Convergencia entre Tecnologías de Información y Tecnologías de Operación y su impacto en la Seguridad de la Información.

Autor: Romero Federico Pablo

Tutoría técnica: Profesor Kamlofsky Jorge

Profesora de Trabajo Final de Carrera: Dra. Marcela Samela

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

- Julio de 2021 -

Resumen

La integración entre la tecnología operacional y la tecnología de la información es un paso fundamental para las industrias y las infraestructuras críticas en el contexto de un mundo hiperconectado**.** Las empresas al dar este paso, no tuvieron en cuenta los riesgos de seguridad al que se exponen. Existen numerosas propuestas para abordar los problemas de seguridad, pero no hay documentación que exponga los controles que mitiguen los nuevos riesgos.

En esta investigación, se analizó la convergencia entre la tecnología operacional y la tecnología de la información, con la finalidad de identificar los nuevos riesgos y vulnerabilidades de la seguridad de la información. Por esta razón, se estudió la bibliografía correspondiente a la temática, estándares internacionales e incidentes de seguridad reportados. Se lograron identificar los nuevos riesgos de seguridad a los que se exponen los sistemas de control industrial.

Adicionalmente, se propone una serie de recomendaciones para mitigar los riesgos y reducir la brecha de seguridad, con el fin de lograr que estas tecnologías convivan con niveles de seguridad aceptables, sin comprometer la operación de las empresas.

Palabras Clave: infraestructuras críticas, redes industriales, seguridad, seguridad de la información, sistemas SCADA, tecnología de la información, tecnología operacional

Abstract

In a hyperconnected world, the integration between the operational technology and the information technology is an essential step for industries and critical infrastructures. The companies didn´t take in account the security risk that are expose. Despite of exists numerouses proposals for embrace the security problem, there is not control documentation which expose way to mitigate the new security risk.

This investigation analyzes the convergence between operational technology and information security with the propose of identify new risks and security vulnerabilities.

For this reason, it studies the different bibliographies, international standard, and the security incident that was reported. identifying new security risk that industrial control system is exposed.

Additionally, it proposed several recommendations in order to mitigate risks and reduce the security benchmark, with the objective of this technologies coexist with acceptable security level without jeopardize the company operation.

Keywords: critical infrastructure, industrial networks, information security, information technology, operation technology, SCADA systems, security

Agradecimientos

En primer lugar, le agradezco a mi familia por acompañarme en este proceso de formación profesional.

Agradezco a todas las personas que me ayudaron con el trabajo de investigación, compañeros de estudio, compañeros de trabajo y amigos, quienes invirtieron su tiempo para aconsejarme con ideas para mejorarlo.

Por último, agradezco a la Universidad Abierta Interamericana y a cada uno de los profesores que supieron transmitir su vocación y conocimiento. En particular agradezco a Jorge Kamlofsky, mi tutor, quien me ayudo en todo el trabajo orientándome con detalles, compartiendo información muy enriquecedora y siempre con un espíritu de mejora continua.

Acrónimos

IT	Information Technology
IIoT	Industrial Internet of Thing´s
OT	Operation Technology
ICS	Industrial Control System
HMI	Human Machine Interface
DCS	Distributed Control System
RTU	Remote Terminal Unit
MTU	Master Terminal Unit
PLC	Programmable Logic Controller
IP	Internet Protocol
FTP	File Transfer Protocol
DEC	Digital Equipment Corporoation
PaaS	Plataform as a Service
IaaS	Infraestructure as a Service
SaaS	Service as a Service
MES	Manufacturing Execution System
SCADA	Supervisory Control and Data Acquisition
IEC	International Electrotechnical Commission
IED	Dispositivos electrónicos inteligentes.
VCL	Virus Creation Laboratory
ICSA	Asociación Internacional de Seguridad Informática
ISO	International Organization for Standardization
SGSI	Sistemas de Gestión de Seguridad Informática
ISA	International Society of Automation
ERP	Enterprise Resource Planning
BI	Business Intelligence
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
SEI	Sowtware Engineering Institue

Tabla de contenido

Lista de figuras

Lista de tablas

Capítulo 1 - Introducción

1.1 Justificación del Tema

Desde 1970 las empresas de diversas industrias utilizan dos tipos de tecnologías la operacional y la de información. Estas fueron creadas y desarrolladas con diferentes objetivos y finalidad. (Basco et al. 2018)

A partir de 1990 estas dos tecnologías fueron convergiendo de forma paulatina conformando una arquitectura que en la actualidad se encuentra aceptada. La cuarta revolución industrial produce una disminución de la brecha entre las redes corporativas y las redes industriales (las máquinas, camiones o robots que poseen las industrias, son capaces de integrarse con sistemas de información). (Basco et al. 2018) Estas se conectan para la explotación de datos utilizando herramientas de big data o para realizar un análisis predictivo por medio de un algoritmo de machine learning, con el fin de realizarle mantenimiento a las máquinas antes mencionadas.

Tanto la tecnología operacional como la tecnología de la información se enfrentan a nuevos riesgos de seguridad que, al no ser mitigados de forma oportuna, podrían provocar grandes pérdidas económicas en las organizaciones como así también pérdidas humanas. Las antiguas redes industriales cerradas, se fueron transformando en hiper conectadas. A medida que evolucionaron también lo hicieron las modalidades de ataques informáticos, apoyándose en las virtudes de la tecnología.

En el presente trabajo, se realiza un análisis detallado de las tecnologías operativas, las tecnologías de la información y la seguridad informática. En lo que respecta a la convergencia de estas dos tecnologías, hay múltiples trabajos y estándares que abordan el tema, pero con el correr de los años estos quedan desactualizados sin aportar controles que mitiguen los nuevos riesgos.

Los riesgos de ciberseguridad son relevantes para las organizaciones, y como evidencia de estos, el Ranking Allianz Barometer 2020 (Allianz - Ranking Allianz Barometer 2020), que se encargan de medir el riesgo en las organizaciones, posiciona primero en su ranking a los incidentes de ciberseguridad.

En conclusión, se espera, de los resultados obtenidos poder dar visibilidad de los nuevos riesgos de seguridad y sus controles mitigantes. Evitar que se materialicen los potenciales riesgos con el fin de que se tomen las decisiones adecuadas basadas en los estándares internacionales, los antecedentes de incidentes de seguridad reportados y los datos relevados de la situación particular.

1.2 Hipótesis

Existe una relación directa entre el aumento de los riesgos tecnológicos sobre las redes industriales y su integración con las tecnologías de información.

1.3 Objetivo General

Analizar la problemática que afrontan las distintas organizaciones para interconectar los sistemas industriales OT y los sistemas corporativos IT.

1.4 Objetivos Particulares

Exponer los riesgos que deben asumir las organizaciones al interconectar los sistemas industriales OT y los sistemas corporativos IT, partiendo de la seguridad de la información frente a ataques cibernéticos.

Conocer los incidentes de seguridad con impacto significativo que tuvieron lugar en la última década.

Comparar los sistemas de control industrial y sistemas IT tradicionales.

1.5 Metodología de Investigación

Para el desarrollo de esta investigación se empleará la metodología de investigación cualitativa, en donde se realizará una valoración de la documentación recolectada en base a su año de publicación, tema abordado, y el tipo de documento.

La documentación recolectada es obtenida a través de libros, estándares internacionales reconocidos mundialmente, consultoras reconocidas en el ámbito de la tecnología de la información y sitios web oficiales de empresas dedicadas a la seguridad informática.

Capítulo 2 – Marco teórico

2.1 Tecnologías de la Información

La tecnología de la información involucra al uso de redes de computadoras, software, hardware, personas que poseen conocimiento técnico e internet. (Christensson, P. 2006) Con respecto al ámbito laboral, los puestos de trabajo de IT incluyen programación informática, administración de redes, ingeniería informática, desarrollo web, soporte técnico y muchas otras ocupaciones relacionadas.

La tecnología de la información forma parte de la vida cotidiana, permite ponernos en contacto mediante la telecomunicación con otra persona, desarrollar modelos matemáticos de aprendizaje supervisado y no supervisado, etc. y constantemente desarrolla nuevas funcionalidades. (Cobo, 2009)

2.1.1 Evolución de la Tecnología en el ámbito industrial.

La tecnología ha evolucionado a lo largo de la historia y el ser humano la supo utilizar en función de las necesidades que se le presentaban.

En el presente trabajo, abordaremos los hitos tecnológicos de las revoluciones industriales.

La primera revolución industrial tuvo comienzos en el siglo XVIII y se desarrolló a lo largo de todo el siglo XIX. Lo más importante de esta revolución es que se introdujeron elementos mecánicos que facilitarían las tareas de producción, mediante el uso de la energía hidráulica, de vapor o herramientas para máquinas. (Basco et al. 2018)

La segunda revolución industrial tuvo lugar a finales del siglo XIX, momento en el que comenzó a utilizarse la electricidad en la producción y se introdujo la fabricación en masa. (Sanchez, 2018)

La tercera revolución industrial o revolución digital inició aproximadamente en 1970, cuando comenzó a utilizarse la electrónica y las tecnologías de la información, con el objetivo de poder llegar a automatizar tareas de producción. (Cantor, 1994)

La cuarta y última revolución industrial, que comenzó en el año 2011 y está teniendo lugar en la actualidad, se centra en los sistemas ciber físicos, la robótica, internet de las cosas, internet como servicio y fábricas inteligentes. (Basco et al. 2018)

En la Figura 1 obtenida de [Industry 4.0 – new era of manufacturing] se presenta de manera gráfica el desarrollo de revoluciones industriales a lo largo del tiempo, así como las características claves de cada una de ellas.

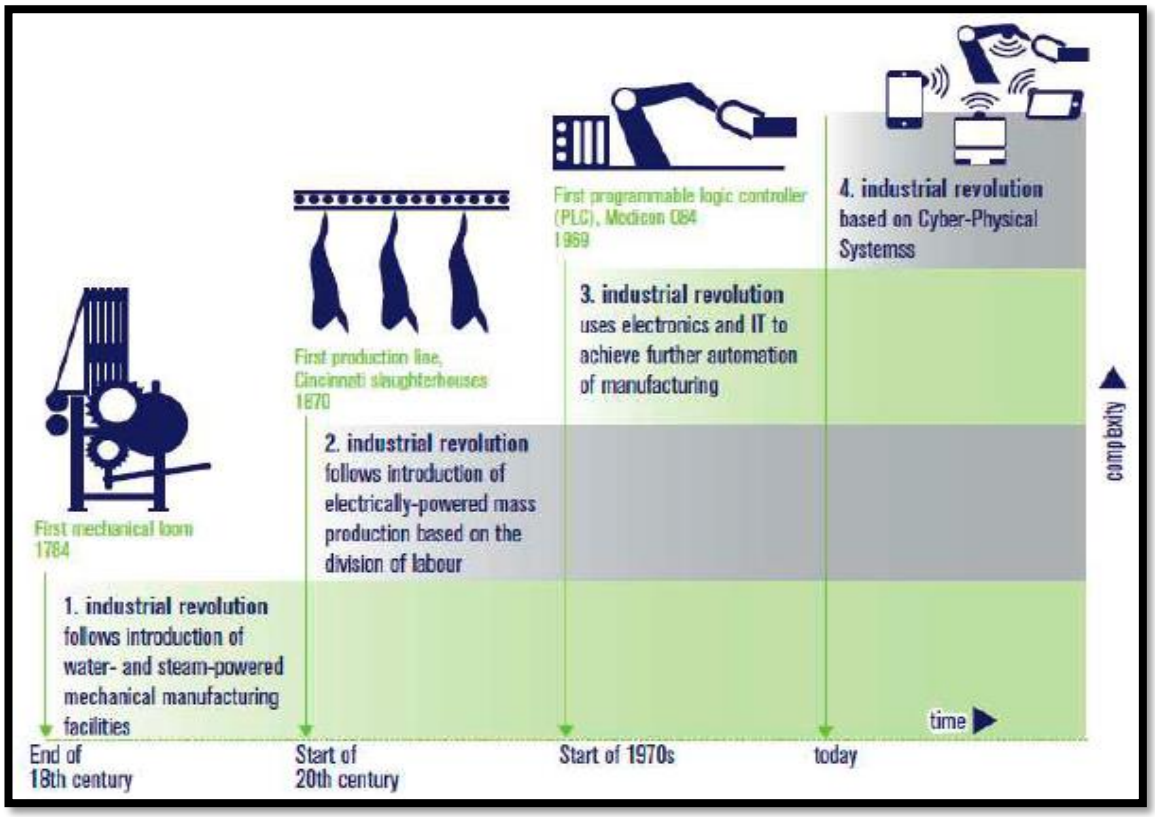

Figura 1. Evolución de la industria y la tecnología a lo largo del tiempo. Industry 4.0 – new era of manufacturing.

2.1.2 Evolución de la Infraestructura de IT

La infraestructura de IT en las organizaciones fue evolucionando durante los últimos cincuenta años. Laudon K. C. y Laudon J.P. (2012) en su libro "Sistemas de Información General", identificaron cinco etapas, cada una de estas representa una configuración diferente en cuanto a la capacidad de procesamiento y a los componentes de infraestructura. Se abordará en el presente las configuraciones típicas que caracterizaron a las distintas evoluciones.

Etapa 1: Mainframe y minicomputadoras.

Los Mainframe se comenzaron a comercializar en 1959, en 1965 esta computadora llegó a su cumbre cuando fue comercializada por IBM como "Serie IBM 360", estas fueron sustituidas de forma paulatina con la llegada al mercado de las minicomputadoras. (Laudon K. C. y Laudon J.P, 2012) Las minicomputadoras tenían una máquina mucho más poderosa a un menor costo que los Mainframe de IBM.

Etapa 2: Computadora personal.

Comienza con la comercialización de las computadoras personales de IBM en 1981, esta fue la primera máquina que se adaptó de forma extendida al público en general. (Laudon K. C. y Laudon J.P, 2012) Las máquinas se llamaban Wintel PC debido a que

tenían un sistema operativo Windows con un microprocesador Intel. En la actualidad, un gran porcentaje de las computadoras del mundo utiliza el estándar Wintel.

Etapa 3: Arquitectura cliente-servidor.

Esta etapa comienza en el año 1983, en donde las computadoras de escritorio o notebook llamadas clientes, se conectan por medio de una red a una máquina con un gran poder de procesamiento llamado servidor, los cuales proveen a los clientes servicios y herramientas. (Laudon K. C. y Laudon J.P, 2012) En la mayoría de las organizaciones se puede encontrar un esquema de cliente/servidor, pero multinivel llamado N-Niveles, en donde se encuentra por ejemplo un servidor web en un primer nivel, el cual otorga servicios a una página web. El servidor web se encarga de almacenar y gestionar el contenido de la página web que almacena.

Etapa 4: Computación empresarial.

En 1992 las empresas tenían un gran problema con las incompatibilidades entre distintos dispositivos que existían en el mercado, por lo que recurren a estándares de redes y herramientas, con el fin de poder integrar las redes y aplicaciones de toda la empresa. (Laudon K. C. y Laudon J.P, 2012) Se afianza internet y las empresas comienzan a utilizar el protocolo (TCP/IP) – "Protocolo de control de transmisión/Protocolo Internet", el cual les permitía conectar distintas redes.

Etapa 5: Computación en la nube y móvil.

En el año 2000, apalancados por el poder de ancho de banda de internet, se impulsa al modelo Cliente/Servidor hacia lo que hoy conocemos como "Cloud Computing". (Laudon K. C. y Laudon J.P, 2012) Cloud computing es un modelo, que consiste en proveer acceso a recursos informáticos (computadoras, almacenamiento, aplicaciones y servicios) a través de Internet. (NIST 800-145, 2011) Es posible el acceso a estas "nubes" de recursos informáticos, según la necesidad de cada usuario, desde cualquier ubicación y desde cualquier dispositivo que tenga acceso a Internet. En la actualidad, la computación en la nube es de uso común en la mayoría de las corporaciones.

2.1.3 Cloud Computing

El cloud computing es una de las opciones a tener en cuenta a la hora de externalizar servicios de infraestructura. Este modelo ofrece múltiples ventajas que resultan atractivas para las organizaciones que buscan reducir sus costos. La contratación de estos servicios cambia el paradigma de administración de la infraestructura y genera nuevos riesgos.

Esta sección tiene como objetivo comprender el funcionamiento del cloud computing y resaltar sus principales características. Según el estándar NIST, se define a cloud computing de la siguiente forma:

> La computación en la nube es un modelo para permitir el acceso de red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción del proveedor de servicios. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación. (NIST 800-145, 2011, p. 2)

Bajo el concepto de cloud computing, el estándar NIST 800-145 (2011), identifica las siguientes características esenciales:

Autoservicio bajo demanda: las personas pueden obtener herramientas informáticas o almacenamiento de red de forma autogestionada. (p.2)

Acceso ubicuo a la red: las personas pueden acceder a la red "nube" desde cualquier dispositivo con acceso a Internet. (p.2)

Agrupamiento de recursos sin importar la ubicación: los recursos informáticos son agrupados para dar servicio a varios usuarios. (p.2)

Elasticidad rápida: los recursos se pueden suministrar, incrementar o reducir con rapidez para satisfacer la demanda de los usuarios, la cual puede ser cambiante según su necesidad. (p.2)

Servicio medido: el importe que deberá abonar el usuario por los recursos de la nube se basa en la cantidad de recursos utilizados. (p.2)

Modelos de servicio Cloud:

La NIST define en el estándar 800-145 (2011) tres modalidades para que los proveedores puedan ofrecer servicios en la nube, el criterio hace referencia al nivel de abstracción del servicio ofrecido por el proveedor:

Software como servicio (SaaS): Se accede a las aplicaciones desde distintos dispositivos, los cuales deben estar conectados a Internet. El servicio se utiliza a través de un navegador web. La responsabilidad de gestionar y controlar la infraestructura de la nube, incluida la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades de las aplicaciones individuales, es responsabilidad del proveedor que se contrate. El usuario puede realizar algunas configuraciones específicas de la aplicación.

Un ejemplo de este servicio es el correo electrónico como Hotmail, que son basados en web. (p.2)

Plataforma como servicio (PaaS): En esta modalidad se le proporciona al cliente la capacidad de implementar en la infraestructura de la nube, aplicaciones creadas o adquiridas por el cliente. Estas pueden ser creadas utilizando un lenguaje de programación, servicios, herramientas y bibliotecas que son compatibles con el proveedor de nube. La responsabilidad de controlar y administrar la infraestructura es del proveedor. El cliente solo tiene control sobre las aplicaciones que implementa y las configuraciones sobre dicho entorno, en donde se aloja la aplicación. (p.2)

Infraestructura como servicio (IaaS): En la modalidad IaaS se aprovisiona al cliente de almacenamiento, redes, procesamiento y otros recursos informáticos fundamentales donde el cliente puede implementar y ejecutar software a demanda, que puede incluir sistemas operativos y aplicaciones. La responsabilidad de controlar y administrar la infraestructura es del proveedor. El cliente tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente un control limitado de componentes de red que pueden ser los firewalls. (p.3)

Estos modelos ayudan a delimitar la responsabilidad que tienen el cliente y el proveedor sobre el servicio, mientras más control tenga una de las partes, menor control tendrá la otra y viceversa. La seguridad informática es un factor a tener en cuenta al momento de contratar un servicio de nube y dependiendo del tipo de necesidad que tenga el cliente, este factor se convierte en crítico. La adopción de los servicios en nube incluye nuevos riesgos a los que se expone la organización, por esta razón se debe previamente identificarlos para adoptar los controles necesarios.

2.1.4 Tecnologías Emergentes

La innovación es la que impulsa el crecimiento en las industrias y la que crea nuevos riesgos de seguridad, en este contexto la ciberseguridad es un desafío tecnológico relevante que debe seguir un proceso de mejora continua. Según Hype Cycle for Emerging Technologies (2019), se identificaron tres tecnologías emergentes que tendrán una intervención directa en el mundo de IT.

Estas tecnologías son:

Sensibilidad y movilidad: Esta tecnología emergente consiste en cámaras de detección 3D, la cual permite una conducción autónoma más avanzada. Los robots autónomos obtendrán una mejor percepción del mundo que los rodea a medida que los sensores y la

inteligencia artificial evolucionan. Por ejemplo, las tecnologías emergentes como los aviones no tripulados de carga liviana, los cuales optimizaran los recorridos en sus entregas. (Gartner, 2019)

Entre otras de las tecnologías emergentes, podremos encontrar AR Cloud (Realidad Aumentada Cloud), la cual lleva a otro nivel el paradigma "Cloud Computing" y permitirá mediante el uso de lentes inteligentes, obtener información de los objetos que nos rodean.

Humano aumentado: Esta tecnología tiene como fin mejorar las partes cognitivas y físicas de los humanos al incluir tecnologías como biochips e inteligencia artificial de emoción. Cabe destacar, que esta tecnología es impulsada por la industria militar. (Gartner, 2019) El objetivo principal es conseguir "superhombres" con cualidades que sobresalgan de la especie, específicamente en el ámbito laboral. Estos superhombres, tendrán una mayor fuerza física, estarán mucho más informados y serán más seguros.

Computación y comunicaciones posclásicas – computación Cuántica: La computación cuántica es un tipo de computación no clásica basada en el estado cuántico de partículas subatómicas. La computación cuántica es fundamentalmente diferente de las computadoras clásicas, que funcionan con bits binarios. (Bonillo, 2013) Los bits pueden ser positivo o negativo, 0 o 1, verdadero o falso. Sin embargo, en la computación cuántica, el bit se denomina bit cuántico o qubit. A diferencia de los bits estrictamente binarios de la informática clásica, los qubits pueden, extrañamente, representar un rango de valores en un qubit. Esta representación se llama "superposición".

La informática clásica o binaria que utiliza bits binarios evolucionó haciendo cambios en las arquitecturas tradicionales existentes. Estos cambios dieron como resultado CPU más rápidas, memoria más densa y un aumento en el rendimiento. (Gartner, 2019)

Los cálculos y las comunicaciones posclásicas están utilizando arquitecturas completamente nuevas (computación cuántica). Esto incluye 5G, los estándares para celulares de próxima generación, que tiene una nueva arquitectura que incluye cambios en el núcleo de la red. (Gartner, 2019)

El Gartner Hype Cycle se enfoca en tecnologías que ofrecerán un alto grado de ventaja competitiva durante la próxima década. Las implementaciones de estas nuevas tecnologías en las organizaciones deben realizarse teniendo en cuenta a la seguridad desde el diseño, respetando las políticas que tenga la organización como así también las regulaciones que se encuentren vigentes en el país de su implementación.

En la Figura 2 obtenida del informe realizado por la consultora Gartner (Hype Cycle for Emerging Technologies, 2019), se puede observar las tecnologías emergentes.

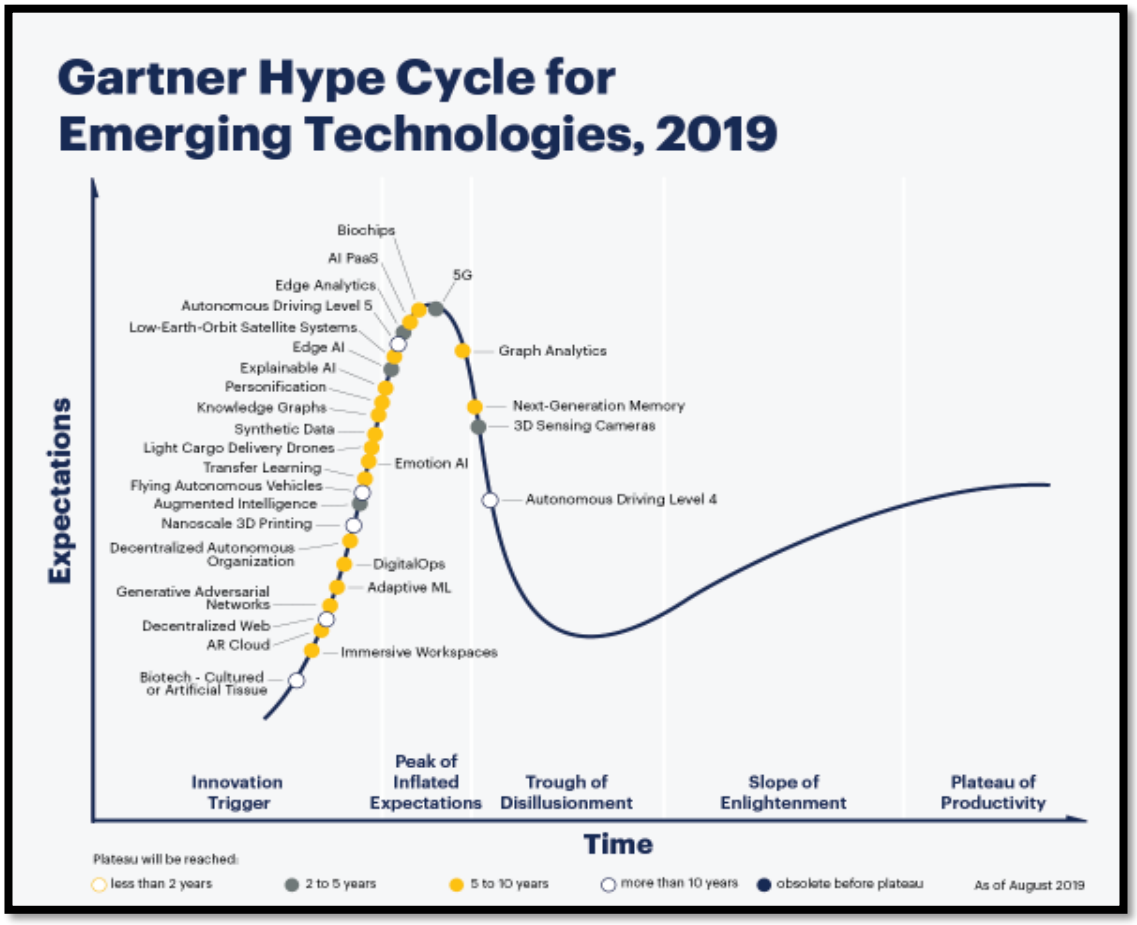

Figura 2: El gráfico Gartner Hype Cycle for Emerging technology, (2019) identifica las tecnologías emergentes que tendrán impacto en los negocios.

2.2 Tecnologías Operativas

La tecnología de la operación se refiere a sistemas de control y supervisión de procesos industriales, que abarcan instrumentación de campo, sistemas HMI, SCADA, DCS y MES basadas en plataformas propietarias de unos pocos fabricantes. (General Electric, Rockwell, ABB, Schneider, Siemens, entre otros). La consultora de investigación tecnológica Gartner la define como “hardware y software que detecta o causa un cambio, a través de la supervisión directa y/o el control de equipos industriales, activos, procesos y eventos” (Gartner, 2020)

Esta tecnología es utilizada en los sistemas de telecomunicaciones, sistemas de suministro eléctrico, sistemas de combustibles de gas natural y combustibles basados en hidrocarburos, transporte, sistema de suministro de agua y gestión de residuos entre otros.

Por lo antes indicado, se puede observar que estas tecnologías dan soporte a los

procesos de industrias importantes. El fallo producto de un ciberataque podría ocasionar la interrupción de un proceso productivo, comprometer la seguridad física de las personas, provocar daños en el medio ambiente y afectar la integridad de los equipos e instalaciones.

2.2.1 Historia

En 1960 se comenzó a utilizar la señal analógica (4-20 mA) en redes de comunicación industrial. Luego comenzó a reemplazarse algunas de estas señales por tecnologías de campo digital. (Alonso, 2013)

Según Alonso, N. O. (2013), al existir una gran cantidad de protocolos propietarios de bus de campo, surge la necesidad de la integración y estandarización de las comunicaciones industriales, con el fin de aumentar la confianza sobre estas tecnologías. Se pretendía garantizar una estabilidad y una fiabilidad en la inversión tecnológica realizada. (p. 211)

Para llevar adelante el proceso de estandarización, se requirió el trabajo de varios comités que estudiaron las diferentes tecnologías en función al ámbito de aplicación. Se estableció de esta manera una puja tanto en tecnologías, protocolos, dispositivos, calidad y precio. Diversas tecnologías de redes de campo surgieron, producto de las necesidades que se plantearon en la industria. (p. 211)

La tecnología de bus de campo es definida por Alonso (2013) como “un sistema de dispositivos de campo (sensores y actuadores) y dispositivos de control, que comparten un bus digital, serie bidireccional para transmitir información entre ellos” (p. 165). Esta tecnología ha modificado diversos aspectos en un control de procesos como ser:

- Volumen de información, eficiencia en el procesamiento de datos
- Tipo y número de conexiones, velocidad de operación, inmunidad a las perturbaciones
- Confiabilidad y seguridad
- Instalación, implementación, servicio y mantenimiento

Organismos como “Fieldbus Committee of International Electrotechnical Comisión”, “International Society for Measurement and Control”, “System Project” y empresas privadas fueron trabajando en el desarrollo de un estándar para redes de campo. Esta tarea demandó grandes esfuerzos para la integración de una amplia cantidad de procesos y dispositivos de operación presentes en todo el mundo. Estos trabajos concluyen en la especificación 61158 de la IEC. A su vez se pueden descubrir diversas redes que no se encuentran normalizadas bajo esta especificación, pero que se aplican convenientemente en redes industriales, como por ejemplo Modbus. (p. 212)

2.2.2 Redes Industriales

Una red industrial es una red de tiempo real, es decir que sus componentes tienen un tiempo máximo de respuesta. Estas redes son utilizadas en un sistema de producción para conectar procesos industriales, asegurando la utilización e instalación de forma adecuada. (Alonso, N. O. 2013)

En muchas empresas los procesos de producción necesitan ser controlados, por lo cual existen una serie de equipos y dispositivos encargados de realizar esta tarea, dando origen a las redes industriales.

El desarrollo de estas ha establecido una forma de unir dispositivos, aumentando el rendimiento y proporcionando nuevas posibilidades, surgiendo ventajas desconocidas hasta el momento de aplicación de esta tecnología. (Alonso, N. O. 2013)

Las redes industriales suelen ser un blanco de ataque por el hecho de no tener una política de seguridad robusta que les permita implementar medidas básicas como firewall, realizar análisis de vulnerabilidades y tener un proceso de monitoreo continuo de los sistemas. (Alonso, N. O. 2013)

2.2.3 Control de variables sobre Redes Industriales

Las variables son todos los parámetros físicos cuyo valor puede ser medido. Dichas variables deben ser controladas por un operario quien decide como y cuando se deben modificar, pudiendo obtener una cadena productiva eficiente y continua.

Otra forma de monitorear estos controles es mediante la automatización sin intervención humana.

Existen dos tipos de Sensores (Discretos o Analógicos). (Alonso, N. O. 2013)

Sensores Discretos: Normalmente proporcionados por contacto físico indicando abierto o cerrado (condición on/off) o por nivel alto o bajo asociado a una alarma. (p. 208)

Sensores Analógicos: Convierten parámetros continuos tales como temperatura o flujo a señales analógicas como 4-20mA o 0-5V. (p. 208)

Para que la información de campo llegue al sistema de control, esta debe ser digitalizada.

En el caso que no se requiera la intervención humana en el proceso de control, se debe realizar una automatización, la cual consiste en un sistema de control totalmente automático. El sistema valida su funcionamiento, realiza las mediciones que les fueron configuradas y por último realiza correcciones sin necesidad de la intervención humana.

(Alonso, N. O. 2013). Uno de los desafíos que tiene la seguridad de la información en redes industriales es proteger los datos recolectados, que se encuentren disponibles de una forma íntegra y que solo tengan acceso las personas que se encuentren autorizadas.

2.2.4 Componentes de Control

Según el estándar NIST SP800-82 (Stouffer et al., 2015), un sistema de control industrial (ICS) está compuesto principalmente por los siguientes componentes:

PLC (Programmable Logic Controller): Los sistemas se pueden supervisar y monitorear mediante una lectura de los valores de las diversas variables del proceso, con el objeto de identificar el estado en tiempo real. (p-12)

El PLC son equipos que sustituyeron a controladores basados en relés ya que son más económicos y pequeños. En la Figura 3, obtenida de la guía de ICS realizada por NIST (NIST Guide to Industrial Control Sistemas - Security) se puede observar la implementación de un PLC en un sistema de control. (p-12)

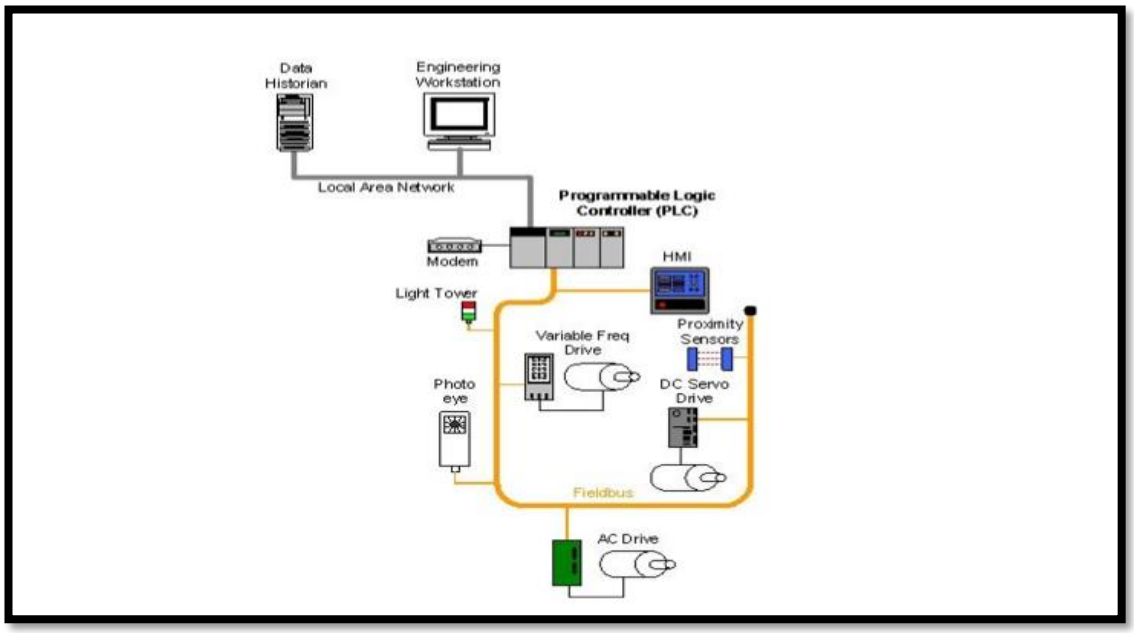

Figura 3: Ejemplo de implementación de un PLC según la guía de ICS de NIST.

RTU (Remote Terminal Unit – Unidad Terminal Remota): Es un dispositivo que se instala en una ubicación remota, el cual recolecta datos y se utiliza para convertir los datos de forma analógica y discreta a información digital, con el fin de que puedan ser transmitidos a una estación central. También tiene la bondad de manejar numerosas opciones de comunicación y protocolos. (p. 13)

En la Figura 4 obtenida de la web oficial Siemens (Siemens - serie SIMATIC RTU3000C) se puede observar un RTU versión RTU300C Siemens.

Figura 4: Ejemplo de un RTU Siemens.

DCS (Distributed Control System – Sistemas de Control Distribuido): Son sistemas de control distribuidos, similar a SCADA. Los DCS comunican el hardware de control y presentan los datos a un HMI y muestra constantemente los datos de un controlador, pero no los almacena para informes históricos. (p. 2-10)

- Servidor SCADA o Unidad Terminal Maestra (MTU). El Servidor SCADA es el dispositivo que actúa como maestro en un sistema SCADA. Se centra en la supervisión, es decir, el sistema ejecuta instrucciones de control que son indicadas por el operador. Su foco es la adquisición de datos y su presentación a través de dispositivos HMI. (p. B-10)
- Dispositivos electrónicos inteligentes (IED). Un IED es un equipo de regulación electrónica, el cual contiene la inteligencia necesaria para la adquisición de datos, comunicarse con otros dispositivos, y realizar el procesamiento y el control local.

  Un IED podría combinar un sensor de entrada y salida analógica, control de bajo nivel, un sistema de comunicación y la memoria del programa en un solo dispositivo. (p. B-8)
- Historiador de datos. El historiador de datos es una base de datos centralizada para el registro de toda la información de proceso dentro de un ICS. La información almacenada en esta base de datos se puede acceder para realizar diversos análisis, por ejemplo, el control estadístico de procesos para la planificación a nivel de empresa. (p. 5-20)
- Servidores de entrada / salida (I/O). El servidor IO es un componente de control responsable de la recolección, el almacenamiento en búfer y el acceso para procesar la información de los subcomponentes de control, tales como PLCs y

RTUs. Un servidor IO puede residir en el servidor de control o en una plataforma de equipo independiente. Los servidores IO, también se utilizan para interconectar los componentes de control de terceros, tales como un panel o un servidor de control. (p. B-8)

HMI (Human Machine Interface – Interfaz Hombre Maquina): Con el fin de brindarle al operador una representación gráfica del entorno controlado, se utilizan los HMI, los cuales tienen como función, controlar, monitorear y gestionar alarmas. Los HMI pueden ser sistemas software en una PC, o sistemas standalone como paneles táctiles o dispositivos móviles. En algunos casos recolectan datos de los dispositivos (PLC, RTU, etc.) y los envían a una base de datos para históricos y análisis de tendencias. (p. B-7)

El estándar NIST los define en su IR 6859 de la siguiente forma:

El hardware o software a través del cual un operador interactúa con un controlador. Una HMI puede variar desde un panel de control físico con botones y luces indicadoras hasta una PC industrial con una pantalla de gráficos en color que ejecuta un software HMI dedicado. (Falco, J. 2002, p.15)

En la Figura 5 obtenida de la web oficial Siemens (Siemens - SIMATIC Advanced HMI) se puede observar los nuevos paneles portátiles HMI de Siemens.

Figura 5: Ejemplo de Interfaz Hombre Máquina que se utilizan para controlar y monitorear las variables como así también la visualización de alertas.

2.2.5 Componentes de Red

Hay diferentes características de la red para cada capa dentro de una jerarquía de sistema de control. Las topologías de red, a través de diferentes implementaciones de los

sistemas de control industrial, varían con los sistemas modernos que utilizan las estrategias de integración de la empresa de IT, basados en internet.

Principales componentes de una red de ICS

Según el estándar NIST SP800-82 (Stouffer et al., 2015), algunos de los principales componentes de red en un ICS son:

Red de bus de campo: La red de bus de campo vincula sensores y otros dispositivos a un PLC u otro controlador. El uso de tecnologías de bus de campo elimina la necesidad de cableado punto a punto entre el controlador y cada dispositivo. Los dispositivos se comunican con el controlador de bus de campo usando una variedad de protocolos. Los mensajes enviados entre los sensores y el controlador identifican de manera única cada uno de los sensores. (p. 2-11)

Red de Control: La red de control conecta el nivel de control de supervisión a los módulos de control de nivel inferior. (p. B-3)

Routers y Comunicaciones: Un router, es un dispositivo de comunicaciones que transfiere mensajes entre dos o más redes. Los usos más comunes para los routers incluyen la conexión de una LAN a una WAN, y la conexión de MTU y RTUs a un medio de red de larga distancia para la comunicación con un SCADA. (p. B-14)

Firewall: Un firewall protege los dispositivos de una red mediante la vigilancia y el control de paquetes de comunicación, utilizando las políticas de filtrado predefinidas. Los firewalls también son útiles en el manejo de estrategias de segregación de la red del ICS. (p. B-7)

Módems: Un módem es un dispositivo utilizado para convertir los datos digitales en serie y una señal adecuada para su transmisión por una línea de teléfono para permitir que los dispositivos se comuniquen. Los módems se utilizan a menudo en sistemas SCADA para permitir comunicaciones en serie de larga distancia entre MTU y dispositivos de campo remotas. También se utilizan en sistemas SCADA, DCS y PLC para obtener acceso remoto para las funciones de operación y mantenimiento, tales como la introducción de órdenes o la modificación de parámetros, y con fines de diagnóstico. (p. 6-11)

Puntos de acceso remoto: Son distintos dispositivos, zonas y ubicaciones de una red de control que permiten configurar remotamente los sistemas de control y acceso a los datos de proceso. Ejemplos, uso de un asistente digital personal (PDA) para acceder a los datos a través de una LAN mediante un punto de acceso inalámbrico, y el uso de un ordenador portátil y conexión de módem para acceder de forma remota un sistema ICS. (p. B-13)

Estos componentes de red antes descriptos son fundamentales para una red industrial y su protección debe ser priorizada.

2.2.6 Generalidades de los Sistemas de Control Industrial

Según el NIST Special Publication 800-82 (2015), un sistema de control industrial (ICS) es un término general, el cual abarca varios tipos de sistemas de control, dentro de este término, encontramos a los sistemas de adquisición de datos SCADA, sistemas de control distribuidos, control de supervisión y otras configuraciones de sistemas de control, tales como los controladores lógicos programables PLC.

El NIST define a los Sistemas de Control industrial (ICS) de la siguiente forma: *"*Un ICS consiste en combinaciones de componentes de control (por ejemplo, eléctricos, mecánicos, hidráulicos, neumáticos) que actúan juntos para lograr un objetivo industrial (por ejemplo, fabricación, transporte de materia o energía)*".* (NIST Special Publication 800-82, 2015 2, p.16)

Los ICS se utilizan normalmente en las industrias tales como electricidad, agua y aguas residuales, petróleo y gas natural, química, transporte, farmacéutica, papel, alimentos y bebidas, y la fabricación discreta (por ejemplo, automotriz, aeroespacial y bienes duraderos). Cabe mencionar, que estos son utilizados en la mayoría de las infraestructuras críticas, es por ello, la imperiosa necesidad que sean implementados con las medidas de seguridad adecuadas o basándose en estándares internacionales.

2.2.7 Sistemas SCADA

Según el NIST Guide to Industrial Control Systems (ICS) (2015), los sistemas SCADA se utilizan para controlar los activos dispersos, dado que la adquisición de datos centralizada es tan importante como el control. Estos sistemas se utilizan en los sistemas de distribución, como por ejemplo sistemas de distribución de agua y alcantarillado, tuberías de petróleo y gas natural, sistemas de transmisión y de distribución de servicios eléctricos, el ferrocarril y otros sistemas de transporte público.

Los sistemas SCADA están diseñados para recoger información de campo, transferirla a un centro de procesamiento, y mostrar la información al operador de forma gráfica o textual, lo que permite al operador supervisar o controlar todo un sistema desde una ubicación central en tiempo real. Sobre la base de la sofisticación y la configuración del sistema individual, la operación o tarea puede ser automática, o realizada por los comandos del operador. (Stouffer et al., 2015)

Los sistemas SCADA están compuestos tanto de hardware como de software. El hardware típico incluye un MTU colocado en un centro de control, equipos de

comunicaciones (por ejemplo, radio, línea telefónica, cable, o satélite), y uno o más sitios distribuidos geográficamente en el campo que comprendan una RTU o PLC, que controla los actuadores y / o supervisa los sensores. Los MTU almacenan y procesan la información de las entradas y salidas de la RTU, mientras que el RTU y el PLC controlan el proceso. El software está programado para indicar al sistema qué debe monitorear, cuándo debe hacerlo, qué parámetro y rangos son aceptables y qué respuesta debe enviar cuando los parámetros no se encuentran dentro de los valores aceptables. En cuanto al transporte de datos, los IED pueden comunicarse directamente con el servidor SCADA o bien centralizar la información en un RTU local para recopilar los datos y luego enviarlos al servidor SCADA.

Según Stouffer (2015) los IED proporcionan una interfaz directa para controlar y supervisar el equipo y los sensores. Estos pueden ser consultados directamente, controlados por el servidor SCADA y en la mayoría de los casos tienen la programación local que permite al IED actuar sin instrucciones directas del centro de control del sistema SCADA. Estos sistemas son generalmente diseñados para ser sistemas de alta disponibilidad con redundancia significativa integrado en la arquitectura del sistema.

La figura 6 obtenida de la guía de ICS, (NIST Guide to Industrial Control Systems (ICS) Security), muestra los componentes y configuración general de un sistema SCADA.

El centro de control cuenta con un servidor SCADA (MTU) y los enrutadores de comunicaciones. Otros componentes del centro de control incluyen la HMI, estaciones de trabajo de ingeniería, y el historiador de datos, los cuales están conectados por una LAN.

El centro de control recoge y registra información recopilada por los sitios de campo, se muestra información al panel del operador, y puede generar acciones basadas en eventos detectados. El centro de control también es responsable de las alarmas centralizadas, el análisis de tendencias y reportes. El sitio de campo realiza el control local de los actuadores y sensores.

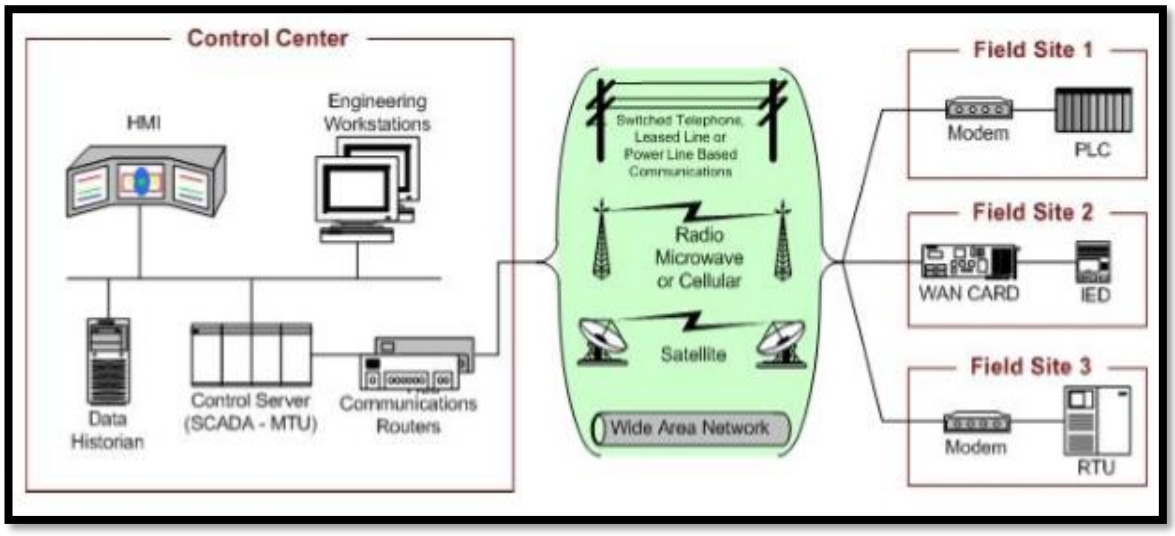

Figura 6: Sistema Genera, muestra los componentes de un sistema SCADA según NIST.

Los sitios de campo están a menudo equipados con una capacidad de acceso remoto para permitir a los operadores realizar un diagnóstico remoto y reparaciones, por lo general mediante un módem dial-up o conexión WAN.

Este tipo de sistema fue creado para mantenerse aislado de redes corporativas, como se indicó al principio del capítulo, pero este paradigma fue cambiando y su convergencia con redes corporativas es inevitable. En consecuencia, esto provocó que los sistemas SCADA sean un potencial blanco para los atacantes, no solo por la conexión a internet, ya que por ejemplo el famoso ataque con Stuxnet fue introducido por puertos USB.

2.2.8 Internet de las Cosas Industrial (IIoT)

En el marco de la integración entre el mundo de IT y de OT nace IIoT, este consiste en el uso de la tecnología internet de las cosas (IoT) en el ámbito industrial, incorporando el aprendizaje de máquinas y el concepto de big data, en donde se manipulan grandes volúmenes de datos, aprovechando la información que se obtiene de sensores. Esto da lugar a las operaciones industriales de forma inteligente, permitiendo a las empresas ser más eficientes y aumentar la confiabilidad en sus operaciones con una menor dependencia de las personas y la interacción con la máquina. Sumando que distintos dispositivos envían información a la nube, con el fin de que se pueda acceder de forma remota para la toma de decisiones, y en consecuencia se debe implementar las medidas de seguridad basadas en los nuevos riesgos.

La Industria 4.0 y el IIoT: El IIoT aporta a la industria el beneficio de aumentar la eficiencia, puesto que las funciones pueden incorporar mayor cantidad de datos sobre

los distintos procesos y productos, debido a la utilización de sensores. Estos datos son procesados y dan una valiosa información para la toma de decisiones.

Según Hall (2018) “el IIoT permite automatizar procesos que pueden mejorar los tiempos de lanzamiento al mercado, medir performance y velozmente, responder a las necesidades del cliente” (p. 72) Gracias a esos aportes, es una buena herramienta para el desarrollo de nuevos modelos de negocios, puede asistir en la reducción de los riesgos operativos y al monitoreo del cumplimiento de protocolos de seguridad. “Las máquinas pueden aprender a monitorear y auditar el cumplimiento de procedimientos” (Hall, 2018, p.72), dar alertas ante un desvío de forma automática para que el humano puedo realizar una acción sin interrumpir el proceso productivo.

2.3 Seguridad Informática

La seguridad informática según Vieites, Á. G. (2011), se puede definir como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

La seguridad informática posee los siguientes objetivos principales:

- Minimizar y gestionar los riegos, detectar los posibles problemas y amenazas de seguridad.
- Garantizar la adecuada utilización de los recursos informáticos, manteniendo la disponibilidad, integridad y privacidad de la información.
- Limitar las pérdidas y conseguir la recuperación eficaz del sistema en caso de un incidente de seguridad. Es decir, ser resiliente en el caso que ocurra un incidente de seguridad.
- Cumplir con el marco legal y las normativas internacionales (Vieites, 2011)

2.3.1 Malware

Un malware según Vieites, Á. G. (2011), es un software diseñado para ocasionar daños o realizar acciones no deseadas en sistemas informáticos. El objetivo es proporcionar control remoto para que el atacante pueda utilizar el equipo infectado, realizar el envío de spam desde equipos infectados, poder acceder a redes de usuarios infectados o directamente realizar el robo de datos sensibles. Cabe destacar, que tiene una gran velocidad de propagación.

Historia de los Virus Informáticos. Los orígenes de los virus según Vieites, Á. G. (2011), se pueden establecer al observar investigaciones sobre inteligencia y vida artificial. Estas ideas fueron evolucionadas por John Von Neuman en 1950 constituyendo el concepto de programas autorreplicables.

En 1960 en los laboratorios de Bell se desarrollaron programas Core Wars que eran una especie de juegos, los cuales tenían como objetivo lograr el mayor espacio de memoria posible. (p. 254)

En 1970, John Soch y Jon Hupp crearon programas autorreplicables que servían para controlar la salud de las redes informáticas. Luego de su creación y despliegue, el programa se multiplicó en las diferentes computadoras, lo cual produjeron el colapso de la red informática. En un principio la finalidad de estos programas fue solo experimental y sin fines perjudiciales. (p. 254)

Los virus tienen su nacimiento en los años 80 y luego en 1983 se instaura la definición de virus para estos. En el año 1985 infectaron al sistema operativo MS–DOS© y luego en 1986 se tornaron más destructivos. En esa época el medio de distribución utilizado y de propagación era el disquete. (p. 254)

El famoso ataque masivo a una red informática conocida como ARPAnet la cual fue precursora de internet, tiene origen el 2 de noviembre de 1988. Para su propagación se utilizó el correo electrónico y en solo 3 horas se extendió en todo EEUU. La erradicación de este gusano costó un millón de dólares y demostró que podía hacer un programa auto replicable fuera de control. Quien reconoció la autoría del virus y admitió que fue un error es Robert Morris, graduado de Harvard con solo 23 años, dicho error lo calificó como “fallo catastrófico”, ya que su idea no era hacer que las computadoras se ralentizaran. (p. 256)

En 1988 surgen los primeros programas antivirus, producto de las consecuencias antes indicadas y la concientización que tienen la industria informática con respecto a proteger los sistemas informático.

En el año 1991 surgen los primeros kits para la creación de nuevos virus informáticos, lo que permitió que sean creados con mayor facilidad. El primer kit fue el VCL (Virus Creation Laboratory), creado por Nowhere Man. (p. 257)

En la década de los noventa se produjeron cambios en el ámbito informática personal generando consecuencias en la actualidad, estos cambios aumentaron los números de virus que estaban en circulación.

La ICSA Labs (Asociación Internacional de Seguridad Informática) es el principal organismo dedicado al seguimiento del fenómeno de los virus en todo el mundo, proporcionando garantías de productos de terceros confiables e independientes para usuarios finales y empresas desde 1989.

En España, en el año 2000 se llevó a cabo la primera campaña nacional de antivirus informáticos impulsada por la empresa Panda Software y otras organizaciones, la misma tuvo lugar desde el 17 al 31 de Julio. (p. 258)

2.3.2 Entre los tipos de Malware existentes, los más peligrosos son los siguientes

A continuación, se realiza una breve descripción de los principales malware que ponen en riesgo tanto a las redes corporativas como a las redes industriales. Este tipo de riesgo se puede mitigar considerablemente con un software antivirus, el cual debe ser actualizado recurrentemente.

Virus Informáticos: Un virus informático según Vieites, Á. G. (2011), es un software que afecta a otros programas, modificándolos de tal manera que causen un efecto negativo en el acto (eliminar o dañar archivos), también puede causar una disminución en el rendimiento o impactar directamente en la seguridad. Estos ataques toman por sorpresa a los usuarios inexpertos. Por lo general, los virus suplantan archivos ejecutables por otros infectados con el código malicioso.

Este software representa una amenaza muy seria, uno de los efectos principales es la propagación casi instantánea que poseen y generalmente este efecto es mayor al tiempo de resolución.

Los virus pueden destruir de forma intencionada todos los datos que posee una máquina de escritorio como así también una workstation utilizada para el mundo industrial, aunque también existen otros más inofensivos. Generalmente se propagan a través de un software que potencialmente pueden contener además otros objetivos como puede ser realizar algún daño que comprometa al sistema, o generar un tráfico excesivo en las redes informáticas para denegar servicios.

Virus de sector de arranque (Virus de boot): Estos virus según Kaspersky (2021), infectan el sector de arranque o tabla de partición de un disco. Generalmente el método de contagio de estos virus se daba por medio de los antiguos disquete (hoy en desuso). Luego de ser infectado el disco duro, este virus tratara de infectar a los demás discos duros que se encuentren conectados en la maquina infectada, el mismo puede ser eliminado con facilidad.

Scam: Según Panda Security (2021), es una técnica para realizar estafas y operaciones fraudulentas mediante Internet, los scam surgieron en el año 2005 y están basados en engaños e ingeniería social, el objetivo es obtener un beneficio económico por parte del atacante ya sea solicitando dinero o información de la víctima. Un caso muy popular fue el del dinero bloqueado en Nigeria el cual consistía en pedirle ayuda a las victimas con el fin de poder transferir una suma muy importante de dinero a su cuenta bancaria con el pretexto de destrabar el mismo, dándole a las victimas un porcentaje de dicha suma como recompensa. Luego de tener la confianza de la víctima, se le solicitaba que le transfiera una suma de dinero con algún pretexto. Este tipo de estafa fue variando según el atacante.

Virus de programa ejecutable: Según Vieites, Á. G. (2011), este tipo de virus infectan programas ejecutables (generalmente, archivos con extensiones .com o .exe), y desvían el flujo de ejecución al propio código del virus, luego vuelven al mismo código ejecutando tareas que el usuario espera sin notar la presencia del virus en el sistema. Usualmente intentan propagarse, infectando los archivos almacenados en la máquina.

Este tipo de virus tiene generalmente un poder destructivo, tratando de formatear el disco rígido o realizar acciones nocivas para el equipo infectado. Eliminar estos virus no es muy complejo, sin embargo, si este ha sobrescrito código o parte de algún código en su totalidad, el archivo quedará modificado para siempre.

Código Java malicioso: Según Vieites, Á. G. (2011), los virus de lenguaje Java, afectan a los applets de Java, la cuales son programas o miniaplicaciones portátiles en Java que se encuentran anidadas en páginas HTML. Se ejecutan automáticamente al visualizar las páginas.

Phishing: Como se pudo obtener de la web oficial de Panda Security (2021), este tipo de ataque consiste en el envío de correos electrónicos por parte de un ciberdelicuente los cuales tiene una apariencia de fuentes confiables, como podría ser una entidad bancaria, una empresa reconocida, o una entidad gubernamental, pero en realidad se pretende engañar al receptor del correo electrónico para robar información. Generalmente el correo electrónico que recibe la víctima posee un enlace web falsificado que invita a la víctima a ingresar información confidencial como contraseñas, PIN bancarios, número de tarjetas de crédito, entre otros. El phishing puede llevarse a cabo por otros medios que no sea el correo electrónico, estos pueden ser:

Phishing por un sitio web: Se crean sitios web apócrifos para engañar a sus víctimas y que estas ingresen información confidencial

Vishing: Consiste en intentar convencer a las victimas vía telefónica para que revelen información personal, con el fin de poder usar la información recolectada más adelante intentando el robo de identidad. (Yeboah-Boateng, 2014)

Smishing: Es un phishing mediante un mensaje SMS, que invita a la víctima a que haga clic en un enlace de descarga o un enlace web. Al realizar clic, se descarga un malware en el teléfono móvil el cual potencialmente podría captar la información personal de la víctima y enviarla al ciberdelincuente. (Yeboah-Boateng, 2014)

Phishing por redes sociales: Es una metodología de engaño por redes sociales que intenta forzar a la gente a enviar enlaces falsificados a sus contactos.

Virus de macro: Son virus que se propagan a sí mismos a través de un lenguaje de programación el cual emplea macros para concebir otro software, el principal riesgo de este virus es su agilidad en la expansión. Estos virus suelen encontrarse en documento de texto, estos son difícil de detectar puesto que solo se activan cuando es ejecutada una macro infectada. (Kaspersky, 2021)

Troyano: Es un malware el cual se oculta detrás de un software legítimo. Estos suelen ser muy utilizados por hackers o cibercriminales para poder acceder a los sistemas de sus víctimas. Las acciones principales que se pueden ejecutar con un troyano son: eliminar, bloquear modificar o copiar datos, otra de sus acciones puede ser la interrupción del funcionamiento de computadoras o redes. Una diferencia que tienen con los demás es que no son capaces de autorreplicarse. (Kaspersky, 2021)

La arquitectura de los troyanos está basada en cliente-servidor, en los equipos infectados se instala el servidor que responden a las acciones enviadas por el cliente, el cual es ejecutado desde la máquina del atacante.

Backdoor o puerta trasera: Según la web oficial Panda Security (2021), son utilizados por los hackers para acceder a funciones de las computadoras de manera oculta pudiendo trabajar en segundo plano. Están diseñados para darle a los atacantes el control del equipo infectado, generalmente este tipo de categoría se utiliza para generar una red Zombi. Sticky Atacks es un ejemplo de estos en donde las víctimas eran atacados por fuerza bruta contra los servidores que tenían habilitados el Remote Descktop Protocol (RDP) consiguiendo las credenciales del equipo para poder acceder.

Rootkits: Según la web oficial Avast (2021), este tipo de virus proviene de los sistemas operativos Unix, en donde la cuenta administradora se denomina root (usuarios raíz), mientras que los conjuntos de herramientas de software reciben el nombre de kits. Consiste en modificar las herramientas del sistema operativo ya sea netstat, password,

entre otras, con el fin de obtener acceso a la maquina victima sin que esta actividad fuera detectada por el administrador.

Gusano: Un Gusano es un software malicioso el cual tiene como característica principal su replicación a si mismo a través de redes, sin poder detectar que equipo se encuentra infectado. Se pueden propagar como un Email-Worm, IM-Worm, IRC-Worm, Net-Worm, P2P-Worm o Virus. (Kaspersky, 2021)

Ransomware: Según los datos obtenidos del sitio web Avast (2021), este tipo de malware impacta bloqueando la maquina infectada y toma el control de esta, cifra los archivos almacenados y luego solicita un rescate económico para liberarlos. Estos tipos de ataques suelen provocar costosas interrupciones en las operaciones y perdida de datos críticos en las organizaciones ya sea el sector público o privado.

Los tipos de ransomware pueden ser:

Filecoders: Provocan el cifrado y bloqueo de archivos en dispositivos, exigiendo un pago para obtener la clave de descifrado, la cual le permitirá a la víctima acceder a los datos que fueron afectados. (Eset, 2016)

Screenlocker: Impide acceder al equipo infectado, ya sea una computadora, smartphone o Tablet. En algunos casos se hacen pasar por el FBI indicando el incumplimiento de una ley y solicitando un pago de una multa para desbloquear la maquina afectada. (Eset, 2016)

Doxing: Este tipo de ransomware consiste en el acceso a datos confidenciales de la víctima, estos pueden ser datos de tarjeta de crédito, usuarios y contraseña de entidades bancarias entre otros. Se solicita a la víctima un pago para que no se divulguen los datos obtenidos.

Scareware: Es un software falso el cual nos indica que encontró un problema en el equipo y demanda un pago con el fin de solucionar el mismo. (Eset, 2016)

Uno de los ransomware más conocidos es WannaCry, el cual provocó el cifrado de archivos en máquinas que tenían Windows como sistema operativo, dejando cien millones de usuarios afectados en todo el mundo, esto se debía a la explotación de una vulnerabilidad de Windows que permite a un ciberdelicuente ejecutar código de forma remota. El malware Petya el cual cifraba tablas maestras de archivos del disco duro para bloquear a los dispositivos afectados. Cabe destacar que la mayoría de sus infecciones fueron los países de Rusia y Ucrania.

Rogue o falso antivirus: Un rogue simula ser una aplicación de seguridad para brindar protección contra malware, generalmente pueden encontrarse para descargar de forma gratuita, como consecuencia de la instalación de este tipo de aplicaciones se instalan también otros programas dañinos. Este tipo de software lejos está de ser un antivirus, ya que deja mucho más expuesto al equipo en donde se instale. (Segu-Info, 2021)

2.3.3 Vulnerabilidades

Según Vieites, Á. G. (2011), recién en el año 1988 se tomaron con mayor seriedad a los ataques cibernéticos, en ese año, Rober Morris creó un gusano de internet, que fue protagonista del primer incidente de seguridad informática. El gusano afectó miles de computadoras y el servicio de las redes fue interrumpido por varios días. Otros ataques fueron realizados accediendo a la red simplemente averiguando una clave válida o básicamente saltando controles de acceso físico, como puede ser el acceso a una computadora o a un Data Center.

Con el correr de los años, se fueron desarrollando nuevos métodos cada vez más complejos para la explotación de vulnerabilidades. Esto permitió a los atacantes tomar el control de sistemas completos y acceder a información crítica produciendo verdaderos desastres irrecuperables.

En los sistemas industriales, al no tener un proceso maduro de gestión de parches o actualizaciones de los sistemas operativos, se tiene una mayor brecha de seguridad que permite a los atacantes hacer uso de estas. En la actualidad los distintos proveedores tienen un proceso de comunicación optimizado para poder dar a conocer las vulnerabilidades reportadas y los parches que mitigan las mismas.

Definición de vulnerabilidad informática: Según Urbina, G. B. (2016), una vulnerabilidad informática está relacionada a debilidades que posee un sistema informático en donde se podría potencialmente concretar una amenaza. Esta vulnerabilidad posibilita a un atacante afectar la confidencialidad, integridad y disponibilidad de un sistema industrial o un sistema corporativo.

Una de las vulnerabilidades más comunes que puede suceder es que el diseñador del sistema no tenga la capacidad de poder prever las potenciales amenazas que existen o que puedan surgir en un futuro.

Las vulnerabilidades en las aplicaciones suelen corregirse con la aplicación de parches de seguridad, hotfixs o con cambios de versión. En algunos casos se requiere un cambio físico.

Causas que provocan vulnerabilidades informáticas: Las vulnerabilidades existentes en la actualidad según Vieites, Á. G. (2011), son provocadas por una serie de causas que se pueden identificar de la siguiente manera:

A. Fácil acceso a herramientas que facilitan realizar ataques cibernéticos

Con el simple hecho de tener acceso a internet, se puede acceder a muchas herramientas gratuitas con una interfaz gráfica muy simple de manejar y que facilitan la explotación de vulnerabilidades. Es por ello, que se multiplicaron los ataques por parte de personas con conocimientos mínimos en seguridad informática. (p. 179)

B. Errores de programación

Una de las causas que provoca gran cantidad de vulnerabilidades, son los errores de diseño de programación, que como acción mitigante se requiere aplicar los parches que el proveedor publique para subsanar la vulnerabilidad. Por otro lado, es bueno destacar los errores en el tratamiento de entradas no validas, los cuales pueden provocar un desbordamiento de memoria conocida como "Buffer Overflow". (p. 175)

C. Debilidades en el diseño de protocolos utilizados dentro de la red

Este tipo de debilidades se encuentra en los protocolos utilizados por los servicios de redes o inclusive internet, los cuales fueron diseñados sin tener en cuenta la seguridad de los datos. Esto permite intercambiar datos que pueden ser sensibles sin cifrar. Como ejemplo de esto se pueden mencionar a los protocolos telnet, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Protocol). (p. 174)

D. Políticas de seguridad deficientes o inexistentes

Tener un marco normativo débil, expone a las organizaciones ante vulnerabilidades en los sistemas de información, las cuales pueden ser aprovechadas por atacantes. Las siguientes debilidades potencialmente podrían ser reguladas por un marco normativo eficiente:

- Políticas de contraseñas poco robustas, las cuales se podrían adivinar con facilidad, y que no son modificadas con una frecuencia adecuada.
- Deficiencia en el control de acceso a los sistemas, puesto que las cuentas de usuarios no son bloqueadas por una cierta cantidad de intentos fallidos.
- Control de acceso a los recursos deficiente, ya que los usuarios pueden acceder a los sistemas con permisos de acceso superior a los que necesitan.
- Debilidad en los procedimientos de soporte sobre los equipos de ofimática que utilizan los usuarios.
- Escaso control a empresas que nos brindan servicios informáticos.

- Deficiencia en el acceso físico al centro de cómputo que resguarda los servidores sensibles para la operación de la organización.
- Instalación de programas no homologados por la organización.
- Falta de política en la aplicación de parches de seguridad.
- Falta de política de clasificación de Información y procedimientos que indiquen como transmitir y almacenar los datos. Estas políticas regularían el tratamiento de los datos, evitando el almacenamiento y transferencia de datos sensibles sin cifrar. (p. 177)

E. Configuración inadecuada de los sistemas informáticos

Una inadecuada configuración en los sistemas informáticos posibilita explotar las vulnerabilidades que estos poseen desde su fabricación. Una de las más conocidas, es la utilización de contraseñas de los super usuarios por defecto, las cuales se pueden obtener de publicaciones en internet. (p.176)

F. Falta de capacitación adecuada a los usuarios y administradores de sistemas de información

Una de las mayores causas relacionadas a la seguridad de la información tiene origen en el factor humano. En consecuencia, es importante que los usuarios finales como los administradores de los sistemas, tengan la capacitación adecuada a su función. (p. 179)

G. Descuidos del fabricante

Los fabricantes en cierta forma han contribuido en la propagación de virus o malware, al incluir el código en los discos rígidos que vienen de fábrica o en los dispositivos de almacenamiento que contiene el software de instalación. Un ejemplo de esta vulnerabilidad es la empresa Creative, la cual creo un modelo de reproductor de MP3 Zen Neeon, este contenía un gusano informático que afectaba a los sistemas operativos Windows. (p. 182)

H. Existencia de puertas traseras en los sistemas de información

Esta vulnerabilidad llamada puerta trasera, es una vía de acceso no autorizada a un sistema, la que permite acceder a usuarios saltando las medidas de seguridad que provee la aplicación. (p. 181)

Es muy importante identificar las distintas causas que provocan las vulnerabilidades más conocidas, ya que son el punto de partida para poder subsanarlas.

Las causas antes mencionadas afectan las tecnologías operativas como para las redes industriales.

Métodos de mitigación de vulnerabilidades: Actualmente existen varias formas de mitigar las vulnerabilidades a las cuales están expuestos los sistemas informáticos de redes corporativas como los de redes industriales.

Las más relevantes son las siguientes:

- Patch Management (Administración de Parches).
- Establecer perímetros de seguridad.
- Formación básica para los usuarios y administradores.
- Implementar un Firewall.
- V.A. (Vulnerability Assessment o Evaluación de la Vulnerabilidad).
- IPS (Intrusión Prevention System o en español Sistema de Prevención de Intrusiones).
- IDS (Intrusión Detection System o en español Sistema de Detección de Intrusiones).

Del listado antes indicado, es imprescindible que se implemente un IDS y un IPS, con el fin de poder prevenir y detectar una gran cantidad de vulnerabilidades. El NIST publica el Estándar SP 800-94, el cual es una guía para detectar y prevenir intrusos sobre sistemas informáticos.

IPS (Sistema de Prevención de Intrusos): Según Vieites, Á. G. (2011), un sistema de prevención de intrusos es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas de información de ataques cibernéticos. Cabe mencionar, que los IPS actúan en las capas dos, tres, cuatros y siete del modelo OSI. Los IPS están muy relacionados con los IDS y se consideran como una extensión de estos ya que pueden bloquear ataques antes de que se materialicen.

Los IPS son clasificados en cuatro diferentes tipos:

- **Basados en Red LAN (NIPS):** monitorean la red LAN en busca de tráfico de red sospechoso, al analizar la actividad por protocolo de comunicación LAN.
- **Basados en Red Wireless (WIPS):** monitorean la red inalámbrica en busca de tráfico sospechoso al analizar la actividad por protocolo de comunicación inalámbrico.
- **Análisis de comportamiento de red (NBA):** Examina el tráfico de red para identificar amenazas que generan tráfico inusual, como ataques de denegación de servicio, ciertas formas de malware y violaciones a políticas de red.
- **Basados en Host (HIPS):** Se efectúa mediante la instalación de paquetes de software que monitoriza un host único en busca de actividad sospechosa.

Los IPS poseen las siguientes categorías.

- **Detección basada en firmas:** utilizando una base de firmas al igual que un antivirus.
- **Detección basada en políticas:** el IPS requiere que se declaren muy específicamente las políticas de seguridad.
- **Detección basada en anomalías:** en función con el patrón de comportamiento normal de tráfico.
- **Detección basados en estadísticas de anomalías:** el IPS analiza el tráfico de red por un periodo determinado estableciendo una línea base de comparación. Cuando el tráfico varía de esta línea base de comportamiento se genera una alarma.
- **Detección honey pot (jarra de miel):** funciona mediante la utilización de un equipo que llama la atención a los atacantes. Los atacantes utilizan sus recursos para tratar de ganar acceso en el sistema y dejan intactos a los sistemas verdaderos.

IDS (Intrusión Detection System): Según Vieites, Á. G. (2011), un sistema de detección de intrusos es un programa usado para detectar accesos no autorizados a una computadora o a una red, basado en sensores virtuales, permitiendo así evitar posibles ataques. Estos accesos pueden ser ataques de hackers, o de script que utilizan herramientas automáticas.

Existen cuatro tipos de sistemas de detección de intrusos:

- **HIDS - IDS basados en Host:** Pueden identificar tráfico malicioso que se origina en el propio host, evitando la propagación del malware. (p. 965)
- **NIDS - IDS basados en Red**: Examinan de forma pasiva del tráfico que circula por algún punto de la red en busca de intrusos. El NIDS debe ser implementado en un punto estratégico de la red para obtener mejores resultados. (p. 967)
- **DIDS – IDS distribuido:** Son parecidos a los NIDS, solo que distribuido en varios lugares de la red y envían alertas a un sistema centralizado. (p. 967)
- **IDS basados en log:** Revisa los archivos de logs en busca de posibles intrusos, se caracteriza por su precisión y completitud.

2.3.4 Política de Seguridad

Los objetivos, las estrategias y la política de seguridad se pueden definir para cada nivel de una organización y para cada área o departamento. Con el objeto de obtener una política de seguridad eficaz, es necesario tener muy claros los distintos focos, estrategias, riesgos y políticas para poder elaborar un marco normativo en materia de seguridad y

basado en riesgos, que logren satisfacer los requisitos establecidos. La política de seguridad según Vieites, Á. G. (2011), es una declaración de intención con un alto nivel, la cual debe cubrir la seguridad y los riesgos de los sistemas informáticos. (p. 122) Esta proporciona las bases para definir y delimitar responsabilidades en las diversas áreas de la organización, de esta política derivarán las distintas normativas que regulan el accionar sobre una determinada tecnología y los distintos procedimientos que detallarán los pasos a ejecutar para llevar a cabo una tarea determinada, alineada a la normativa y la política.

"Las políticas definen, qué se debe proteger en el sistema y los procedimientos indican cómo se debe llevar a cabo dicha protección" (Vieites 2011, p 125)

En la Tabla 1 se proporciona una visión del marco normativo, hasta llegar a una tarea específica. Es recomendable tener dicha visibilidad para poder entender en un alto nivel, qué se quiere proteger y cómo se está logrando.

Política	Normativa	Procedimiento	Tarea
Política de Seguridad de la Información	Norma de ABM de usuarios.	Controlar ABM de usuarios finales.	✓ Revisión semanal de bajas de usuarios desvinculados de la organización. ✓ Revisión diaria sobre la correcta alta de usuarios finales.
	Norma de control de logs.	Control de logs sobre Bases de Datos.	✓ Revisión semanal de logs para detectar acciones anómalas. ✓ Revisión a demanda de logs sobre las cuentas administradoras de las bases de datos.

Tabla 1: Modelo para tener un visión completa del marco normativo. Elaboración propia en base a la recomendación de la ISO 27001.

2.3.5 Estándares

ISO/IEC. ISO (International Organization for Standarization**)** es una organización internacional no gubernamental independiente, la cual reúne a los distintos expertos para compartir conocimiento y desarrollar estándares internacionales, los cuales son relevantes para el mercado que apoya la innovación y brindan soluciones a los desafíos globales. IEC (International Electrotechnical Commission) es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas. (Vieites, 2011)

Dentro de los estándares ISO/IEC, se encuentra la familia ISO/IEC 27000, los cuales son una serie de estándares relacionados con los sistemas de gestión de seguridad

informática (SGSI). Un sistema SGSI, tiene como objetivo fundamental garantizar la confiabilidad, disponibilidad e integridad de los datos. A continuación, se amplían estos tres conceptos importantes para un SGSI por Vieites (2011):

Confidencialidad: Es la forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados por la organización. (p. 65)

Disponibilidad: Es toda aquella información la cual puede ser accedida cuando se necesita a través de los canales adecuados siguiendo los procesos correctos. (p. 67)

Integridad: Es la forma en la cual la información se mantiene inalterada ante accidentes o intentos maliciosos. La información solo puede ser modificada mediante autorización. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información. (p. 66)

El estándar ISO/IEC 27001:2013 proporciona un marco de referencia para implementar, mantener y mejorar un sistema de gestión de seguridad informática (SGSI) dentro de una organización. Este sistema permite evaluar riesgos o amenazas que podrían poner en peligro información confidencial de las organizaciones permitiendo establecer controles para eliminar o minimizar los peligros a los que son expuestos los sistemas de información. Dicho estándar se encuentra enfocado en el ciclo de mejora continua el cual consiste en planificar-hacer-verificar-actuar (PDCA).

En la Figura 7 se puede visualizas cada una de las acciones que propone el estándar ISO 27001 utilizando el ciclo de mejora continua para un sistema de gestión de seguridad informática.

La norma ISO/IEC 27001 posee una estructura de once secciones y el anexo A. Las secciones cero a la tres son meramente introductorias y no son de carácter obligatorio, por otro lado, las secciones cuatro a la diez son de carácter obligatorias, es decir, las mismas deben estar en cumplimiento para poder realizar la certificación de dicho estándar.

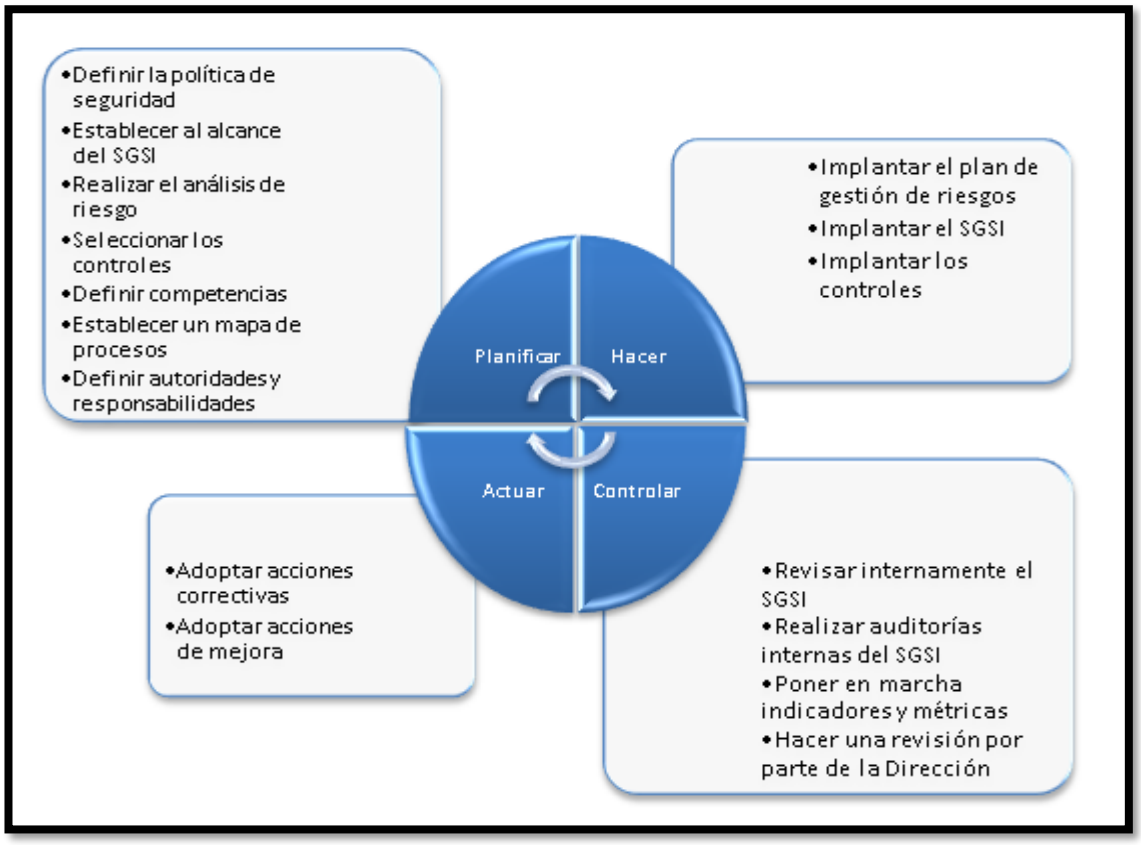

Figura 7: Permite tener una visual del modelo PDCA con las acciones a realizar para implementar un SGSI. Elaboración propia en base a la metodología propuesta por ISOTOOLS del Estándar ISO 27001.

Cabe destacar, que los controles declarados en el anexo A serán implementados siempre y cuando corresponda según su aplicabilidad.

La norma ISO/27001 es certificable por auditores externos, y esta puede ser adaptada a cualquier organización, sin importar su tamaño o que sea pública o privada. Si bien el hecho de certificar no garantiza que la organización sea segura en su totalidad, se puede obtener los siguientes beneficios:

• Lograr ventaja competitiva.

• Garantizar la gestión de la calidad.

• Controlar y reducir los riesgos operativos y comerciales.

• Cumplir con la legislación y normativa de cada país y sector.

• Poner en marcha procesos de mejora continua.

A continuación, se realiza un breve resumen preliminar de las secciones antes mencionadas, segregando las introductorias y las obligatorias las cuales representan a la estructura de la norma.

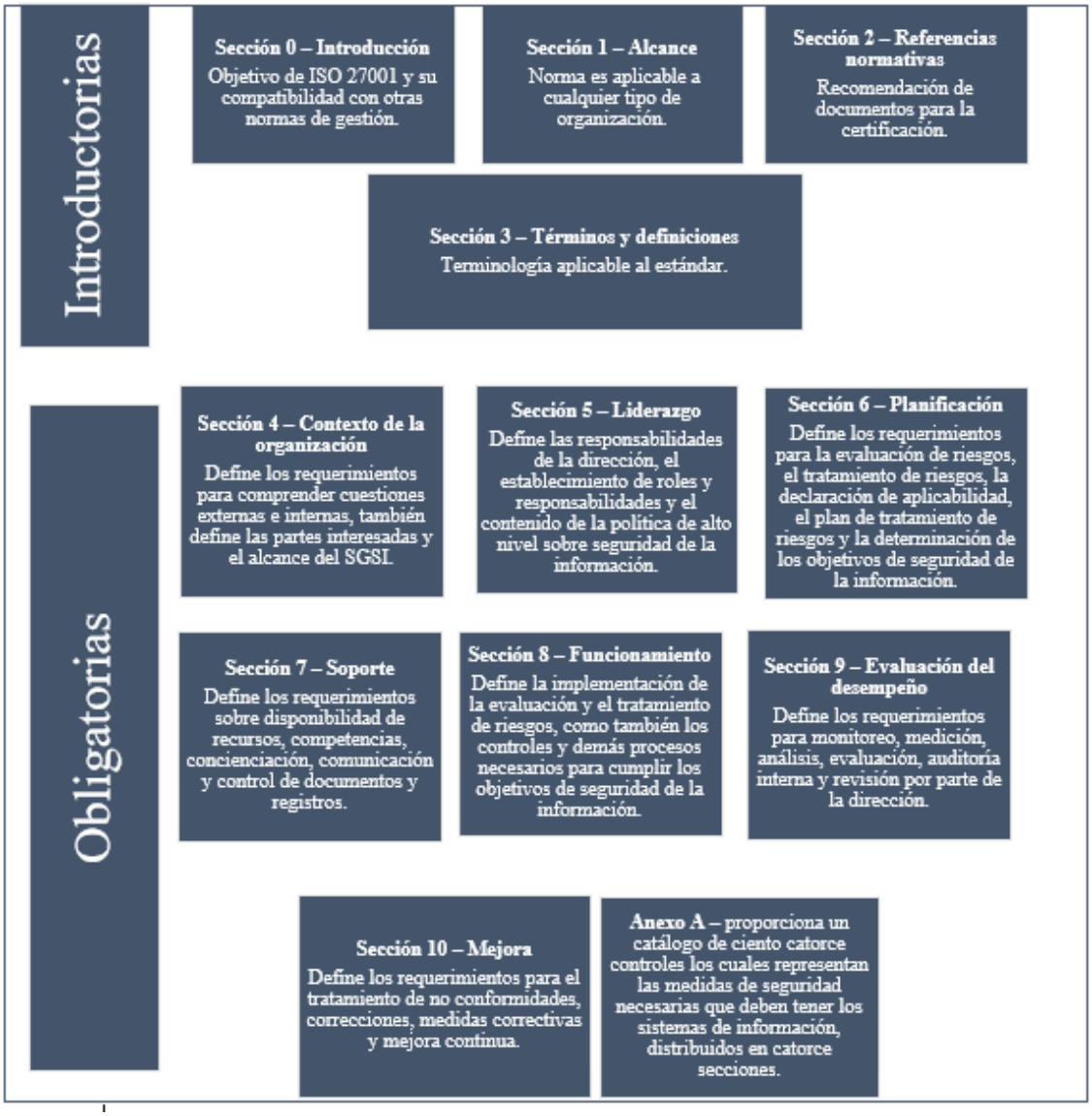

Figura 8: Permite tener una visual de las secciones propuestas por ISO 27001. Elaboración propia en base a la estructura de norma ISO 27001.

ISA: La International Society of Automation (ISA), publicó la norma IEC 62443 la cual es un conglomerado de estándares basados en la norma **ISA99**. La norma IEC 62443 contiene las mejores prácticas del mercado para robustecer la seguridad de los sistemas de control industrial.

Dentro de la norma ISA 99 (2021) se encuentran cuatro documentos y dos informes técnicos. Cabe destacar, que la norma ISA 99 se encuentra segregada en cuatro capas las cuales se detallan a continuación:

1) **General** – Contiene conceptos básicos y contexto del desarrollo de las capas siguientes.

2) **Políticas & Procedimientos** – Consiste en la definición de políticas y procedimientos.
3) **Sistema** – Propone las mejores prácticas para una implementación segura en entornos industriales.
4) **Componentes** – Indica los requerimientos a cumplir por los fabricantes de dispositivos industriales con el fin de que sean considerados secured by design.

ISA-95: Dentro de los estándares ISA, podemos encontrar el estándar ISA-95 el cual trata la integración de empresas y sistemas de control, estableciendo cinco niveles.

Estos niveles son:

0) **El proceso –** Proceso industrial en sí mismo, la maquinaria y los recursos humanos necesarios.
1) **La automatización –** Interacción entre la parte física con los sistemas de control más básicos como pueden ser los PLCs y sus periféricos, sensores y actuadores en general.
2) **La interface humana –** Interacción del hombre con los elementos de la planta, utilizando los HMI o monitores de operarios en donde se pueden encontrar las pantallas de operador que controlan un determinado proceso y los sistemas SCADA.
3) **Históricos y enlace con el último nivel –** En este nivel se encuentran los historian, los cuales son una base de datos donde guardan todo aquello que reciben de la planta, desde medidas de los sensores, producción, paradas de emergencias, entre otros. Por otro lado, tenemos al MES, el cual es interface entre el nivel cuatro y el nivel dos.
4) **El cerebro empresarial –** En este nivel se encuentran los programas económicos, contables y de marketing. Se puede encontrar los ERP y los BI entre otros.

NIST: El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia de la administración de tecnología del departamento de comercio de los Estados Unidos. Fue fundada en 1901 por el congreso de los Estados Unidos y tiene como misión promover la innovación y la competencia industrial en los Estados Unidos. NIST tiene un marco de ciberseguridad que consta de estándares, pautas y mejores prácticas para la gestión de riesgos cibernéticos sobre las infraestructuras críticas, dicho marco fue creado a pedido del ex presidente de los EE. UU. Barack Obama en febrero del 2013 debido al incremento de incidentes de ciberseguridad que se producían en EE. UU. Este marco

posee como enfoque principal, promover la protección y la resistencia de la infraestructura crítica ante ciberataques.

Siendo más específico dentro del marco NIST, se encuentra la NIST SP 800-82 R2 la cual es una guía se seguridad para los sistemas de control industrial ICS. Adicionalmente nos orienta a brindar seguridad a los siguientes componentes de una red industrial:

- Sistemas de control de supervisión y adquisición de datos (SCADA)
- Sistemas de control distribuidos (DCS)
- Controladores lógicos programables (PLC)

Cabe destacar que el framework NIST se compone de tres partes, estas son:

- El núcleo del marco
- Los niveles de implementación del marco
- Los perfiles de dicho marco

En la Figura 9 (Elaboración propia en base a - NIST Framework for Improving Critical Infrastructure Cybersecurity V1.1) se puede apreciar una visión general del framework de ciberseguridad NIST con sus distintos componentes.

El framework NIST propone siete pasos para la implementación o mejora de un programa de ciberseguridad los cuales se detallan a continuación:

Priorización y definición de alcance: Identificación de objetivos y misión del negocio en conjunto con las prioridades en términos organizacionales. El alcance puede ser la organización es su completitud, una línea de negocio o un proceso.

Orientación: Identificación de sistemas, activos, requerimientos regulatorios, amenazas y vulnerabilidades.

Crear un perfil actual: Aplicando las funciones del framework se obtiene un perfil actual de la ciberseguridad en la organización.

Ejecutar un análisis de riesgos: Ejecución de análisis de riesgo con el fin de obtener la probabilidad y el impacto de eventos de ciberseguridad en el alcance que se desea analizar.

Crear un perfil objetivo: Establecer objetivos en cuanto a ciberseguridad que se desea alcanzar luego de aplicar el framework.

Determinar, analizar y priorizar las brechas detectadas: Se identifican las diferencias entre el perfil actual y el perfil objetivo con el fin de crear el plan de acción que deberá ejecutar la organización para llegar al grado de madurez esperado.

Implementar el plan de acción: Se procede a abordar el plan de acción priorizado con el fin de alcanzar el perfil objetivo.

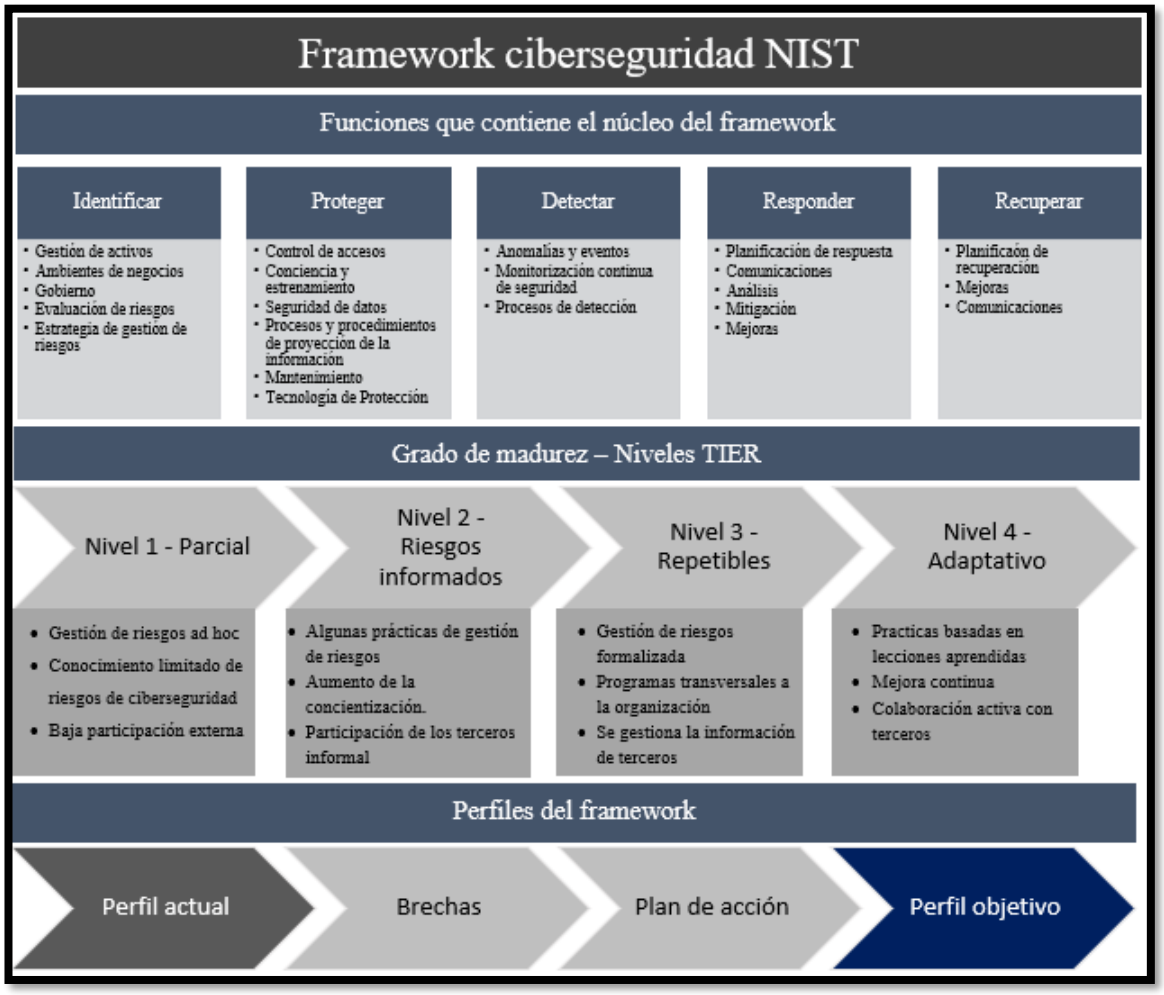

Figura 9: Permite tener una visual completa del framework NIST para Ciberseguridad.

Cabe destacar, que las acciones que se implementan se deben ejecutar dentro de un entorno de mejora continua, optimizando los controles de seguridad y que estos puedan evolucionar dentro del framework. (Sedgewick, A. 2014.)

2.3.6 Riesgos de ciberseguridad

Una buena práctica que recomiendan los estándares internacionales es la gestión de los riesgos cibernéticos, identificando el impacto en el negocio por un fallo de seguridad que suponga la perdida de la confidencialidad, integridad y disponibilidad de un activo de información.

Conceptualmente, un riesgo consiste en el impacto y la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto sobre la organización. (Magerit, 2012)

Tipos de riesgos

- **Riesgo inherente:** Corresponde al riesgo existente ante la ausencia de una acción que altere el impacto o la probabilidad.
- **Riesgo residual:** Es el nivel de riesgo que persiste luego de haber ejecutado las acciones definidas.

Metodologías de gestión de riesgos para el mundo IT

De las metodologías existentes, las más destacadas son MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) la cuales nos permiten realizar un análisis de riesgo a una organización determinada.

La metodología MAGERIT fue creada por el consejo superior de Administración Electrónica del Gobierno de España, para minimizar los riesgos de la implantación y uso de las tecnologías de la información. Los objetivos principales de según Magerit (2012) son:

- Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de adoptar las medidas para limitar su impacto. (p. 8)
- Ofrecer un método sistemático para analizar los riesgos identificados. (p. 8)
- Planificar las medidas oportunas para mantener los riesgos identificados bajo control. (p. 8)
- Facilitar todos los procesos de evaluación, auditoria, certificación o acreditación. (p. 8)

La metodología OCTAVE, fue desarrollada por el SEI (Sowtware Engineering Institute). Esta metodología agiliza el proceso de evaluación de riesgos de seguridad sobre los sistemas informáticos.

Los objetivos de OCTAVE Allegro (2007) son:

- Desarrollar una perspectiva de seguridad dentro de una organización, teniendo en cuenta todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad dentro de la organización. (p. 1)
- Permitir la comprensión del manejo de los riesgos. (p. 1)
- Clasificar los componentes de la empresa en activos y ordenarlos de acuerdo con su importancia en amenaza y vulnerabilidad. (p. 1)

Estas dos metodologías de análisis de riesgos son útiles para las organizaciones con el fin de prevenir y controlar las amenazas. Es decir, nos permite anticiparnos a

potenciales pérdidas de información, vulnerabilidades en un sistema de seguridad e implementar los controles necesarios de forma oportuna a fin de que reduzcan el riesgo detectado.

Una de las metodologías para la gestión del riesgo en el mundo OT es la que propone la norma ISA99/IEC 62443, la cual posee un framework de referencia internacional de ciberseguridad en sistemas industriales, la misma nos permite evaluar la madurez en cuanto a ciberseguridad en un sistema de control estableciendo distintos niveles. Es importante destacar que esta norma tiene como prioridad la disponibilidad y la integridad de los sistemas ante amenazas cibernéticas.

El estándar consta de tres fases; evaluación, desarrollo e implementación y mantenimiento. Esta metodología se puede aplicar a sistemas industriales de gran envergadura y de diferentes industrias. Se introduce el concepto de zonas, conductos y canales, dando un gran aporte en el análisis de riesgos de grandes sistemas industriales.

Las zonas son una agrupación física o lógica de activos industriales que comparten el mismo requerimiento de seguridad. Los conductos son un tipo particular de zona, y agrupan las comunicaciones que permiten la transmisión de información entre las distintas zonas. Por otro lado, se encuentra el concepto de canal, que son vínculos de comunicaciones dentro de un conducto.

El enfoque que se debe dar a los riesgos en redes industriales es distinto al de IT ya que, entre los riesgos de OT, se pueden encontrar como típicos: los riesgos de muerte o lesión, daño ambiental y violaciones a regulaciones ambientales entre otros.

2.3.7 Incidentes de Ciberseguridad

La falta de conocimiento sobre los incidentes de seguridad ocurridos son una complicación para la ejecución de tareas preventivas. A la fecha existen varias bases de datos de incidente de ciberseguridad que afectan a varios sistemas, que en su gran mayoría son sistemas SCADA. Según la información extraída del sitio web Risidata (2021), que contiene una gran base de datos de incidente de ciberseguridad, explica en detalle el tratamiento que se realiza en los incidentes de seguridad. Estas bases de datos tienen como objetivo recolectar, analizar y compartir los incidentes que afectan a diferentes empresas con el fin de compartir las experiencias que hayan podido tener las organizaciones afectadas. Estos ataques pueden ser del tipo externo, un incidente accidental, una denegación de servicio, un gusano o un virus.

Los datos que recolectan estas organizaciones pueden ser de tres fuentes diferentes:

- Los incidentes se recolectan con acuerdos de distribución de datos con socios estratégico.
- Una búsqueda constante en todas las fuentes públicas como bases de datos, grupos de noticias e internet en busca de cualquier indicio de algún incidente que haya sucedido.
- Mediante la colaboración de miembros asociados, que pueden ser empresas que trabajan en infraestructura critica.

Luego de realizar un reporte sobre un incidente, se protege la confidencialidad de la empresa, cualquier información confidencial se debe borrar con el fin de no afectar la reputación de la misma. Como segundo paso, se estudia el incidente ocurrido utilizando técnicas estándares y a cada incidente se le asigna una de las cuatro clasificaciones.

- Confirmado
- Probable pero no confirmado
- Desconocido o poco probable
- Engaño conocido / leyenda urbana

Luego de confirmar el incidente, pasa a formar parte de la base de datos y este será utilizado como recurso para afrontar futuros incidentes.

El incidente informático sobre una infraestructura crítica que más repercusión tuvo fue el Stuxnet, concebido para atacar dispositivos Siemens que tenían como vulnerabilidad a usuarios con contraseñas por defecto. Luego de infectar a la maquina se carga la configuración de los dispositivos a un servidor central para que el atacante pueda elegir el objetivo y reprogramar lo que el dispositivo ejecuta. Su primera detección data de junio de 2010, se lo consideró un gusano, ya que se aprovechó de vulnerabilidades de los sistemas para propagarse e infectar diversas máquinas y rootkit siendo capaz de modificar el comportamiento de distintos componentes del sistema y ocultar su presencia para no ser detectado. La complejidad de este malware es llamativa y pone en manifiesto la participación de un amplio equipo de programadores de distintas disciplinas con un importante apoyo económico en su creación. En el año 2012 el New York Times confirma la intervención de los gobiernos de Estados Unidos e Israel en el financiamiento de este proyecto cuyo objetivo final era paralizar el plan nuclear iraní. (David E. Sanger, 2012, NYT)

La principal vía de infección fue a través de llaves USB, aprovechando una vulnerabilidad 0-day que permitía la ejecución automática de los archivos binarios de Stuxnet, con solo visualizar con Windows Explorer los archivos alojados en la memoria

USB. Otra vía de infección fue a través de los recursos de red compartidos en los que la máquina infectada tenía permisos de escritura. La finalidad del rootkit era alterar la programación de los PLC y ocultar las modificaciones realizadas, de tal manera que los usuarios que tratasen de examinar el programa del PLC, desde un host Windows comprometido, no se dieran cuenta de dicha modificación. Stuxnet poseía unos setenta bloques de función (function blocks), con los cuales era capaz de modificar los programas de los PLC y a través de estos cambiar los parámetros de los variadores de velocidad (drives), que controlaban las bombas centrífugas que intervenían en el proceso de enriquecimiento de uranio.

Stuxnet llevó a cabo dos ataques diferentes. En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido, durante unos quince minutos, antes de volver a la velocidad normal. Luego, aproximadamente un mes después, desaceleró las centrifugadoras durante unos cincuenta minutos. Esto se repitió en distintas ocasiones durante varios meses. Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas mil, salieran de servicio. Durante el ataque cibernético, alrededor del veinte por ciento de las centrifugadoras en la planta de Natanz, en Irán, quedaron inutilizadas. Como consecuencia de lo antes indicado, el enriquecimiento de uranio cerró durante una semana en noviembre del 2010. (Risidata, 2021)

En los últimos años existieron ataques importantes que pusieron en riesgo no solo a las infraestructuras críticas y la continuidad de negocio, sino también a las vidas humanas.

A continuación, se realiza una selección de ciberataques en redes industriales que tuvieron relevancia en distintas industrias, poniendo en evidencia las distintas vulnerabilidades que pueden ser explotadas por los atacantes. La información es obtenida de la base de datos Risidata (2021), que contiene una gran base de datos confiables con los distintos incidentes reportados y confirmados.

Tipo de industria: Petróleo

Año del evento: 2012

Fiabilidad: Confirmado

País: Arabia Saudita

Descripción: La compañía petrolera nacional de Arabia Saudita, Aramco, indicó que un ataque cibernético dañó aproximadamente treinta mil computadoras. El ataque tenía como objetivo detener la producción de petróleo y gas en Arabia Saudita. La compañía

cerró su red interna principal durante más de una semana. El virus informático, Shamoon, se propagó a través de la red de Aramco y limpió los discos duros de las computadoras. Afortunadamente, el daño se limitó a las computadoras de oficina y no afectó el software de los sistemas que afectaría las operaciones técnicas.

Los hackers de un grupo llamado "Cutting Sword of Justice" se atribuyeron la responsabilidad del ataque. Sus motivos eran políticos. El virus les dio acceso a documentos en las computadoras de Aramco. Amenazaron con liberar documentos, pero no lo hicieron.

Impacto: Fuga de información en treinta mil computadoras de oficinas por el ataque del virus Shamoon. No se vieron afectadas las operaciones técnicas.

Análisis: El riesgo que se materializó es la fuga de información, y la perdida de los datos almacenados en reposo.

Tipo de industria: Fabricación general

Año del evento: 2006

Fiabilidad: Confirmado

País: Rusia

Descripción: Servidores SCADA redundantes tenían problemas de conexión entre ellos, luego de habilitar el antivirus, se encontraron numerosas instancias del troyano “generic backdoor.k”.

Impacto: Varios ingenieros tuvieron que realizar distintas pruebas en todas las máquinas.

Análisis: Servidores SCADA, presentaron fallas en su funcionamiento producto de troyanos que tenían almacenados.

Tipo de industria: Rieles

Año del evento:2014

Fiabilidad: Confirmado

País: Alemania

Descripción: Varios atacantes utilizaron un ataque avanzado de ingeniería social para obtener acceso a la red de la empresa y luego se abrieron paso hacia la red del sistema de control. Esto dio lugar a un incidente en el que un horno no se podía apagar de la manera habitual y el horno estaba en una condición indefinida que resultó en daños masivos en todo el sistema.

Impacto: Se detuvo la operación por un lapso de tiempo, por no poder apagar un horno de la manera habitual, lo que resultó en daños masivos en todo el sistema.

Análisis: Se presentaba un débil gobierno de las identidades, mediante métodos de ingeniería social pudieron ingresar a los sistemas de la compañía.

Tipo de industria: Energía y utilidades

Año del evento: 2004

Fiabilidad: Confirmado

País: Estados Unidos

Descripción: Las estaciones de trabajo del operador SCADA se vieron afectadas por el virus del gusano W32 / Korgo. Estos tres terminales estaban en la intranet corporativa fuera del firewall SCADA.

Impacto: Instalación inmediata de un parche de Microsoft en todas las estaciones de trabajo afectadas para corregir el problema. Luego se implementó el software antivirus y el mismo parche de Microsoft en todas las demás estaciones de trabajo SCADA.

Análisis: Los equipos SCADA, tenían un bajo nivel de parches de seguridad, y la red se encontraba desprotegida sin ningún firewall.

Como se puede apreciar en estos casos, el impacto puede ser muy alto, debido a esto, es de suma importancia seguir las buenas prácticas del mercado de seguridad para poder prevenir estos ataques.

En la Figura 10 obtenida de un informe realizado por la reconocida consultora de EE. UU. DVC (Data Collective, DCVD, 2019) del sector de capital de riesgo y capital privado, se puede apreciar los incidentes de ciberseguridad según la industria, como se puede ver, el sector energía es el más impactado en todos estos ataques.

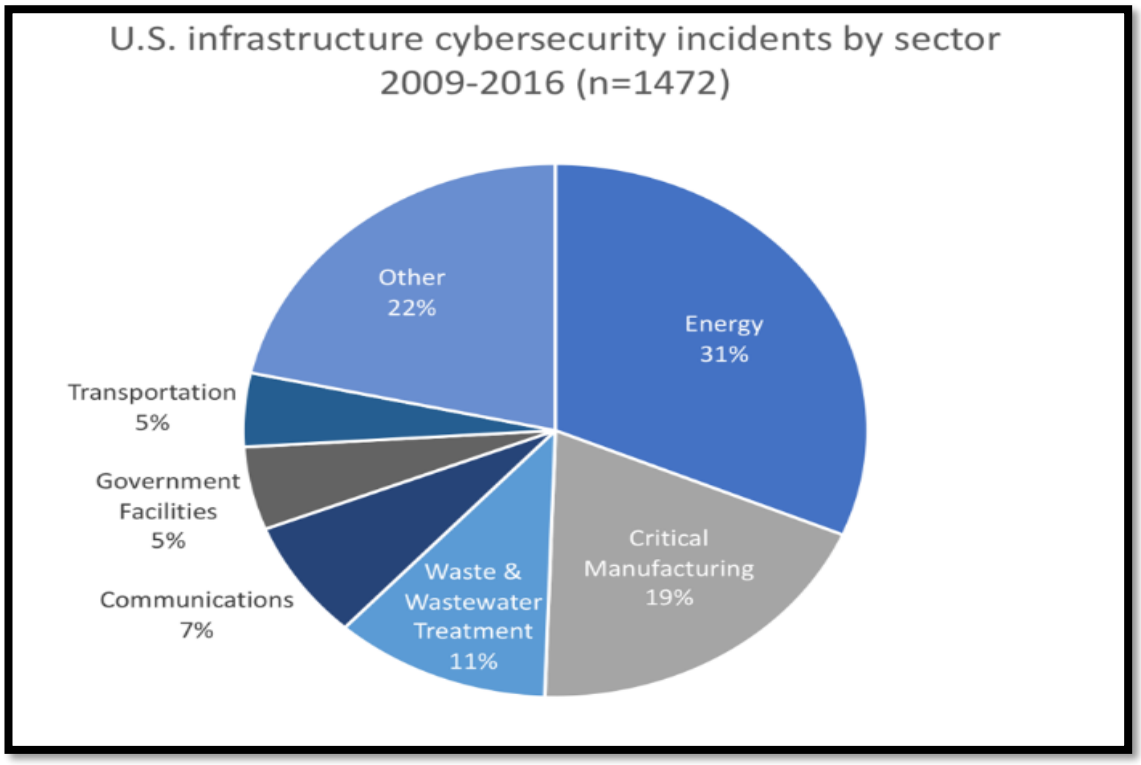

Figura 10: Incidentes de seguridad segregado por industria, según informe realizado por DVC durante el 2019.

Con respecto a los incidentes de ciberseguridad en América Latina y el Caribe existe el observatorio de ciberseguridad impulsado por el Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA) que ayuda a presentar una imagen completa y actualizada del estado de la seguridad cibernética de los países de América Latina y el Caribe como así también, poder entender el grado de madurez que tiene cada país.

Por otro lado, en Argentina se creó la "Dirección Nacional de Ciberseguridad", bajo el Ministerio de Modernización, el cual tiene como misión el desarrollo de estrategias y mecanismos para la protección de la información y los servicios del Estado Nacional y sus ciudadanos, otro punto muy importante es la coordinación de la gestión de incidentes a nivel nacional.

En otra medida, la Ciudad Autónoma de Buenos Aires, tiene su propio centro de ciberseguridad BA-CSIRT, el cual se dedica a dar asistencia y concientización a los ciudadanos y al Gobierno de la Ciudad de Buenos Aires en todo lo relacionado a la seguridad de la información.

A continuación, se realiza una breve descripción de los incidentes de seguridad destacados durante los últimos años.

[IT] Airbus, el segundo mayor fabricante mundial de aviones comerciales, fue objeto de una violación de datos que expuso información personal de algunos empleados producto de un quebrantamiento malicioso en su sistema comercial (Commercial Aircraft business). (Airbus, 2019).

[IT] Según Noticias Ciberseguridad (2020) dos páginas web relacionadas con el aeropuerto internacional de San Francisco, SFOConnect.com, que proporciona actualizaciones sobre el aeropuerto a pasajeros, y SFOConstruction.com, que contiene información sobre proyectos de construcción en el aeropuerto, fueron víctimas de un ciberataque cuyo objetivo fue la obtención de las credenciales de autenticación de los usuarios. Una vez que el ciberataque, fue identificado, ambos portales web fueron desconectados y se procedió a eliminar el código malicioso. Además, se forzó el reseteo de todas las contraseñas relativas al correo electrónico y al acceso a la red del aeropuerto.

[OT] En base a la información extradía de Baufest (2020) **e**l proveedor de energía estatal sudafricano "Eskom" experimentó dos violaciones de seguridad. Una base de datos no segura que contenía información de clientes se expuso en internet y por otro lado hubo una computadora corporativa que se infectó con el troyano AZORult el cual roba información, dicha infección se produjo luego de que un empleado descargó un juego crakeado.

[**OT**] Según los datos obtenidos de us-cert.cisa.gov (2021), se comprometió una planta potabilizadora de agua en febrero del 2021, los atacantes tuvieron acceso remoto a los sistemas SCADA de una instalación de agua potable de Estados Unidos, aumentando la cantidad de hidróxido de sodio como parte del tratamiento del agua. El riesgo no se llegó a materializar puesto que el personal de la planta logro corregir el problema.

[OT] En base a la información obtenida de CERT. E (2020) Petróleos Mexicanos fue blanco de un ataque con ransomware en el área del centro de cómputo SITE, de sus oficinas en el estado de México. Los sistemas de PEMEx se vieron vulnerados por la infección de un virus el cual tenía la capacidad de bloquear la pantalla de un equipo o cifrar archivos predeterminados con contraseña. Los atacantes pedían un rescate equivalente a cinco millones de dólares en bitcoin.

Ciber incidentes 2020.

Según el último informe emitido por la compañía de seguro Allianz Ranking Allianz Barometer (2020) el cual tuvo como objetivo plantear los principales riesgos de negocio, posiciona a los incidentes de ciberseguridad como primeros en su ranking, en

donde indican un crecimiento de forma considerable. En la Figura 11 obtenida del informe Ranking Allianz Barometer (2020) se puede identificar el aumento con respecto al año 2019, posicionándolo primero en el ranking.

Rank		Percent	2019 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**39%**	2 (37%)	▲
2	Business interruption (incl. supply chain disruption)	**37%**	1 (37%)	▼
3	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**27%**	4 (27%)	▲
4	Natural catastrophes (e.g. storm, flood, earthquake)[1]	**21%**	3 (28%)	▼
5	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**21%**	5 (23%)	=

Figura 11: Ranking de los principales riegos según la compañía de seguros Allianz.

Ciberseguridad y COVID-19.

Al comenzar el año 2020 el mundo fue alertado por una pandemia debido al COVID-19. Una de las medidas tomadas por los distintos gobiernos, fue el aislamiento social y preventivo de las personas evitando la circulación y la presencia en oficinas, plantas, refinerías etc. Estas medidas privaron el acceso a los sistemas IT y OT a los empleados, sin poder realizar las tareas diarias. Provocando un desafío para los equipos de tecnología informática ya que en un corto plazo debieron preparar sus sistemas para el acceso remoto. Esta urgencia, potencialmente puede provocar un fortalecimiento ineficiente de los sistemas y sin las medidas de seguridad adecuadas.

Por otro lado, las personas tienen un cambio radical en su forma de trabajo, en términos de la comunicación y la gestión de equipos, teniendo que utilizar distintas herramientas para realizar videoconferencias. Cabe destacar, que no todas las herramientas tienen el grado de madurez de seguridad adecuado y adicionalmente los usuarios no poseen la capacitación suficiente para realizar un uso responsable de estas herramientas.

Como para tener una visión cuantitativa de los ataques producidos, en la Figura 12 obtenida de un informe emitido por la empresa líder en productos y servicios de ciberseguridad Checkpoint se puede apreciar los ciberataques relacionados con coronavirus (“COVID-19 Risks Outlook, a Preliminary Mapping and Its Implications” mayo 2020. -World Economic Forum).

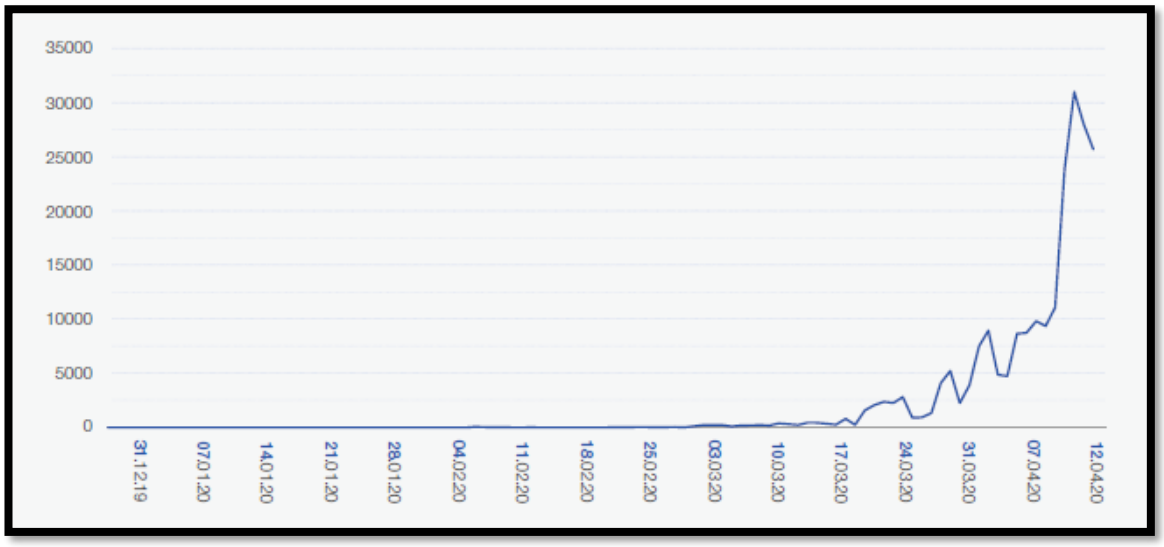

Figura 12: Se puede visualizar el crecimientos de los ciberataques relacionados con el Coronavirus.

Estos ataques están relacionados con casos de phishing, sitios web con la palabra “corona” /” COVID” en su dominio, archivos cuyo nombre es “Corona” o archivos que fueron distribuidos por correo electrónico los cuales se trataba el tema coronavirus.

Capítulo 3 – Desarrollo técnico

3.1 Convergencia

3.1.1 Presentación resumida

En el presente capítulo se muestran los nuevos riesgos de seguridad de la información en los ICS que surgen tras la convergencia entre las tecnologías IT y OT, a su vez se presenta una propuesta para mitigarlos.

Se introduce una comparación entre estas tecnologías culturalmente tan diversas que convergen: IT y OT, configurando un nuevo concepto orientado hacia la eficiencia como lo es la industria 4.0. Aquí se introducen nuevos riesgos en la seguridad de la información de los ICS. Luego se muestran enfoques y prioridades de ambas tecnologías, que en muchas situaciones se contraponen, lo cual genera riesgos adicionales. Continúa con la presentación de la conectividad entre ambos tipos de redes, lo cual materializa la existencia de estos riesgos transformándolos ya en vulnerabilidades.

Se presenta un abordaje para la mitigación de estos riesgos basada en una arquitectura de red segregada con firewalls, con políticas y con controles que eviten la materialización de los riesgos que implica la libre interconexión. Cabe destacar que esta es una de las medidas más importantes en cuanto a las protecciones de las redes ya que el hecho de no tener un firewall aumenta la probabilidad de que se materialice un ataque.

Este capítulo finaliza con el análisis de los resultados obtenidos, exponiendo que no se debe abordar la ciberseguridad en IT y OT con un mismo enfoque, se debe tener una estrategia de ciberseguridad holística y basarse en los estándares internacionales para proteger ICS.

3.2 Industria 4.0: Los nuevos riesgos tras la convergencia IT y OT

3.2.1 Comparación entre ICS (Tecnología OT) y sistemas IT tradicionales

En principio los sistemas de control industrial eran muy distintos con respecto a los sistemas tradicionales, de hecho, estaban totalmente desconectados. Los ICS se encontraban aislados con sistemas que ejecutan los protocolos de control propietarios, utilizando hardware y software especializado. En la actualidad este escenario está cambiando, los dispositivos con protocolo de internet (IP) se encuentran ampliamente disponible y a un bajo costo, están reemplazando a las soluciones propietarias, lo que aumenta la posibilidad de las vulnerabilidades de ciberseguridad e incidentes. Dado que los ICS están adoptando soluciones de IT para promover la conectividad empresarial y capacidades de acceso remoto, se diseñaron e implementaron el uso de computadoras

estándar de la industria, los sistemas operativos y protocolos de red están empezando a parecerse a los sistemas de IT. Esta integración es compatible con las nuevas capacidades de IT y proporciona significativamente, menos aislamiento para los ICS del mundo exterior, creando una mayor necesidad de garantizar la seguridad de estos sistemas. Mientras que las soluciones de seguridad han sido diseñadas para hacer frente a estos problemas en los sistemas típicos de IT, se deben tomar precauciones especiales al introducir estas mismas soluciones a los entornos ICS.

En la siguiente lista, se puede apreciar los diferentes requerimientos o enfoques que se deben tener ante la convergencia de un sistema IT y un ICS:

Requerimientos de rendimiento: Para los ICS por lo general el tiempo de respuesta es crítico en base a los criterios de los niveles aceptables de retardo dictados por la instalación individual. Algunos sistemas requieren respuestas definidas. Un alto rendimiento normalmente no es esencial para el ICS. En contraste, los sistemas de IT suelen requerir un alto rendimiento y pueden soportar un cierto nivel de retardo. Teniendo en cuenta que los ICS no tienen equipos de alto rendimiento generalmente, se debe tener mucho cuidado al momento de realizar escaneos de vulnerabilidades sobre estos ya que podrían interrumpir los procesos productivos.

Requisitos de disponibilidad: Muchos procesos de un ICS son de naturaleza continua. Interrupciones inesperadas de los sistemas que controlan los procesos industriales no son aceptables. Las interrupciones a menudo deben ser planificadas y programadas con días / semanas de antelación. Para asegurar la alta disponibilidad de un ICS es esencial realizar pruebas de pre-despliegue de una forma exhaustiva. Además de los cortes inesperados, muchos sistemas de control no se pueden detener con facilidad sin afectar la producción.

En algunos casos, los productos que se fabrican o el equipo que se utiliza es más importante que la información que se transmite. Por lo tanto, el uso de estrategias de IT típicos tales como reiniciar un componente, por lo general no son soluciones aceptables debido al impacto adverso sobre los requisitos de alta disponibilidad, confiabilidad y facilidad de mantenimiento del ICS. Algunos ICS emplean componentes redundantes, a menudo corriendo en paralelo, para dar continuidad cuando los componentes principales no están disponibles.

Requisitos de Gestión del Riesgo: En un sistema típico de IT, la confidencialidad y la integridad de los datos suelen ser las principales preocupaciones. Para los ICS, la seguridad humana y la culpa para evitar la pérdida de la vida o la puesta en peligro de la salud pública o la confianza, el cumplimiento regulatorio, pérdida de equipos, pérdida de

propiedad intelectual, productos perdidos o dañados, son las principales preocupaciones.

El personal responsable del funcionamiento debe entender la importancia del vínculo entre asegurar y mantener operativo el ICS.

Foco de la Arquitectura de Seguridad: En un sistema típico de IT, el foco principal de la seguridad es la protección de la operación de los activos de IT, ya sea centralizado o distribuido, y la información en reposo o en tránsito entre estos activos. En algunas arquitecturas, la información almacenada y procesada en el centro es más crítica y se le concede más protección. Para un ICS, los clientes de borde (por ejemplo, PLC, estación del operador, regulador DCS) deben ser protegidos cuidadosamente, ya que son directamente responsables del control de los procesos finales. La protección del servidor central sigue siendo muy importante en un ICS, ya que el servidor central podría tener un impacto negativo en cada dispositivo periférico.

Interacción física: En un sistema típico de IT, no hay interacción física con el medio ambiente. Los ICS pueden tener interacciones muy complejas con los procesos y las consecuencias físicas en el ámbito del ICS pueden manifestarse en eventos físicos. Todas las funciones de seguridad integradas en el ICS deben ser probadas (por ejemplo, fuera de línea en un ICS comparable) para demostrar que no se comprometa la funcionalidad normal de ICS.

Respuestas en tiempo real: En un sistema típico de IT, el control de acceso se puede implementar sin tener en cuenta el flujo de datos. Para algunos ICS, el tiempo de respuesta automatizada o respuesta del sistema a la interacción humana es muy crítico. Por ejemplo, lo que requiere la autenticación con contraseña y autorización en un panel de operador, no debe obstaculizar o interferir con las acciones de emergencia para un ICS. El flujo de información no debe ser interrumpido o comprometido. El acceso a estos sistemas debe restringirse por rigurosos controles de seguridad física.

Funcionamiento del sistema: En los ICS los sistemas operativos y aplicaciones pueden no tolerar prácticas típicas de seguridad de IT. Las redes de control suelen ser más complejas y requieren un nivel diferente de experiencia (por ejemplo, las redes de control se gestionan normalmente por los ingenieros de control, no el personal de IT). El software y hardware son más difíciles de actualizar en una red de sistemas de control operacional.

Los sistemas de control en su mayoría no soportan la posibilidad de encriptación de datos en tránsito o en reposo y no poseen logs de actividades.

Limitaciones de recursos: Los ICS y sus operaciones en tiempo real son a menudo sistemas que generalmente no incluyen las capacidades típicas de seguridad de IT con

recursos limitados. Puede que no haya recursos informáticos disponibles en los componentes de ICS para adaptar estos sistemas con capacidades de seguridad actuales.

Además, en algunos casos, las soluciones de seguridad de terceros no pueden ser aplicadas debido a la licencia del proveedor de los ICS, a los acuerdos de servicio y puede ocurrir la pérdida de soporte, si las aplicaciones de terceros se instalan sin el reconocimiento o aprobación de proveedores.

Vida útil de los componentes: Los componentes de IT típicos, tienen una vida útil del orden de tres a cinco años debido a la rápida evolución de la tecnología. Para un ICS donde la tecnología se ha desarrollado en muchos casos para el uso y la aplicación muy específica, la vida útil de la tecnología utilizada a menudo está en el orden de quince a veinte años y a veces más.

Gestión de Cambios: La gestión del cambio es fundamental para mantener la integridad de IT y sistemas de control. El hecho de no tener parches de software actualizados representa una de las mayores vulnerabilidades a un sistema. Las actualizaciones de software en los sistemas de IT, incluyendo los parches de seguridad, se aplican normalmente en el momento oportuno en base a las políticas y procedimientos de seguridad apropiados. Además, estos procedimientos se han automatizado utilizando herramientas basadas en servidor. Las actualizaciones de software de los ICS no siempre pueden ser implementadas de manera oportuna debido a que estos cambios tienen que ser probados a exhaustivamente por el proveedor de la aplicación de control industrial y el usuario final de la aplicación antes de ser implementados. Los cortes en los ICS a menudo deben ser planificados y programados días / semanas por adelantado. El ICS también puede exigir la renovación como parte del proceso de actualización. Otro problema que se pude encontrar en muchos ICS es que utilizan las versiones de sistemas operativos que ya no están soportados por el proveedor. En consecuencia, los parches disponibles pueden no ser aplicables. La gestión del cambio es también aplicable a hardware y firmware.

El acceso a los componentes: Componentes de IT típicos son generalmente locales y de fácil acceso, mientras que los componentes de un ICS pueden encontrarse a mucha distancia, y requieren gran esfuerzo físico para poder acceder a ellos.

3.2.2 Enfoques y prioridades entre IT y OT

Según el estándar ISO 27001, plantea tres principios básicos de seguridad de la información, los cuales son: confidencialidad, disponibilidad e integridad. Estos, no aplican de la misma medida en estos dos mundos, de hecho, las prioridades se invierten. En el mundo OT lo más importantes es que se mantenga de forma constante el proceso

industrial en funcionamiento, ejemplo: no se puede parar un proceso de agua potable o un sistema de suministro de red eléctrica, caso contrario, en las redes IT se realizan de forma programada paradas para mantenimiento y actualización de sistemas.

En esta línea, en la Figura 13 (figura de mi autoría en donde se puede visualizar las prioridades de los sistemas IT y OT en base a la interpretación de la estándar ISO 27001) se puede observar cómo se invierten las prioridades en esas dos tecnologías.

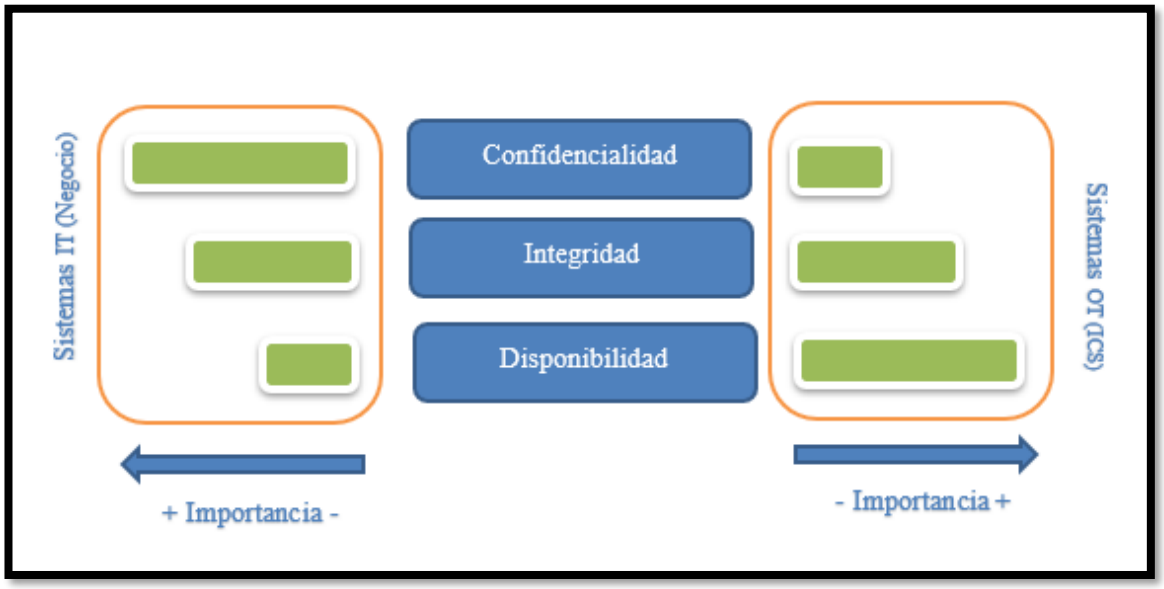

Figura 13: Figura de mi autoría en donde se puede visualizar las prioridades de los sistemas IT y OT en base a la interpretación de la norma ISO 27001.

3.2.3 Conectividad

Los ICS y los sistemas corporativos de IT a menudo se interconectan como resultado de varios cambios en las prácticas de gestión de la información, operativa y necesidades comerciales. La demanda de acceso remoto ha animado a muchas organizaciones a establecer conexiones con el ICS que permiten a los ingenieros y al personal de apoyo, supervisar y controlar el sistema desde puntos fuera de la red de control.

Muchas organizaciones también han añadido conexiones entre redes corporativas y redes de ICS para permitir que los tomadores de decisiones de la organización puedan obtener acceso a datos críticos sobre el estado de sus sistemas operativos, y para enviar instrucciones para la fabricación o distribución de productos.

A menudo, estas conexiones se aplicaron sin una comprensión completa de los riesgos de seguridad que correspondían. Como se explicó en los capítulos anteriores, el

IIoT aumentará la conectividad entre los distintos equipos industriales y expondrá a la nube la información recolectada. Esto sucede también en las redes corporativas que fueron adoptando muchos servicios en la nube con el fin de reducir costos operativos. A menos que se implementen controles de seguridad apropiados y de forma oportuna, estas vulnerabilidades pueden exponer a todos los niveles de la arquitectura de red del ICS a una variedad de amenazas cibernéticas, incluyendo gusanos y todo tipo de malware.

3.2.4 Nuevos Riesgos

En base a lo analizado, y producto de esta convergencia IT y OT que le permite a las organizaciones adaptarse a los nuevos modelos de negocios de una forma ágil, acarrea nuevos riesgos los cuales algunos son significativos. En varias oportunidades las organizaciones son sorprendidas sin ninguna medida de seguridad en sus sistemas, produciendo un daño significativo a su negocio.

Estos riesgos significativos que afectan a los ICS son:

- Fuga de información.
- Accesos no autorizados.
- Explotación de vulnerabilidades en sistemas obsoletos.
- Anulación de funciones o funcionamiento anómalo.

3.3 Mitigación de los Riesgos presentados

3.3.1 Arquitectura y Segregación de Red

Según Ledesma (2018) en el diseño de una arquitectura de red para una implementación de un ICS, por lo general se recomienda separar la red ICS de la red corporativa. La naturaleza del tráfico de red en estas dos redes es diferente: mientras que el acceso a internet, FTP, correo electrónico y acceso remoto normalmente están permitidos en la red corporativa, esto no se debe permitir en la red ICS.

Por cuestiones de practicidad o por requerimientos del negocio, es necesario conectar el ICS y las redes corporativas. Esta conexión representa un riesgo de seguridad importante y se debe analizar cuidadosamente desde el diseño para poder garantizar las condiciones mínimas y aceptables desde el punto de vista de seguridad. En el caso que se deba realizar dicha conexión, se recomienda que sólo sean las conexiones mínimas y que dicha conexión se permita a través de un firewall y una DMZ. Una DMZ es una red desmilitarizada o red de perímetro que se ubica entre la red corporativa y la red externa con el fin de no exponer la red corporativa a potenciales ciberataques.

Las redes de ICS y las redes corporativas pueden ser segregadas para mejorar la seguridad cibernética utilizando diferentes arquitecturas. Las arquitecturas posibles son:

- Firewalls entre la red corporativa y la red de control.
- Firewalls y enrutador entre la red corporativa y la red de control.
- Firewalls con DMZ entre la red corporativa y la red de control.

3.3.2 Firewall

En un entorno de ICS, los firewalls se despliegan más a menudo entre la red de ICS y la red corporativa. Configurado correctamente, pueden restringir considerablemente el acceso no deseado hacia y desde el sistema de control, lo que mejora la seguridad.

Según Vieites, Á. G. (2011), hay tres clases de firewall que se pueden aplicar en estos escenarios de convergencia.

Firewalls de filtrado de paquetes: Son los dispositivos que utilizan la funcionalidad de control de acceso para las direcciones del sistema y las sesiones de comunicación esencialmente de enrutamiento. El control de acceso se rige por un conjunto de directivas que se refiere colectivamente como un conjunto de reglas. Las ventajas de los firewalls de filtrado de paquetes incluyen bajo costo y bajo impacto en el rendimiento de la red, por lo general debido a que sólo uno o unos pocos campos de cabecera en el paquete son examinados. Estos Firewall operan en la capa 3 del modelo OSI. (p. 926)

Firewall de inspección dinámica: Firewalls de inspección de estado son filtros de paquetes que inspeccionan los datos del modelo OSI en la capa 4. La inspección por estado filtra paquetes a nivel de capa de red, determina si las sesiones del paquete son legítimas y evalúa el contenido del paquete y nivel de la capa de transporte (Ej. TCP y UDP). La inspección por estado permite controlar las sesiones activas y usa esta información para determinar si el paquete debe ser reenviado o bloqueado. Esto ofrece un alto nivel de seguridad y un buen rendimiento, pero es más complejo de administrar.

Firewalls de Aplicación: Esta clase de firewalls examina los paquetes en la capa de aplicación y filtra el tráfico basado en las reglas de aplicación específicas (por ejemplo, navegadores). Ofrece un alto nivel de seguridad, pero podría tener efectos sobre el rendimiento de la red, que puede ser inaceptable en un entorno ICS. (p. 927)

No es aceptable una convergencia entre redes industriales y redes corporativas de forma directa, para poder subsanarlo existen varias alternativas como la incorporación de un firewall o su combinación con una DMZ, que brindan una solución más robusta a la arquitectura.

3.3.3 Controles de Seguridad

Los controles de seguridad son necesarios para mantener los sistemas seguros, estos tienen como fin proteger la confidencialidad, integridad y disponibilidad de la información de un sistema. En la Tabla 2, se plasma una matriz de controles que abarca los dos entornos IT y OT con sus diferentes enfoques y basada en los tres ejes principales (confiabilidad, disponibilidad e integridad). Dicha matriz es una propuesta con objetivos de control de un alto nivel la cual permite cubrir con los riesgos más importantes que sufren las distintas organizaciones como pudimos observar en el presente trabajo.

			Entorno							
			OT				IT			
			Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4			
							On premise	Cloud		
	ID	Objetivo de control						IaaS	PaaS	SaaS
Confidencialidad: Buscar que los activos de información sean accedidos por las personas que poseen la necesidad y el privilegio para esto.	C1	La identidad debe estar integrada con el sistema corporativo								
	C2	Si la seguridad fuera propia de la palicación debe cumplir con el estándar de contraseña de la compañía.								
	C3	La aplicación debe tener segregación de funciones								
	C4	Los accesos son revocados ante el cese de relación del empleado con la compañía								
	C5	Los permisos son revalidados al menos una vez por año por los propietarios de los datos de cada aplicación.								
	C6	Las actividades de los usuarios son guardadas en el SIEM corporativo								
	C7	Los sistemas deben tener el ultimo nivel de parche de seguridad implementado								
	C8	Los logs de usuarios seran revisados regularmente								
Integridad: Busca asegurar que los datos de los activos de informacion sean autenticos, completos y consistentes.	I1	Tener implementado y activo un sistema de protección contra software malicicoso o virus.								
	I2	Se debe tener al menos una prueba de restauración programada al año.								
	I3	Los entornos deben estar separados en (Producción/Testing/Desarrollo)								
	I4	El acceso al código fuente de los programas debe ser restringido								
	I5	Los datos en transito deben estar cifrados								
	I6	Debe existir un control de cambios								
	I7	Los datos en reposo deben estar cifrada								
	I8	La red debe tener un diseño seguro								
	I9	Las pruebas funcionales de seguridad deben llevarse a cabo en la etapa de Desarrollo								
Disponibilidad: Busca el acceso confiable y oportuno de los datos, información o recursos para el personal autorizado.	D1	El sistema debe tener redundancia								
	D2	El sisteme debe tener resguardo en Backup								
	D3	El sistema requiere una comunicación redundante								
	D4	Los medios de almacenamiento deben eliminarse de manera segura								
	D5	Los medios de almacenamiento que contengan información deben estar protegidos contra el acceso no autorizado, mal uso o la corrupcion durante el transporte								
	D6	Limitar el acceso a las instalaciones de procesamiento de información								

Tabla 2: Tabla de elaboración propia que contiene objetivos de control propuestos para mitigar los riesgos mas importantes.

Es recomendable realizar un análisis de riesgo antes de implementar la matriz con el fin establecer las prioridades en los controles.

3.4 Análisis de los Resultados

Los resultados obtenidos producto de la investigación realizada son los siguientes:

a) La ciberseguridad en IT y OT no debe ser abordada con el mismo enfoque, estas dos tecnologías tienen distintas prioridades en términos de rendimiento, riesgos y disponibilidad de los datos. Realizar un análisis erróneo de esto puede derivar en

una parada de planta o puede finalizar con un incidente comprometiendo los activos de información de una organización.

b) La estrategia de ciberseguridad debe tener una mirada holística, con el fin de minimizar la probabilidad de riesgos cibernéticos, prevenir incidente, generar una conciencia en ciber-amenazas y dar confianza a clientes y usuarios. Se demostró que un vector de ataque muy importante es el factor humano, es por ello, que se debe mantener concientizados en términos de ciberseguridad a todas las personas que interactúen con los sistemas IT y OT.

c) Se puso en evidencia que, al converger las tecnologías de IT y OT en un marco de innovación constante, aumentan los riesgos cibernéticos poniendo en peligro las infraestructuras criticas ya sea de una organización como la de un país. Cabe destacar, que los estándares internacionales citados en el presente documento, ya sea ISO, NIST o ISA, nos otorgan herramientas de gran utilidad para minimizar los riesgos y alcanzar un grado de madurez aceptables en términos de ciberseguridad.

Los resultados que emergen del análisis de esta propuesta muestran cómo la integración entre las tecnologías IT y OT expone nuevas vulnerabilidades y presentan un abordaje que permite mitigarlas.

Capítulo 4 - Conclusiones

4.1 Conclusiones

Las redes industriales fueron inicialmente diseñadas para maximizar la funcionalidad en los procesos productivos, prestando poca atención a la evolución de los ciberataques. Tradicionalmente las redes industriales se protegieron aislándolas físicamente sin ninguna conexión con las redes corporativas o internet. Por otro lado, las redes corporativas tuvieron una gran evolución tecnológica que se acrecentó con la llegada de internet y el concepto de IoT, provocando una mayor cantidad de dispositivos conectado. Las redes corporativas, también se encuentran expuestas a gran cantidad de ciberataques, pero orientados al robo de información, según se pudo apreciar en los últimos ataques durante el 2019. Como resultado de la investigación y lo fundamentado en los capítulos anteriores**,** quedó demostrado que muchas de las organizaciones, dejaron expuestos sus sistemas industriales y corporativos a una gran cantidad de ciberataques.

Esto sucede por no tener en cuenta a la ciberseguridad en la estrategia de la compañía. Adicionalmente, se suma la convergencia entre las redes industriales y las corporativas, en donde las fronteras tienden a desvanecerse, provocando que aumente el riesgo de sufrir un ciberataque de forma considerable. La ciberseguridad en los sistemas de control es una problemática compleja y en algunos casos al ser tratado como infraestructura crítica, debe inclusive intervenir el Estado de un país.

Las redes industriales, eventualmente realizan funciones claves en la prestación de servicios esenciales y materias primas (por ejemplo, electricidad, gas natural, combustibles, agua, y transporte). Como tales, son parte de la infraestructura crítica y requieren la protección de una variedad de riesgos que existen en el ciberespacio. Estos riesgos deben ser contenidos de forma integral y oportunamente, mediante la aplicación de los estándares internacionales ya sea NIST, ISO o ISA, los cuales, si se tienen en cuenta desde el diseño de las arquitecturas, se puede tener una integración con redes corporativas de forma segura y sostenible en el tiempo. Es importante que las compañías o bien los Estados, tengan presente estos riesgos y se tomen las acciones en consecuencia, ya sea con presupuesto o con la legislación adecuada.

El concepto de seguridad absoluta no existe, pero aplicando las metodologías vistas de forma proactiva con políticas de ciberseguridad robustas, se puede tener un sistema de IT y OT conectado y operando, con niveles de ciberseguridad aceptables, en pos de la continuidad de los negocios y el bien de una población.

4.2 Líneas Futuras de Investigación

A partir del presente trabajo final, se abren dos líneas de investigación que potencialmente podrían ser consideradas para un futuro desarrollo.

Considerar la ciberseguridad en metodologías de proyectos ágiles: la gestión de proyectos en redes corporativas y redes industriales, no priorizan en sus tareas a la ciberseguridad desde sus inicios. Una línea de investigación a considerar es, analizar la inclusión de un Rol de Ciberseguridad en las metodologías agiles de proyecto, pudiendo así evaluar riesgos y analizar posibles mitigantes.

Gobierno de Ciberseguridad en IT y OT: Crear un modelo de gobierno de ciberseguridad que contemple la tecnología operacional y la tecnología de información.

Dicho modelo debe permitir medir mediante indicadores la madurez en términos de ciberseguridad. Adicionalmente, que dicho modelo, permita medir la madurez en términos de ciberseguridad mediante indicadores.

Referencias

Airbus (2019). Declaración de Airbus acerca del ciberincidente. *Obtenido del sitio web*: https://www.airbus.com/newsroom/press-releases/es/2019/01/airbus-statement-on-cyber-incident.html

Alonso, N. O. (2013). *Redes de comunicaciones industriales*. Editorial UNED.

Audit, conseil, installation et sécurisation des systèmes d'information (France). (2018). *Seguridad informática-Hacking ético. Conocer el ataque para una mejor defensa (4a edición)*. Ediciones Eni.

Avast, (2021). Otras amenazas. Obtenido del sitio web: https://www.avast.com/es-es/c-rootkit#topic-1

Avast, (2021). Guía esencial sobre el ransomware. Obtenido del sitio web: https://www.avast.com/es-es/c-what-is-ransomware#topic-3

Basco, A. I., Beliz, G., Coatz, D., & Garnero, P. (2018). Industria 4.0: fabricando el futuro (Vol. 647). Inter-American Development Bank.

Baufest. (2020). Ciberataques: qué tendencias se observaron en 2019. *Obtenido del sitio web:* https://baufest.com/es/7-espanol/blog/820-ciberataques-tendencias-2019

Bonillo, V. M. (2013). Principios fundamentales de computación cuántica. Universidad de La Coruña. Obtenido de la web: https://enginyeriainformatica.cat/wp-content/uploads/2016/05/PRINCIPIOS-FUNDAMENTALES-DE-COMPUTACI%C3%93N-CU%C3%81NTICA.pdf

Cantor, R. V. (1994). La tercera revolución industrial. Universitas Humanística, 39(39). Obtenido del sitio web: https://revistas.javeriana.edu.co

Cert, E. (2020). Lo que sabemos del ataque de ransomware a Pemex. *Obtenido del sitio web de Cert Europa:* https://cert.mnemo.com/lo-que-sabemos-del-ataque-de-ransomware-a-pemex/

Christensson, P. (2006*). IT Definition*. Retrieved 2019, Sep 14. Obtenido de: https://techterms.com.

Cobo Romaní, J. C. (2009). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento.

Corporate, A. G. (2020). Specialty SE, (2020). Allianz Risk Pulse–Allianz Risk Barometer on Business Risks. Obtenido de https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020.pdf

COVID-19 Risks Outlook, a Preliminary Mapping and Its Implications" Mayo 2020. - World Economic Forum

Data Collective, DCVD. (2019). Incidentes de Ciberseguridad por Industria. *Obtenido del sitio web*: https://www.dcvc.com/post/sentinelone-raises-120m-series-d-to-protect-devices-from-diverse-threats-with-ai-driven-behavioral-analysis.html

David E. Sanger, (1-6-2012). Orden De Obama aceleró ola de ciberataques contra Irán. New York Times. Obtenido de: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Eset, (2016). Todo sobre el ransomware: Guía básica y preguntas frecuentes. Obtenido del sitio web: http://www.eset-la.com/pdf/kit-antiransomware/Guia-Todo_Sobre_Ransomware.pdf

Falco, Joe, et al., IT Security for Industrial Control Systems, NIST Internal Report (NISTIR) 6859, (2002), http://www.nist.gov/customcf/get_pdf.cfm?pub_id=821684

Gartner Hype Cycle for Emerging Technologies, (2019). Obtenido de: https://www.gartner.com/

Gartner, (2020). Glosarios - Tecnología operacional (OT). *Obtenido de:* https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Hall, J. O. H. N. La internet industrial de las cosas y la industria 4.0 en colada por gravedad. [Online]. *Obtenido de http://www.cmhmfg.com/pdf/SS_2018_Spring_CMH_SP. pdf*, *10*.

Hansson, S. O. (2005). Seven myths of risk. *Risk Management*.

Herčko, J., Slamková, E., & Hnát, J. (2015). *Industry 4.0 as a factor of productivity increase*. In Proceedings of TRANSCOM PROCEEDINGS 2015-11th European Conference of young researchers and scientists (pp. 118-122). Obtenido de https://www.researchgate.net/profile/Jozef_Hercko/publication/285597330_Industry_40_as_a_factor_of_productivity_increase/links/56f1a70108aee9c94cfd70c8/Industry-40-as-a-factor-of-productivity-increase.pdf

ISA 99, (2021). Industrial Automation and Control System Security. [En línea]. Obtenido del sitio web: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

Kaspersky, (2020). Definiciones. Obtenido del sitio web: https://latam.kaspersky.com/resource-center/definitions/boot-sector-virus

Kaspersky, (2021). Threats. Obtenido del sitio web: https://latam.kaspersky.com/resource-center/threats/viruses-worms

Laudon, K. C., & Laudon, J. P. (2012). *Sistemas de información gerencial*. Naucalpan de Juárez. Obtenido de: https://docs.google.com/file/d/0ByOln-xoAuQQckE2RHdDTFdWMm8/edit

Ledesma, J. (2019). Arquitecturas de Segregación de Redes IT/OT.

MAGERIT (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Noticias Ciberseguridad (2020). Aeropuerto internacional de San Francisco es hackeado; credenciales de red filtradas. *Obtenido del sitio web*: https://noticiasseguridad.com/hacking-incidentes/aeropuerto-internacional-de-san-francisco-es-hackeado-credenciales-de-red-filtradas/

OCTAVE Allegro (2007). Improving the Information Security Risk Assessment Process.

Panda Security, (2020). Glosario Técnico. Obtenido del sitio web: https://www.pandasecurity.com/es/security-info/glossary/

RISI. Repository of Industrial Security Incidents [Online] 2020 Obtenido de https://www.risidata.com/

Sanchez, G. B. (2018). Las primeras cinco revoluciones industriales. Cienciorama. Obtenido del sitio web: http://www.cienciorama.unam.mx.

Sedgewick, A. (2014). Marco para mejorar la ciberseguridad de la infraestructura crítica, versión 1.0 (No. NIST-Cybersecurity Framework).

Segu-Info, (2021). Malware/rogue. Obtenido del sitio web: https://www.segu-info.com.ar/malware/rogue

Siemens. (2020). Productos y Servicios. *Obtenido del sitio web:* https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-remote-communication/telecontrol/rtu-remote-terminal-unit/simatic-rtu-3000c.html

Stouffer, K., Falco, J., & Scarfone, K. (2015). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.

Urbina, G. B. (2016). Introducción a la seguridad informática. Grupo editorial PATRIA.

Us-cert.cisa.gov, (2021). Alerta (AA21-042A). Obtenido del sitio web: https://us-cert.cisa.gov/ncas/alerts/aa21-042a

Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática* (Vol. 6). Grupo Editorial RA-MA.

Yeboah-Boateng, EO y Amanor, PM (2014). Phishing, SMiShing y Vishing: una evaluación de las amenazas contra los dispositivos móviles. Revista de tendencias emergentes en ciencias informáticas y de la información, 5 (4), 297-307.