestión de activos tiene como objetivo proteger los activos físicos y digitales. Este es un área de fuerte colaboración entre los equipos de IT y de seguridad física.

1) Gestión de Activos, Cambios y Configuraciones

El proceso de gestión de activos, cambios y configuraciones limita los tipos de cambios permitidos, cómo y cuándo se pueden hacer, los procesos de procesos de aprobación y de cómo manejar los escenarios de cambios de emergencia.

Tabla 13

Gestión de Activos, Cambios y Configuraciones

Etapa	Tareas
1	Establecer y documentar el uso de los activos críticos. Garantizar que sigan las normas de uso aceptable. Estas normas pueden abordar el manejo de dispositivos y medios de almacenamiento, restricciones de acceso, limitación de la distribución de activos a un mínimo necesario para apoyar la funcionalidad, etc.
2	Crear un inventario de activos y asignar un propietario para los activos importantes o críticos. Clasificar y etiquetar los activos físicos y de información implicados en los principales casos de uso.

Etapa	Tareas
	Desarrollar procedimientos para la manipulación, el procesamiento, el almacenamiento y la comunicación de activos de forma coherente con su clasificación. Crear estándares de configuración de sistemas, cambios y gestión de las configuraciones en los casos que sea apropiado.
3	Garantizar que las políticas de gestión de activos, cambios y configuración cubran los activos de IT y OT. Desarrollar guías para proteger los activos de software, incluida la integridad del proceso de arranque (boot), la integridad del software (por ejemplo, detección de malware), protección de la memoria y actualizaciones de seguridad. Incorporar el principio de mínima funcionalidad configurando sistemas para proporcionar sólo las capacidades esenciales.
4	Ampliar la política de gestión de activos para proporcionar una estructura de ciclo de vida para la gestión de activos de IT y OT desde la adquisición y la inscripción hasta el retiro y la eliminación. Garantizar que la política aborda tanto los componentes individuales como los sistemas completos (por ejemplo, el motor del avión y el avión completo) en todas las etapas del ciclo de vida. Implantar procesos de arranque seguro de hardware y actualizaciones seguras para garantizar la integridad del sistema.

3) Protección Física

El proceso de protección física aborda la seguridad física y la protección de los locaciones, personas y sistemas para evitar robos y garantizar el funcionamiento continuo y seguro de las implementaciones.

Tabla 14

Protección Física

Etapa	Tareas
1	Adoptar políticas de seguridad para proteger los dispositivos de daños físicos o afectación de las operaciones de forma accidental o intencional.
2	Definir zonas de confianza en las arquitecturas de sistema de IT y establecer perímetros de seguridad entre IT y OT para separar y proteger los sistemas dentro de cada zona. Utilizar carcasas a prueba de manipulaciones fuera del perímetro de seguridad.
3	Automatizar la gestión de identidad y sistemas de alerta para gestionar e informar sobre acceso físico a ubicaciones y activos. Imponer reglas de control de acceso más granulares, como basados en el horario del día. Utilizar carcasas a prueba de manipulaciones para sistemas y cosas que fueron implementados fuera del perímetro de seguridad.
4	Definir el perímetro de seguridad con claridad, con su ubicación y fortaleza en función de los activos contenidos en el perímetro y de los resultados de una evaluación de riesgos.

3.2.2.3. Protección de Datos

El subdominio de protección de datos tiene como objetivo impedir la divulgación o manipulación no autorizada de los datos, tanto para los datos almacenados, como en tránsito y en uso. Esto es importante para la seguridad, la privacidad, el cumplimiento cumplimiento de la normativa, protección legal y de la propiedad intelectual.

1) El Modelo de Ciberseguridad y la Política de Protección de Datos

El proceso del modelo de ciberseguridad y la política de seguridad para práctica de datos identifica si existen diferentes categorías de datos y cómo protegerlos, y considera los objetivos específicos y normas de protección de datos.

Tabla 15

Modelo de Ciberseguridad y Política de Protección de Datos

Etapa	Tareas
1	Aplicar una política de protección de datos basada en las leyes y reglamentos pertinentes. Abordar la seguridad de los datos en movimiento, los datos en almacenamiento y los datos en uso.
2	Ampliar la política de protección de datos para incluir la clasificación de datos, vinculando los datos a su negocio y los objetivos de seguridad dentro de diferentes entornos de IT y OT.
3	Crear una política de datos unificada para abordar los datos generados desde y procesados a través de recursos de IT y OT. Sustentar las reglas de normas de protección de datos refiriéndose a las normas, directrices y mejores prácticas.
4	Ampliar la política de protección de datos para incluir el ciclo de vida completo de los datos. Integrar la política de protección de datos con la política de gestión de cambios y configuraciones.

2) La Implementación de los Controles de Protección de Datos

El proceso de la implementación de los controles de protección de datos describe la aplicación de los mecanismos para abordar la confidencialidad, la integridad y la disponibilidad de estos.

Tabla 16

Implementación de los Controles de Protección de Datos

Etapa	Tareas
1	Utilizar los controles incorporados para cumplir los requisitos de la política de protección de datos. Emplear medidas de propósito común como el cifrado de datos en movimiento con mecanismos como cifrado mediante TLS (Transport Layer Security).
2	Evaluar la estrategia de protección de datos para subsistemas más amplios o para grupos de datos más grandes. Implementar controles de red y de aplicación pertinentes para restringir el acceso a datos, como segmentación de red, filtrado, máquinas virtuales, puertas de enlace y otras medidas para gestionar el flujo de datos.
3	Aplicar sistemáticamente los requisitos de protección de datos. Garantizar que los controles de protección de datos se eligen de acuerdo con la política y reglas de protección de datos, como las recomendadas por las mejores prácticas. Automatizar las medidas de protección en los casos posibles.
4	Garantizar que se encuentre una gestión de claves para proteger el acceso a datos encriptados. Realizar periódicamente una evaluación de los mecanismos de control de flujo de datos. Introducir mecanismos de detección que apoyen las políticas de protección de datos y controles. Establecer un mecanismo para garantizar inmutabilidad y autenticación de la fuente de los datos.

3.2.3. Endurecimiento de la Ciberseguridad

El dominio de endurecimiento se refiere a las prácticas de seguridad utilizadas durante el funcionamiento del sistema, incluyendo la gestión de vulnerabilidades y parches, el conocimiento de la situación y la respuesta a incidentes para la continuidad de las operaciones.

Este dominio incluye medidas organizativas y técnicas para evaluar, reconocer y remediar los riesgos en curso para mejorar la fiabilidad del sistema.

3.2.3.1. Gestión de las Vulnerabilidades y Parches

Las políticas y procedimientos del subdominio de gestión de vulnerabilidades y parches se utilizan para mantener sistemas componentes actualizados y menos propensos a ataques debido a las vulnerabilidades en los sistemas. El conocimiento de la situación también es necesario para mantenerse al tanto de las nuevas vulnerabilidades.

1) Evaluación de Vulnerabilidades

Este proceso ayuda a identificar las vulnerabilidades, determinar el riesgo que cada una podría representar para la organización y desarrollar un plan de plan de remediación priorizado.

Tabla 17

Evaluación de Vulnerabilidades

Etapa	Tareas
1	Designar a una persona para que evalúe las vulnerabilidades conocidas de un componente determinado. Describir de manera informal los tipos y ejemplos de fuentes de información para la evaluación.
2	Identificar los componentes críticos. Designar al personal, detallar y priorizar sus responsabilidades para la evaluación de las vulnerabilidades, y establecer procedimientos para realizar los reportes. Describir las fuentes de información obligatorias y opcionales para la evaluación.
3	Establecer un esquema de evaluación que implique un escaneo de vulnerabilidades periodico de todos los activos utilizando herramientas automatizadas y evaluaciones de terceros. Incorporar al programa de evaluación de vulnerabilidades fuentes de inteligencia de amenazas recibida desde foros y otras fuentes.

Etapa	Tareas
	Garantizar que el programa de vulnerabilidad tenga en cuenta los cambios en el inventario de la organización en casi tiempo real. Describir los tipos de vulnerabilidades, nivel de detalles en su descripción, en el reporte. Establecer un programa para mejorar la calidad de componentes durante todo el ciclo de vida, incluyendo el diseño y el desarrollo. Establecer un proceso de mejora continua del proceso de evaluación de vulnerabilidades.
4	Implementar actividades periódicas con la participación de terceras partes para descubrir las vulnerabilidades. Negociar los métodos, herramientas y priorizar las actividades en función de la exposición de los componentes a los ataques y los riesgos asociados. Revisar los resultados de terceros y del programa de gestión de vulnerabilidades para identificar mejoras de procesos estratégicos.

2) Gestión de Actualizaciones de Seguridad

El proceso de gestión de actualizaciones de seguridad define cuándo y con qué frecuencia aplicar las actualizaciones de seguridad del software, establece procedimientos de emergencia para aplicarlos y propone mitigaciones adicionales en caso de acceso restringido al sistema u otros problemas relacionados con la aplicación de las actualizaciones de seguridad.

Tabla 18

Gestión de Actualizaciones de Seguridad

Etapa	Tareas
1	Establecer las reglas para instalar actualizaciones de seguridad proporcionadas por proveedores. Utilizar las actualizaciones automáticas cuando sea posible.

Etapa	Tareas
2	Priorizar el proceso de actualización del software según los resultados del análisis de riesgos y la evaluación de vulnerabilidades. Incluir las pruebas preliminares de los parches y actualizaciones de seguridad cuando sean necesarias.
3	Establecer normas para la aplicación de actualizaciones de seguridad de manera uniforme y coherente utilizando la automatización y la gestión centralizada. Iniciar el proceso de sustitución del software pertinente por otra versión u otro software similar cuando no sea posible instalar una actualización de seguridad necesaria para disminuir los riesgos a valores aceptables.
4	Establecer y gestionar un proceso de actualizaciones de seguridad de forma continua a lo largo del tiempo con consideraciones para el ciclo de vida de los componentes de IT y OT. Examinar el software de los sistemas críticos para comprenderlo en profundidad, incluyendo las vulnerabilidades que conducen a actualizaciones de seguridad.

3.2.3.2. Concientización Situacional

El subdominio de concientización de la situación comprende técnicas y actividades organizativas y comunitarias de la organización utilizadas para lograr una comprensión del estado actual de la seguridad que permita a una organización priorizar y gestionar las amenazas con mayor eficacia.

1) Monitoreo de Seguridad

El proceso de monitoreo de seguridad se utiliza para controlar el estado del sistema, identificar anomalías y ayudar a la resolución de conflictos.

Tabla 19

Monitoreo de Seguridad

Etapa	Tareas
1	Seguir las guías generales de seguridad existentes sobre la supervisión básica de la seguridad utilizando los mecanismos existentes sin preocuparse específicamente de las particularidades del sistema específico. Asignar la responsabilidad del análisis de la seguridad y de los eventos relacionados con la seguridad al administrador del sistema u otra persona responsable del software, sistema o red.
2	Considerar los eventos causados tanto por acciones humanas (por ejemplo, acceso a los recursos críticos y gestión de credenciales) y procesos existentes (por ejemplo, actualizaciones de software, escaneos periódicos de malware). Los reportes de fallos proporcionan información sobre las fallas de los dispositivos y aplicaciones, y visibilidad de las amenazas de seguridad. Lograr el enfoque en los eventos que pueden tener un impacto más significativo en el funcionamiento normal de los sistemas, por lo que es recomendable remitir los resultados de la evaluación de riesgos. Comunicar la información sobre eventos dentro de la organización.
3	Considerar diferentes fuentes y varios sistemas avanzados adicionales de control (sistemas de detección de intrusos, SIEMs, etc.). Involucrar a personal de seguridad o terceros contratistas capacitados que rastreen eventos de seguridad y proporcionen información sobre el estado de la seguridad al personal responsable interesado. Implementar medidas de protección para la información de monitoreo, por ejemplo, con un registro seguro (almacenamiento seguro e inalterable).
4	Automatizar la mayor parte del análisis de los eventos de seguridad y realizar una revisión manual cuando corresponda. Realizar el monitoreo en varios niveles del sistema: hosts, red, equipos específicos, y podría implicar personal de seguridad o contratistas de terceros

Etapa	Tareas
	calificados (por ejemplo, en forma de un Centro de Operaciones de Seguridad [SOC]). Implementar todo el ciclo de monitoreo desde el establecimiento de indicadores de incidentes vinculados a los riesgos hasta la protección y copia de seguridad de los datos de monitoreo. Probar y mejorar continuamente el proceso de detección.

2) Concientización de la Situación e Intercambio de Información

Este proceso ayuda a las organizaciones a estar mejor preparadas para responder a las amenazas. El intercambio de información sobre amenazas mantiene los sistemas y a las personas actualizados y preparados para enfrentarlas.

Tabla 20

Concientización de la Situación e Intercambio de Información

Etapa	Tareas
1	Especificar la política de divulgación de incidentes y vulnerabilidades de acuerdo con las regulaciones y las consideraciones de intercambio de conocimientos necesarios. Compartir la información sobre incidentes de seguridad general con partes externas. Incluir en los incidentes generales de seguridad la infección por malware, el acceso no autorizado al servicio o al software, las credenciales comprometidas, el uso de equipos o medios no autorizados, etc. Incluir en las instrucciones las recomendaciones sobre los medios y proceso de la comunicación sobre los incidentes de seguridad (los destinatarios, forma de comunicación, etc.). Concientizar y comunicar los incidentes de seguridad en base a la necesidad de conocer. Mantenerse al tanto sobre las noticias de los proveedores de productos.

Etapa	Tareas
2	Analizar qué tipos de incidentes de seguridad pueden afectar especialmente al sistema o a la organización. Proporcionar instrucciones adecuadas sobre cuándo compartir la información sobre los incidentes, a quién y cómo. Los dispositivos producen informes de fallos y existe un mecanismo para compartir los registros y eventos.
3	Mantener las suscripciones a los avisos de seguridad, las listas de correo de los proveedores, las comunidades del sector para mantener el conocimiento de la situación sobre los problemas de seguridad que surgen en el sector particular o que son relevantes para las tecnologías utilizadas. Obtener información de los programas y servicios, incluidas las soluciones antimalware y otros software de seguridad que realizan un seguimiento del estado de seguridad enviando automáticamente informes sobre seguridad detectados sobre eventos de seguridad y vulnerabilidades. Los dispositivos automáticamente producen informes sobre fallas que pueden ser compartidos con fabricantes y los sistemas de gestión centralizada. Incluir en las instrucciones orientación para la configuración de los programas informáticos de monitoreo las recomendaciones sobre los medios y proceso de la comunicación (los destinatarios previstos, forma de comunicación, etc.) y la estrategia general de divulgación de las vulnerabilidades con agentes externos (por ejemplo, la divulgación responsable).
4	Compartir las vulnerabilidades de día cero con el proveedor del software o equipo e informar a las autoridades, agencias y empresas de seguridad pertinentes para permitir el trabajo conjunto para mitigar el efecto de la posible explotación futura de estas vulnerabilidades. Definir una política que describa el uso apropiado de los datos sobre incidentes de seguridad, vulnerabilidades descubiertas y prácticas aplicadas de otros participantes de la comunidad de la IoT, especificando cómo y cuándo colaborar con las autoridades reguladoras, comités y organizaciones voluntarias para

Etapa	Tareas
	proporcionar una devolución sobre la información sobre los actos normativos, directrices, normas y recomendaciones que ellos hacen. Crear un equipo de respuesta que esté preparado para abordar rápidamente los problemas que surjan.

3.2.3.3. Respuesta a Eventos e Incidentes, Continuidad de las Operaciones

El subdominio de respuesta a eventos e incidentes comprende una combinación de actividades políticas y técnicas diseñadas para permitir que una organización responda a los incidentes con rapidez y para minimizar la interrupción de la organización, permitiéndole continuar con su actividad principal.

1) Plan de Detección de Eventos y Respuesta ante Incidentes

Un plan de detección de eventos y respuesta a incidentes define qué es un evento de seguridad y cómo detectar y asignar eventos para investigación, escalarlos según sea necesario y responder adecuadamente. Debe incluir un plan de comunicación para compartir la información de forma adecuada y de manera oportuna con las partes interesadas.

Tabla 21

Plan de Detección de Eventos y Respuesta ante Incidentes

Etapa	Tareas
1	Crear una política que aborde los incidentes conocidos por tipo y personal responsable. Estos incidentes pueden incluir ataques de denegación de servicio, acceso no autorizado a redes, acceso a información protegida y privada, desfiguración de páginas web, uso indebido de servicios, etc. Basar las acciones de detección de cada tipo de incidente de seguridad en indicadores claros de violaciones de seguridad. Considerar la información sobre los flujos de información y el uso general de los componentes informáticos para el análisis de los incidentes. Definir inicialmente un plan básico de respuesta que no contemple ninguna desviación de las acciones prescritas.

Etapa	Tareas
2	Determinar qué incidentes de seguridad pueden requerir una reacción inmediata, enumerar los tipos y describir los pasos que deben darse para responder al incidente y mitigar los daños. Describir las funciones del personal y el orden de las operaciones cuando se necesita una respuesta. Emplear el análisis básico, incluido el examen manual en profundidad de los datos relacionados con el incidente para determinados casos de uso. Realizar análisis como parte de las actividades forenses. Alinear las acciones de notificación con la política de concientización de la situación. Prescribir respuestas que incluyan las acciones para la recuperación de los sistemas, la remediación y el apoyo a la continuidad de las operaciones de forma alineada con las políticas.
3	Utilizar técnicas avanzadas de monitoreo y soluciones automatizadas como el registro de uso y comportamiento de redes y registro, sistema de detección de intrusos, sistema de prevención de intrusiones y firewalls de nueva generación para la detección y análisis. Implementar notificaciones automatizadas sobre los incidentes de seguridad incluyendo toda la información relevante que debe ser entregada a los responsables para la recuperación de los sistemas, remediación y el mantenimiento continuo de las operaciones. Integrar la respuesta a incidentes con la concientización de la situación así como con la Remediación, Recuperación y Continuidad de Operaciones.
4	Considerar los síntomas secundarios de las violaciones de seguridad o del mal uso del sistema, como un tráfico inusualmente intenso o un uso elevado de la CPU, cuentas bloqueadas, archivos de registro borrados, cambios inesperados en la configuración, y correlacionar estos síntomas. Implementar un enfoque basado en la correlación de los síntomas para prevenir los incidentes.

Etapa	Tareas
	Definir con precisión la noción de evento relevante para la seguridad, que suele ser más amplia que una violación de la seguridad. Implementar la respuesta para prevenir tales eventos.

2) Remediación, Recuperación y Continuidad de Operaciones

La remediación, recuperación y continuidad de las operaciones representa una combinación de redundancias técnicas en las que el personal capacitado y la política de continuidad de las operaciones ayudan a una organización a recuperarse rápidamente de un evento para acelerar la vuelta a la normalidad.

Tabla 22

Remediación, recuperación y Continuidad de Operaciones

Etapa	Tareas
1	Identificar los componentes críticos y proporcionar instrucciones para recuperación basadas en mecanismos generales.
2	Definir una política de remediación y recuperación, establecer planes de contingencia para escenarios de casos de uso particulares. Mantener todos los sistemas de copia de seguridad al mismo nivel que los sistemas primarios. Establecer medidas para confirmar la recuperación completa de los sistemas. Considerar enfoques adicionales para la recuperación, como el uso de componentes redundantes o la recuperación de datos bajo demanda. Garantizar que los dispositivos pueden ser restaurados automáticamente a un estado seguro después de un compromiso. Garantizar que la compartimentación mediante barreras reforzadas por hardware entre los componentes de software impide que una brecha en uno de ellos se propague a los demás.

Etapa	Tareas
3	Implementar la eliminación automática del malware, restauración de los datos de las copias de seguridad de las bases de datos, eliminación sistemática de las acciones de contención temporal, reinicio de todos los sistemas y aplicaciones operativas. Definir procedimientos para la continuidad operativa. Implementar que tras la detección de un incidente de seguridad, los mecanismos secundarios de contingencia se activen inmediatamente. Apoyar la continuidad de las operaciones basándose en la observación de los usuarios (enfoque reactivo basado en anomalías de comportamiento). Hay que tener en cuenta que este enfoque puede conllevar una serie de riesgos adversos. En particular, no evita los daños al equipo primario ni otras consecuencias del incidente mientras se evita la interrupción.
4	Establecer una política de pruebas periódicas y planificadas de funcionamiento continuo de forma programada para verificar que los sistemas de copia de seguridad y de contingencia funcionarán correctamente cuando se recurra a ellos y que el sistema puede restablecerse a un estado anterior al incidente. Apoyar la continuidad de las operaciones de forma automatizada, permitiendo el uso de mecanismos y datos redundantes mientras se recibe información sobre la posible interrupción o daño de los mecanismos primarios. Garantizar que la recuperación restablece el sistema y lo hace más seguro, manteniendo las mismas capacidades operativas y protegiéndolo contra lo que causó el incidente (materialización del riesgo/amenaza, explotación de la vulnerabilidad, etc.). Establecer las políticas y tecnologías para permitir el análisis forense.

Capítulo 4 - Conclusiones

Durante la investigación llevada a cabo se identificó que las infraestructuras OT se encuentran amenazadas, principalmente, por dos situaciones que se dan simultáneamente ante la aparición de I.IoT y la convergencia IT-OT. En primer lugar, las infraestructuras OT no cuentan con un nivel de madurez de ciberseguridad, ya sea en la implementación de las tecnologías de protección, prevención y monitoreo, como tampoco en sus procesos estándares de ciberseguridad. En general la protección de las infraestructuras OT se lograba a través del aislamiento con el resto. En segundo lugar, con la implementación de I.IoT y la convergencia IT-OT, las infraestructuras OT no sólo comienzan a verse expuestas a las infraestructuras IT, sino también a Internet, lo cual conlleva la aparición de una gran cantidad de nuevos riesgos y amenazas.

En este trabajo se desarrolló un Programa de Ciberseguridad orientado a I.IoT, a través del análisis de la situación actual de la Industria 4.0, OT e I.IoT, como también los marcos de trabajo más relevantes de ciberseguridad, tanto generales como particulares, de esta industria. Para su realización se consideraron todas las amenazas y riesgos que fueron previamente presentados en investigaciones realizadas por otros autores.

La finalidad es que las organizaciones que se encuentren implementando soluciones tecnológicas de I.IoT, o que tengan pensado hacerlo en el corto o mediano plazo, puedan adoptar el programa aquí desarrollado. Se espera también que con el mismo logren una mejora en sus niveles de riesgo de una forma simple, ágil y medible, protegiendo sus activos de información e infraestructuras IT-OT convergentes.

Si bien se lograron concretar los objetivos particulares planteados mediante la investigación llevada a cabo, también se encontraron limitaciones ya que no ha sido posible realizar la verificación empírica de la hipótesis planteada. Esto fue así dado que, con el sólo hecho de presentar un Programa de Ciberseguridad orientado a I.IoT, no se reducen los riesgos ni contienen las amenazas. Para lograrlo es necesario implementar el programa y realizar las pertinentes evaluaciones de riesgo, anterior y posterior a la ejecución del mismo, por lo cual se sugiere continuar con esta etapa en un futuro trabajo.

Capítulo 5 - Líneas Futuras de Investigación

Para continuar en línea con la investigación desarrollada en este trabajo se considera necesario realizar una intervención de campo del Programa de Ciberseguridad orientado a I.IoT. Con esto se espera obtener la suficiente información para poder verificar la hipótesis planteada, como también comprobar el funcionamiento del mismo y obtener métricas de eficacia y eficiencia para poder realizar los ajustes requeridos.

Algunos requisitos identificados para realizar en esta intervención de campo son: análisis de riesgos del entorno OT en general y de los dispositivos I.IoT en particular, tanto de forma previa como posterior a la ejecución del programa. También se sugiere realizar un análisis de riesgos en puntos intermedios o en la finalización de la implementación de cada etapa, con el fin de monitorear la evolución de los riesgos detectados con la mayor frecuencia posible.

Acrónimos

3D	***3 Dimensions / 3 Dimensiones***
4G	***4th Generation / 4ta Generación***
5G	***5th Generation / 5ta Generación***
AI	***Artificial Intelligence / Inteligencia Artificial***
CAPEC	***Common Attack Pattern Enumeration and Classification***
CISO	***Chief Information Security Officer / Oficial en Jefe de Seguridad de la Información***
CTO	***Chief Technical Officer / Oficial en Jefe de Tecnología***
CVSS	***Common Vulnerability Scoring System***
DCS	***Distributed Control System / Sistemas de Control Distribuido***
DDoS	***Distributed Denial of Service / Denegación de Servicio Distribuida***
DL	***Deep Learning / Aprendizaje Profundo***
DMZ	***Demilitarized Zone / Zona Desmilitarizada***
DNS	***Domain Name Service / Servicio de Nombres de Dominio***
DoS	***Denial of Service / Denegación de Servicio***
HMI	***Human-Machine Interface / Interfaz Hombre-Máquina***
IT	***Information Technology / Tecnología de la Información***
ICS	***Industrial Control System / Sistema de Control Industrial***
ICS-CERT	***Industrial Control Systems - Cyber Emergency Response Team / Equipo de Respuesta ante Ciber Emergencias - Sistemas de Control Industrial***
IISF	***Industrial Internet Security Framework / Marco de Seguridad de la Internet Industrial***
I.IoT	***Industrial Internet of Things / Internet de las Cosas Industriales***
IoP	***Internet of People / Internet de las Personas***
IoT	***Internet of Thing / Internet de las Cosas***
KPI	***Key Performance Indicator***
M2M	***Machine to Machine Interface / Interface Máquina-Máquina***
MitM	***Man in the Middle / Hombre en el medio***
ML	***Machine Learning / Aprendizaje Automático***
MOS	***Metal Oxide Semiconductor / Semiconductor Metal Óxido***
MTU	***Master Terminal Unit / Unidades terminales Maestro***

NIST CSF	***National Institute of Standards and Technology - Cyber Security Framework / Marco de Ciberseguridad del Instituto Nacional de Tecnología y Estándares***
OTP	***One Time Password / Contraseña de Un solo Uso***
OT	***Operational Technology - Tecnología Operacional***
OWASP	***Open Web Application Security Project***
PLC	***Programmable Logical Controller - Controlador Lógico Programable***
PKI	***Public Key Infrastructure / Infraestructura de Clave Pública***
PROFIBUS	***Process Field Bus / Bus de Campo de Proceso***
ROI	***Return of Investment / Retorno de la Inversión***
RTU	***Remote Terminal Unit / Unidad Terminal Remota***
SCADA	***Supervisory Control And Data Acquisition / Supervisión, Control y Adquisición de Datos***
SIEM	***Security Incident and Event Management***
SOC	***Security Operations Center / Centro de Operaciones de Seguridad***
SLA	***Service Level Agreement***
TLS	***Transport Layer Security / Seguridad de Capa de Transporte***
VAR	***Virtual and Augmented Reality / Realidad Virtual y Aumentada***
VR	***Virtual Reality / Realidad Virtual***
WAAM	***Wire Arc Additive Manufacturing / Fabricación Aditiva por Arco de Alambre***
WAF	***Web Application Firewall / Firewall de Aplicación Web***
VM	***Virtual Machine / Máquina Virtual***

Referencias

Abramowski, T. (2013, Septiembre). Application of artificial intelligence methods to preliminary design of ships and ship performance optimization. *Naval Engineers Journal*, *125*(3), 101-112. https://www.researchgate.net/publication/259361068_Application_of_Artificial_Intelligence_Methods_to_Preliminary_Design_of_Ships_and_Ship_Performance_Optimization

Coolfire Solutions. (2019, April 12). *What is the Difference Between IT and OT?* Coolfire Solutions. https://www.coolfiresolutions.com/blog/difference-between-it-ot/

Coolfire Solutions. (2019, May 10). *Mr. CTO Tear Down This Wall: Ushering In a New Era of Industrial IT/OT Convergence*. Coolfire Solutions. https://www.coolfiresolutions.com/blog/it-ot-convergence/

Costa, M., Aguiar Lima, L. M., Schaefer, J., & Baierle, I. C. (2019, Septiembre). Industry 4.0 technologies basic network identification. *Scientometrics*, *121*(2), 977-994. https://www.researchgate.net/publication/335663787_Industry_40_technologies_basic_network_identification

Cybersecurity & Infrastructure Security Agency. (2016, Septiembre). *Recommended Practice: Defense in Depth*. CISA. https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

da Rosa Righi, R., Alberti, A. M., & Singh, M. (2020). *Blockchain Technology for Industry 4.0: Secure, Decentralized, Distributed and Trusted Industry Environment*. Springer. 10.1007/978-981-15-1137-0

Desjardins, J., & Ali, A. (2018, January 9). *Timeline: The History of the Industrial Internet of Things*. Visual Capitalist. https://www.visualcapitalist.com/timeline-industrial-internet-things/

European Commission. (2018, Abril 25). *Artificial Intelligence for Europe*. Communication Artificial Intelligence for Europe. https://digital-strategy.ec.europa.eu/en/library/communication-artificial-intelligence-europe

Fraga-Lamas, P., Blanco-Novoa, Ó., Fernández-Caramés, T. M., & Vilar-Montesinos, M. (2018, Febrero). A Review on Industrial Augmented Reality Systems for the Industry 4.0 Shipyard. *IEEE Access*, *6*(2018), 1-18. https://www.researchgate.net/publication/323323793_A_Review_on_Industrial_Augmented_Reality_Systems_for_the_Industry_40_Shipyard

Ganzer, M. (2019, December 23). *What is the NIST Cybersecurity Framework?* Verve Industrial. https://verveindustrial.com/resources/blog/what-is-the-nist-cybersecurity-framework/

Gartner. (2019). *Magic Quadrant for Industrial IoT Platforms*. Gartner (2019) Magic Quadrant for Industrial IoT Platforms. https://www.gartner.com/

Gomes da Costa, T., Lisboa, I., & Teixeira, N. M. (2021). *Handbook of Research on Reinventing Economies and Organizations Following a Global Health Crisis*. IGI Global. 10.4018/978-1-7998-6926-9.ch004

Gomez, A., Dopico, M., Garcia, N., & De la Fuente, D. (2016, Julio 1). *A Vision of Industry 4.0 from an Artificial Intelligence*. International Conference on Artificial Intelligence. https://www.researchgate.net/publication/305073161_A_Vision_of_Industry_40_from_an_Artificial_Intelligence

Heymsfeld, R. (2018, August 4). *Confidentiality, Integrity and Availability - The CIA Triad*. CertMike. https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

Huq, N. (2016, 04 16). *Cyber Threats to the Mining Industry*. Trend Micro. https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-cyber-threats-to-the-mining-industry.pdf

IBM. (2020, 2 6). *La Carrera Mundial por la AI*. El 82% de las empresas españolas explora ya el uso de la inteligencia artificial, según un estudio de IBM. https://es.newsroom.ibm.com/2020-02-06-El-82-de-las-empresas-espanolas-explora-ya-el-uso-de-la-inteligencia-artificial-segun-un-estudio-de-IBM

IIoT World. (2018, Mayo 18). *Report on State of IIoT Adoption and Maturity in Three Industries*. IIoT World. https://iiot-world.com/connected-industry/report-on-state-of-iiot-adoption-and-maturity-in-three-industries/

Industrial Internet Consortium. (2016, Septiembre 26). *Industrial Internet of Things Volume G4: Security Framework*. Industrial Internet of Things Volume G4: Security Framework. https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Industrial Internet Consortium. (2020, Mayo 05). *IoT Security Maturity Model | Industry IoT Consortium*. Industrial Internet Consortium. https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

International Organization for Standardization. (2013). *ISO/IEC 27001 — Information security management*. ISO. https://www.iso.org/isoiec-27001-information-security.html

i-SCOOP. (2019, Julio 26). *Utility industrial control systems: the top six utility ICS security weaknesses*. i-SCOOP. https://www.i-scoop.eu/utility-industrial-control-systems-utility-ics-security-weaknesses/

i-SCOOP. (2021, Septiembre 09). *Operational technology (OT) - definitions and differences with IT*. i-SCOOP. https://www.i-scoop.eu/industry-4-0/operational-technology-ot/

Iscrupe, L. (2020, July 17). *Everything You Need to Know About 5G Technology*. Allconnect.com. https://www.allconnect.com/blog/5g-is-coming-what-to-know-about-the-tech-that-will-change-everything

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021, 08 12). Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain: Research and Applications*, *2*(1), 30. https://www.sciencedirect.com/science/article/pii/S2096720921000221

Kagermann, H., Wahlster, W., & Helbig, J. (2013, Abril). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

Kaspersky. (2021, Agosto 23). *What is Cyber Security? | Definition, Types, and User Protection*. Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Khan, R., Maynard, P., Mclaughlin, K., & Laverty, D. (2016, Octubre). Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. *Conference: 4th International Symposium for ICS & SCADA Cyber Security Research*. https://www.researchgate.net/publication/316060984_Threat_Analysis_of_BlackEnergy_Malware_for_Synchrophasor_based_Real-time_Control_and_Monitoring_in_Smart_Grid

Knezović, N., & Topić, A. (2018, Mayo 11). *Wire and Arc Additive Manufacturing (WAAM) – A New Advance in Manufacturing*. New Technologies, Development and Application. https://www.researchgate.net/publication/325092297_Wire_and_Arc_Additive_Manufacturing_WAAM_-_A_New_Advance_in_Manufacturing

Lee, J., Singh, J., Davari, H., & Pandhare, V. (2018, Septiembre 10). Industrial Artificial Intelligence for industry 4.0-based manufacturing systems. *Manufacturing Letters*, *18*(.), 20-23. https://www.researchgate.net/publication/327557176_Industrial_Artificial_Intelligence_for_Industry_40-based_Manufacturing_Systems

Lopes de Miranda, H., de Albuquerque Bezerra, N. R., Bezerra, M., & Rodrigues Farias Filho, J. (2017, Diciembre). The internet of things sensors technologies and their applications for complex engineering projects: A digital construction site framework. *Brazilian Journal of Operations & Production Management*, *14*(4), 567-576. https://www.researchgate.net/publication/321694673_The_internet_of_things_sensors_technologies_and_their_applications_for_complex_engineering_projects_a_digital_construction_site_framework

The Medical Futurist. (2019, May 4). *5G In Healthcare: Boosting Remote Brain Surgeries, Connected Health, Or Medical VR*. The Medical Futurist. https://medicalfuturist.com/5g-in-healthcare-boosting-telehealth-vr-connected-health/

Moreno Nieto, D., Molina, S. I., & Casal López, V. (2018, Julio). Large-format polymeric pellet-based additive manufacturing for the naval industry. *Additive Manufacturing*, *23*(.), 79-85. https://www.researchgate.net/publication/326614137_Large-format_Polymeric_Pellet-Based_Additive_Manufacturing_for_the_Naval_Industry

Mourtzis, D., Doukas, M., & Bernidaki, D. (2014, Diciembre 10). Simulation in manufacturing: Review and challenges. *Procedia CIRP*, *25*(8th International Conference on Digital Enterprise Technology - DET 2014 Disruptive Innovation in Manufacturing Engineering towards the 4th Industrial Revolution), 213-229. https://doi.org/10.1016/j.procir.2014.10.032

Palavicini, G., Bryan, J., Sheets, E., Kline, M., & San Miguel, J. (2017, Enero). Towards Firmware Analysis of Industrial Internet of Things (IIoT) - Applying Symbolic Analysis to IIoT Firmware Vetting. *Special Session on Innovative CyberSecurity and Privacy for Internet of Things: Strategies, Technologies, and Implementations*. 10.5220/0006393704700477

Panchal, A., Khadse, V., & Mahalle, P. (2019, Noviembre). Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures. 10.1109/GCWCN.2018.8668630

Papp, D., Ma, Z., & Buttyan, L. (2015, Julio). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. *2015 13th Annual Conference on Privacy, Security and Trust (PST)*. 10.1109/PST.2015.7232966

Qualcomm. (2021). *What is 5G | Everything You Need to Know About 5G | 5G FAQ*. Qualcomm. https://www.qualcomm.com/5g/what-is-5g

Roldán, J. J., Martín-Barrio, A., Peña-Tapia, E., & Crespo, E. (2019, Octubre). A training system for Industry 4.0 operators in complex assemblies based on virtual reality and process mining. *Robotics and Computer-Integrated Manufacturing*, *59*(2019), 305-316. https://doi.org/10.1016/j.rcim.2019.05.004

Ross, A. (2019, June 11). *Why 5G is the heart of Industry 4.0*. Information Age. https://www.information-age.com/5g-is-the-heart-of-industry-4-0-123483152/

Shakarian, P. (2012). Stuxnet: Revolución de Ciberguerra en los Asuntos Militares. *Air and Space Power Journal*. https://www.researchgate.net/publication/230898141_Stuxnet_Revolucion_de_Ciberguerra_en_los_Asuntos_Militares

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, C. (2009). AVOIDIT: A Cyber Attack Taxonomy. https://www.researchgate.net/publication/229020163_AVOIDIT_A_Cyber_Attack_Taxonomy

Subic, A., Swinburne University of Technology, Capgemini, Xiang, Y., Pai, S., & de La Serve, E. (2018, 05 10). *Blockchain and Industry 4.0: Why Blockchain is at the heart of the Fourth Industrial Revolution and Digital Economy?* Capgemini. https://www.capgemini.com/au-en/wp-content/uploads/sites/9/2018/10/Blockchain-and-Industry-4.0.pdf

T4. (2020, April 30). *Industrial IoT Market Size (IIoT) | T4*. t4.ai. https://www.t4.ai/industry/industrial-iot-market-size-iiot

Tenable. (2021). *Tenable.ot Industrial Cybersecurity eBook*. Tenable. https://www.tenable.com/industrial-cybersecurity-ebook

Trend Micro. (2016, August 3). *Securing ICS Environments in a Connected World - Security News*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/securing-ics-environments-in-a-connected-world

Trend Micro. (2019). *Industrial Control System - Definition*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/definition/industrial-control-system

Trend Micro. (2019, Abril 3). *Security in the Era of Industry 4.0: Dealing With Threats to Smart Manufacturing Environments - Security News*. Trend Micro.

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/security-in-the-era-of-industry-4-dealing-with-threats-to-smart-manufacturing-environments

ur Rehman, M. H., Salah, K., Yaqoob, I., & Imran, M. (2019, Abril). The Role of Big Data Analytics in Industrial Internet of Things. *Future Generation Computer Systems*, *99*(.), 247-259. https://www.researchgate.net/publication/332289804_The_Role_of_Big_Data_Analytics_in_Industrial_Internet_of_Things

Verve. (2021, Julio 09). *The Ultimate Guide to Understanding OT Security*. What is OT security, how does it work, and where should you start when building a robust cyber security program? https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security

Wahlster, W., Kagermann, H., & Lukas, W. (2021, April 22). *Ten Years of INDUSTRIE 4.0 – Germany Driving Industrial AI as the Means to Future Value Creation*. Deutsches Forschungszentrum für Künstliche Intelligenz. https://www.dfki.de/en/web/news/ten-years-of-industrie-4-0-interview-wolfgang-wahlster-cea-dfki/

Wu, M., & Moon, Y. (2017, Noviembre). Taxonomy of Cross-Domain Attacks on CyberManufacturing System. *Procedia Computer Science*, *114*(2017), 367-374. https://doi.org/10.1016/j.procs.2017.09.050.

Yao, X., Lin, Y., Yu, H., Zhou, J., Li, Y., & Liu, Y. (2017, Diciembre 28). Smart manufacturing based on cyber-physical systems and beyond. *Journal of Intelligent Manufacturing*, *30*(8), 751-760. https://www.researchgate.net/publication/322112340_Smart_manufacturing_based_on_cyber-physical_systems_and_beyond