UNIVERISDAD DE BELGRANO

DESARROLLO DE UN MARCO DE BUENAS PRÁCTICAS DE CIBERSEGURIDAD PARA SISTEMAS SCADA CON INTEGRACIÓN DE IoT

Facultad: Ingeniería y Tecnología Informática

Carrera: Ingeniería Informática

Alumno: María Belén Ortiz Fiocca

Tutor: Gustavo Aldegani

Plan: 2012

Año: 2024

Agradecimientos

Antes que nada, quiero expresar mi más sincero agradecimiento a mi tutor, Gustavo Aldegani, por su paciencia, dedicación y las valiosas devoluciones brindadas a lo largo del desarrollo de esta tesina.

A mis padres, gracias por haber hecho posible mi educación en esta universidad. En especial, a mi mamá, quien siempre me acompañó y se interesó por mi progreso. Extiendo este agradecimiento a toda mi familia, tanto la que reside en Argentina como la que se encuentra en Perú.

A mi pareja, gracias por ser mi refugio en los momentos difíciles y por celebrar cada pequeño logro como si fuera propio. Tus palabras de aliento y tu apoyo incondicional fueron fundamentales para que no bajara los brazos, especialmente en los momentos de mayor presión.

Asimismo, quiero agradecer al director de nuestra carrera, Sergio Aguilera, y a todo el equipo docente que me guió durante estos cinco años. A mis compañeros de cursada y hoy grandes amigos, gracias por su compañía y por haber hecho este camino mucho más llevadero. Nada hubiera sido igual sin ustedes.

Finalmente, no puedo dejar de mencionar a mi gata, Fanta, quien fue mi fiel compañera durante toda la carrera y especialmente en los momentos más exigentes del desarrollo de esta TFC, estando junto a mí en mis desvelos frente a la computadora con su silenciosa pero invaluable presencia.

A cada persona que formó parte de mi vida en estos últimos cinco años, les agradezco profundamente. Su presencia reafirma que el trabajo en equipo y las relaciones interpersonales son fundamentales para alcanzar cualquier meta. Me siento afortunada de haber aprendido tanto y de haber conocido personas tan maravillosas en este camino.

Resumen

Las infraestructuras críticas son fundamentales para nuestra sociedad porque forman parte de tareas vitales para nosotros, pudiendo ser encontradas (por ejemplo) en sectores como el energético, el de suministro de agua, el de telecomunicaciones y el de transporte, sólo por mencionar los que más nos atraviesan. La problemática surge de que, así como la tecnología nos facilita muchos procesos, también, al vivir en un mundo que se encuentra altamente interconectado y dependiente de ella, lleva a la preocupación de que estos sistemas no se vean interrumpidos, así como también, a la búsqueda de evitar que eso ocurra debido a los impacto socioeconómicos que puede acarrear.

Ahora bien, así como infraestructuras críticas son “la columna vertebral de la sociedad”, la Supervisión, Control y Adquisición de Datos (SCADA) son componentes esenciales de estas infraestructuras, permitiendo la monitorización y gestión eficiente de procesos críticos en tiempo real. Sin embargo, como se mencionó anteriormente, la interconexión es una problemática y más cuando se ven involucradas redes de comunicación, como Internet, que llevan al aumento de la exposición a posibles amenazas informáticas.

El presente Trabajo de Final de Carrera (TFC) busca abordar estos desafíos con foco a la ciberseguridad, centrándose en los sistemas SCADA integrados con tecnologías de Internet de

las cosas (IoT), y desarrollar un framework que pueda ser de utilidad para quienes se enfrente a estos casos.

Como se verá a lo largo del presente documento, a pesar de que la integración de IoT ofrece nuevas oportunidades para la automatización y la eficiencia operativa, también introduce nuevas vulnerabilidades. Es crucial, por tanto, investigar y desarrollar planes de respuesta a riesgos, así como políticas y procedimientos de ciberseguridad, que protejan estos sistemas críticos de manera efectiva y proactiva.

Para lograr este objetivo, se aplicará un enfoque multidisciplinario que abarca diversas áreas de conocimiento. En primer lugar, dentro del campo de Tecnologías Aplicadas, se desarrollará un Marco de Buenas Prácticas de Ciberseguridad específicamente adaptado a sistemas SCADA que integren IoT. El mismo proporcionará directrices que permitan mitigar y encarar las posibles amenazas que puedan llegar a surgir y proteger la integridad de las infraestructuras críticas.

Por otro lado, el análisis de vulnerabilidades en sistemas SCADA constituye una parte fundamental de este estudio, encuadrado en el área de Información y Conocimiento. Identificar y comprender las posibles vulnerabilidades con las que nos podemos topar permitirá desarrollar estrategias defensivas más efectivas y anticiparse a posibles ataques.

Asimismo, el aspecto de Gestión también estará presente en este proyecto, abordando la implementación de las buenas prácticas propuestas y colaborando con una gestión eficiente de recursos y procesos.

Además, se explorarán otros campos, como la gestión de riesgos y la continuidad del negocio. Esto se enmarca dentro de una perspectiva más amplia de Innovación y Tecnología, donde se busca aprovechar las últimas tendencias y avances en ciberseguridad para fortalecer la protección de las infraestructuras críticas.

Índice de Contenido

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Problemática y Contexto

Es imposible negar que cada vez vivimos en un mundo más dependiente de la tecnología e interconectado. De hecho, las infraestructuras críticas que forman parte de nuestra sociedad actual son consideradas hoy en día como los pilares de la misma, incluyendo por ejemplo: la generación y distribución de energía, la gestión y suministro del agua e incluso el control de sistemas de transporte.

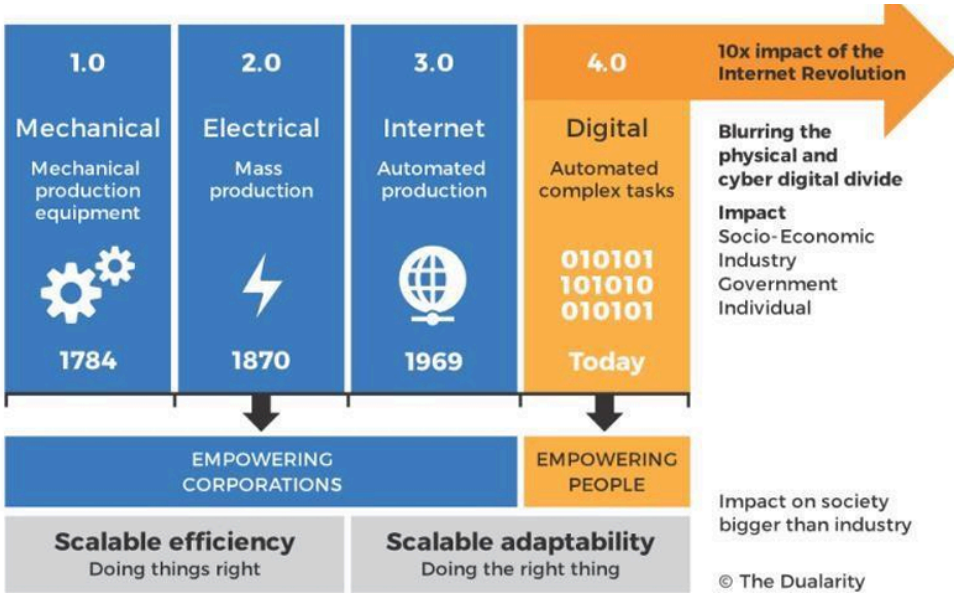
Las actividades cotidianas, como ir a la oficina a trabajar, dependen de una serie de sistemas críticos cuya interrupción puede tener un impacto significativo en nuestras vidas. Pensemos, por ejemplo, en la rutina matutina. Comenzamos el día realizando tareas básicas como lavarnos los dientes y bañarnos (acciones que dependen del suministro de agua). A continuación, nos trasladamos a nuestro destino, muchas veces utilizando medios de transporte público, como el subte. Pero, ¿qué sucedería si alguno de estos sistemas fallara? La falta de disponibilidad del subte, por ejemplo, no sólo retrasaría a miles de usuarios, sino que podría obligarlos a cancelar sus actividades planeadas, invertir tiempo en regresar a sus hogares y enfrentar consecuencias como frustración y/o agotamiento.

Estos inconvenientes diarios son solo una parte del problema. Detrás de estas actividades aparentemente simples, existe una infraestructura crítica interconectada, donde el suministro de agua, el transporte público y la energía eléctrica (solo por nombrar algunos) son pilares fundamentales. La energía, en particular, juega un rol transversal, ya que garantiza el funcionamiento de los otros dos sistemas. Esta interdependencia hace evidente la clara necesidad de proteger a estos sistemas y más aún cuando los mismos están expuestos a un creciente riesgo de ciberataques, cosa que podrían tener devastadoras consecuencias **[1]** que van más allá de no poder llegar a trabajar.

Para todos estos sistemas críticos se suele hacer uso de lo que se denomina como *Sistemas de Supervisión, Control y Adquisición de Datos* (SCADA) que poseen un papel más que importante, ya que son ellos los que permiten monitorizar y gestionar estos sistemas en tiempo real, pero no siempre fue así. Hasta la primera mitad del siglo XX, la industria dependía principalmente de la supervisión de las personas y, recién en los años 70, gracias a la evolución de la tecnología, se comenzaron a hacer populares los *Controladores Lógicos Programables*[1] (PLC) digitales y los SCADA, llegando así la tercera revolución industrial **[2]**.

[1] Son dispositivos electrónicos diseñados para automatizar procesos industriales, controlando máquinas y equipos mediante programación lógica y entrada/salida de datos.

Figura 1



Nota. En la imagen se puede ver la revolución de la industria hasta la 4.0. Tomado de *Industry 4.0 -Digital Transformation, Challenges and Benefits* (p. 139), por Grade, M. y Deoskar, 2020, International Conference on Computer Technology.

Estos sistemas podrían considerarse como "omnipresentes" dentro de la gran mayoría de las operaciones industriales que se llevan a cabo en el día a día y son de gran utilidad, como ya hemos mencionado. De todas maneras, a causa de la adopción e integración del *Internet de las Cosas* (más conocido como IoT) junto con los sistemas SCADA, a pesar de haber colaborado con la automatización y la eficiencia operativa, también se introdujo nuevos desafíos en términos de seguridad informática que hace evidente la necesidad urgente de un enfoque de ciberseguridad altamente especializado **[3]**.

Es dentro de éste contexto en el que se desarrolla el *Trabajo de Final de Carrera* (TFC). Siendo el foco y objetivo de esta investigación contribuir al desarrollo de un marco de buenas prácticas que esté diseñado específicamente con el fin de proteger aquellas infraestructuras críticas que hagan uso de sistemas SCADA y que tenga integrado IoT.

1.2. Objetivo Principal y Secundarios

1.2.1. Objetivo Principal

Lo que se busca es desarrollar un framework de ciberseguridad que esté diseñado específicamente para sistemas SCADA que integren IoT y que éste pueda ser usado como una guía a fin de proteger los sistemas críticos frente a posibles amenazas.

1.2.2. Objetivos Secundarios

- Identificar las Vulnerabilidades Actuales: Realizar un análisis en profundidad de las vulnerabilidades actuales que afectan a los sistemas SCADA.
- Revisión de Prácticas Recomendadas Existentes: Investigar y analizar las prácticas recomendadas existentes en el campo de la ciberseguridad de sistemas SCADA, identificando las más pertinentes y adaptándolas al foco del marco que es la integración con las tecnologías IoT.

- Evaluación y Descripción del Impacto de la Integración IoT: Evaluar los desafíos de la integración de dispositivos IoT con sistemas SCADA, con el objetivo de comprender cómo esta convergencia impacta en la seguridad y operación de infraestructuras críticas. Así mismo, describir los tipos de consecuencias que pueden surgir, con el propósito de comprender la magnitud de los riesgos y las posibles áreas de debilidad, utilizando casos reales para ejemplificar.

1.3. Hipótesis

A través de la implementación de un marco de buenas prácticas de ciberseguridad, se logrará una integración efectiva de IoT y sistemas SCADA para infraestructuras críticas.

Esto favorecerá el fortalecimiento desde el punto de vista de la seguridad informática, principalmente en la protección de los activos[2] críticos, al abordar las vulnerabilidades específicas de SCADA y las relacionadas con la incorporación de IoT en estos sistemas, que reducirá de forma significativa la probabilidad de que las mismas se vean interrumpidas por un tema vinculado a la seguridad en sí.

[2] Es cualquier cosa de valor que es propiedad de una organización. Incluyen elementos tangibles (ej. computadoras de trabajo) e intangibles (ej. propiedad intelectual).

1.4. Limitaciones y Alcances

En primer lugar, se reconoce que el alcance de la infraestructura crítica constituye una limitación importante, ya que el estudio podría restringirse a ciertos tipos de infraestructuras, como plantas de energía o redes de suministro de agua, sin abordar todas las posibles aplicaciones de sistemas SCADA en otros sectores industriales.

Así mismo, dada la restricción planteada con anterioridad, puede ocurrir que no se tengan en cuenta ciertas vulnerabilidades que sean más específicas a un sector en sí. Abordando el desarrollo del presente marco en torno a vulnerabilidades halladas que sean más generalistas y no tan específicas por lo que, a pesar de lo que se plantee como vulnerabilidades, tiene también el lector que hacer investigación de aquellas específicas al caso de uso al que se quiere aplicar.

Otra delimitación clave es el enfoque predominante en soluciones técnicas, sin abordar a gran profundidad aspectos organizativos, regulatorios o humanos que también desempeñan un papel crucial en la seguridad informática de las infraestructuras críticas.

Finalmente, en lo que respecta al contexto geográfico, no se tendrá en cuenta las normas y regulaciones específicas de cada país. De todos modos, el presente marco va a hacer mayor foco en aquellas que sean globales o de aceptación/uso general para poder abarcar y ser de utilidad para el mayor público posible.

1.5. Áreas de Conocimiento Involucradas

La presente TFC integra diversas áreas de conocimiento, tal como establece la CTTI. En primer lugar, se encuentra el área de *Tecnologías Aplicadas*, donde se enfoca en el desarrollo de un marco de mejores prácticas de ciberseguridad para sistemas SCADA en infraestructuras críticas. Esto implica la aplicación de tecnologías y prácticas de seguridad informática, con un enfoque específico en la subárea de "Seguridad Informática, Contingencia y Gestión de Riesgos". Aquí, se explorarán soluciones técnicas para proteger los sistemas SCADA y mitigar las amenazas informáticas.

Por otro lado, el proyecto también aborda el área de *Información y Conocimiento*, ya que implica la identificación de vulnerabilidades en sistemas SCADA. Esto requiere la recopilación y análisis de información relevante en el ámbito de la ciberseguridad, con el objetivo de comprender mejor las amenazas y diseñar estrategias de protección adecuadas.

Además, aunque el proyecto se centra principalmente en investigación, también se ven involucrados aspectos del área de *Gestión*. Esto se relaciona con la implementación de las buenas prácticas de ciberseguridad propuestas en el marco desarrollado, lo que implica la coordinación de recursos, la planificación de acciones y la supervisión de procesos para garantizar la eficacia de las medidas de seguridad implementadas.

1.6. Metodologías Aplicadas

Se utilizará la *Metodología de Investigación Bibliográfica* para la revisión exhaustiva de la literatura existente relacionada con la ciberseguridad en sistemas SCADA y las infraestructuras críticas, ya que permite recopilar y analizar investigaciones previas, informes técnicos, documentos normativos y cualquier otra fuente relevante que contribuya al entendimiento de la problemática y el desarrollo del framework.

En segundo lugar, tenemos la *Metodología de Revisión Sistemática* que permite analizar de manera estructurada y exhaustiva las tácticas de ataque utilizadas junto con su impacto, ayudando a identificar patrones, tendencias y vulnerabilidades recurrentes. Además, facilitará la evaluación comparativa de diferentes enfoques de seguridad implementados en diversos contextos, lo que contribuirá a identificar las mejores prácticas y lecciones aprendidas en la protección de sistemas SCADA.

Ambas metodologías se complementan para proporcionar una visión integral de la problemática de la ciberseguridad en sistemas SCADA, permitiendo tener una comprensión profunda de las vulnerabilidades y soluciones existentes en el ámbito de la ciberseguridad, sentando así las bases para el desarrollo del marco de buenas prácticas propuesto en la Tesina.

2. Marco Teórico

2.1. Infraestructura Crítica

Primero que nada, debemos comenzar comprendiendo qué significa la palabra "infraestructura", ya que es el activo en sí que se busca proteger y lo que da comienzo a la necesidad de desarrollar este framework. Cuando pensamos en esta palabra, ¿qué se nos viene a la cabeza? En la mayoría de los casos vamos a estar pensando en puentes, suministro de agua o energía, hospitales, aeropuertos, telecomunicaciones, entre otros. Pero, dicho concepto va más allá de ejemplos de lo que es una infraestructura. Para poder entender la importancia de lo que se busca preservar (hablando siempre desde el punto de vista de la seguridad informática), debemos tener en claro qué significa en sí. Para ello, comencemos con la definición de la RAE.

> *"Conjunto de elementos, dotaciones o servicios necesarios para el buen funcionamiento de un país, de una ciudad o de una organización cualquiera."* **(Real Academia Española, s.f., definición 2).**

El término en sí fue desarrollándose a lo largo del tiempo, pero si tenemos que poner en palabras sencillas qué significa, podemos decir que es aquel activo físico que puede ser empleado para producir un servicio (ej. plantas de tratamiento de agua) o para dar soporte a la estructura de una empresa (ej. red de distribución de logística), o mismo de la sociedad (ej. sistema de transporte público) **[4]**.

Sin embargo, dentro de este vasto conjunto, surgen ciertos elementos críticos que adquieren una relevancia excepcional debido a su papel fundamental en el mantenimiento de la estabilidad, la seguridad y el bienestar de una nación. Estas son las denominadas "infraestructuras críticas", definidas como aquellas instalaciones físicas y virtuales cuya interrupción parcial o total, ya sea por destrucción o perturbación, podrían tener un impacto significativo en la vida humana, así como también en el funcionamiento efectivo del Estado, la economía, la seguridad, la salud pública y el bienestar social en general **[5]**.

Es esencial comprender que las infraestructuras críticas no operan de manera aislada, sino que están interconectadas en una red compleja que sostiene la vida cotidiana de una sociedad moderna. Por lo tanto, su protección y gestión efectiva son imperativas para la continuidad de los servicios esenciales y la resiliencia frente a amenazas internas y externas.

El concepto de infraestructuras críticas abarca una amplia gama de sectores y subsectores, cada uno con su propia importancia estratégica. Entre estos, se incluyen los sistemas de energía eléctrica, que alimentan no solo los hogares y las industrias, sino también los hospitales, las redes de transporte y las infraestructuras de comunicaciones. La interrupción de estos sistemas podría conducir a apagones generalizados, afectando negativamente la vida cotidiana y la seguridad de la población **[5]**.

Además, los sistemas de transporte, como trenes, puertos y aeropuertos, son vitales para la movilización de personas y mercancías, el comercio nacional e internacional, y la conectividad entre regiones. Cualquier interrupción en estas infraestructuras podría tener un impacto devastador en la economía y la cohesión social, y he aquí la importancia de proteger los mismos. Las infraestructuras de telecomunicaciones representan otro ejemplo crítico, ya que facilitan la transmisión de datos, voz y video, y son fundamentales para la comunicación interpersonal, el intercambio de información comercial y gubernamental, y el acceso a servicios digitales esenciales en la era moderna.

Otros sectores críticos incluyen instalaciones de salud, sistemas financieros, redes de agua potable y saneamiento, así como centros de investigación y desarrollo. Cada uno de estos elementos desempeñan un papel vital en la seguridad y el bienestar de la población, y su protección es esencial para garantizar la estabilidad y el desarrollo sostenible de una sociedad.

De hecho, las infraestructuras críticas suelen dividirse en dos categorías. Por un lado están aquellas conocidas como “Infraestructuras Comerciales”, que contiene: sistemas de telecomunicaciones, salud, energía, financieros, entre otros. Mientras que, por el otro lado, tenemos las denominadas “Infraestructuras Públicas”, que incluyen: sistemas de transporte o instalaciones gubernamentales. Independientemente del tipo que sea, la interrupción de cualquiera de estos sistemas implica un gran impacto en el día a día no sólo de las empresas y/o

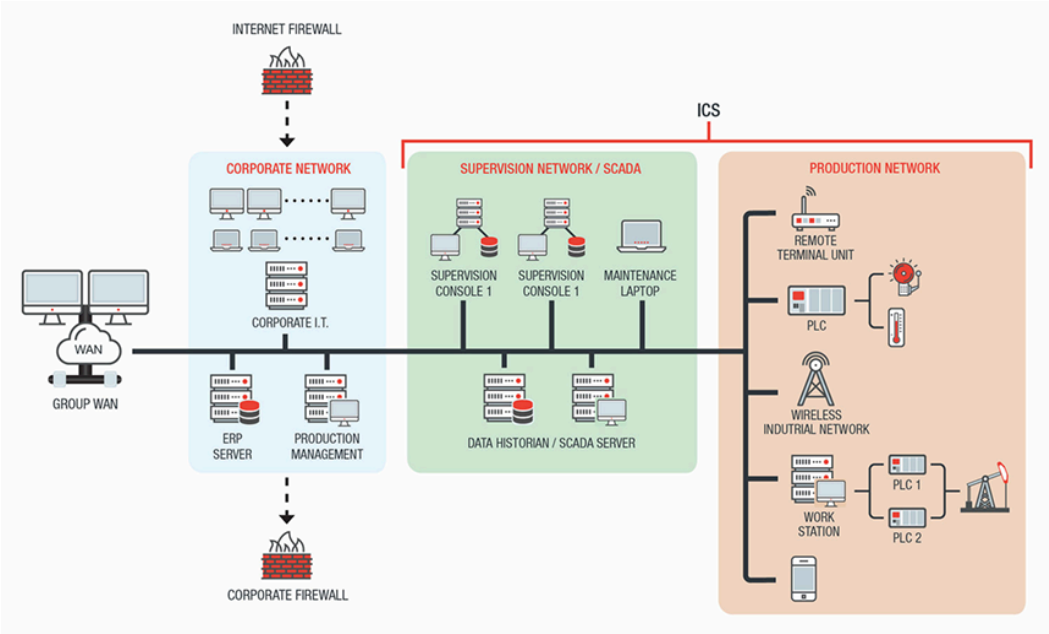
gobiernos, sino también a la sociedad en sí, para quienes estos servicios resultan indispensables **[5]**.

2.2. Sistemas de Control Industrial

Un *Sistema de Control Industrial* (ICS, por sus siglas en inglés) se define como una red de dispositivos, sistemas, controladores y software integrados que supervisan y controlan procesos industriales **[4]**. Inicialmente concebidos como sistemas aislados que operaban con software y protocolos de control propietarios, los ICS han evolucionado significativamente, incorporándose cada vez más en los sistemas de información organizacionales convencionales para promover la conectividad, la eficiencia y las capacidades de acceso remoto. Esta integración ha hecho que los ICS comiencen a asemejarse a los sistemas de información tradicionales, utilizando componentes de hardware y software comercialmente disponibles.

Desempeñan un papel crucial en la automatización y la gestión de infraestructuras críticas, abarcando sectores como la manufactura, la energía, el transporte, y las instalaciones municipales. La arquitectura de los ICS ha evolucionado para soportar nuevas capacidades de sistemas de información, lo cual, aunque mejora la funcionalidad y eficiencia operativa, también reduce el aislamiento de estos sistemas respecto al mundo exterior, introduciendo vulnerabilidades similares a las de los sistemas de información en red convencionales. Esta convergencia ha incrementado la necesidad de robustecer la seguridad informática de los ICS.

Figura 2



Nota. Este gráfico ilustra la segmentación y estructura de las redes industriales. Tomado de *Industrial Control System*, (s.f.), Trend Micro.

2.3. Sistemas SCADA

Un *Sistema de Control y Adquisición de Datos* (SCADA, por sus siglas en inglés) es un tipo de ICS utilizado para supervisar y controlar infraestructuras y procesos industriales a gran escala. Los sistemas SCADA toman ventaja de los desarrollos en miniaturización de sistemas y tecnología de redes de área local (LAN) para distribuir el procesamiento a través de múltiples

sistemas, lo cual proporciona más poder de procesamiento y mejora la redundancia y la fiabilidad del sistema en su conjunto **[4]**.

El objetivo principal de utilizar SCADA es permitir el monitoreo y control de sitios remotos a través de un sistema centralizado. En lugar de que los empleados deban desplazarse grandes distancias para realizar tareas o recopilar información, un sistema SCADA puede automatizar estas funciones. Los dispositivos en el campo gestionan las operaciones locales, como abrir o cerrar válvulas y disyuntores, recopilar datos de sensores, y monitorear el entorno para identificar condiciones de alerta o alarma **[22]**.

Es fundamental comprender que los Sistemas de Control Industrial (ICS) son una categoría amplia que incluye diversos tipos de sistemas utilizados para automatizar y controlar procesos industriales. Inicialmente, los ICS eran sistemas aislados que operaban con software y protocolos propietarios, sin conectarse a redes más amplias. Sin embargo, con el tiempo, estos sistemas se han integrado cada vez más en los sistemas de información organizacionales principales para promover la conectividad, eficiencia y capacidades de acceso remoto **[4]**.

Dentro de la categoría de ICS, los sistemas SCADA representan una implementación específica que se destaca por su capacidad de distribuir las funciones del sistema a través de múltiples sistemas conectados en red. Esta distribución no sólo incrementa el poder de procesamiento, sino que también mejora la redundancia y la fiabilidad del sistema en su

conjunto. A diferencia de otros ICS que pueden ser más centralizados y propietarios, los SCADA utilizan una arquitectura de sistema abierto, emplean el Protocolo de Internet (IP) para la comunicación y servicios basados en la nube, lo cual proporciona mayor agilidad y reducción de costos. Además, los sistemas SCADA modernos pueden monitorear inventarios, enviar alertas automáticas para pedidos de materias primas, contactar transportistas y rastrear la entrega de productos **[4]**.

2.4. IoT

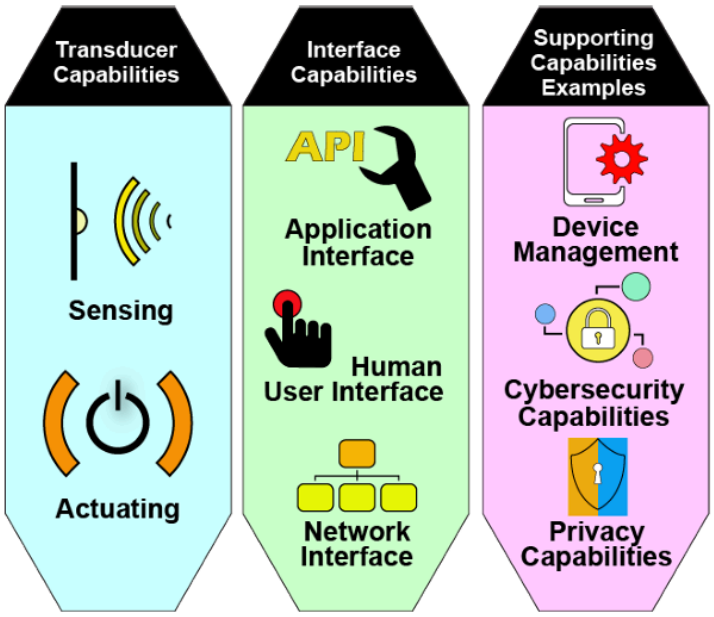
El *Internet de las Cosas* (IoT) se refiere a la interconexión de dispositivos, de manera directa, dentro de una red la cual puede producir datos (por ejemplo, por medio de uso de sensores) que, posteriormente, son enviados a la nube **[6]**. Cada uno de estos dispositivos son lo que, en las siglas de IoT, se conocen como “cosas”. Estas se caracterizan, como bien se dijo en la definición, por generar datos y, cuando hay datos, es crucial tomar medidas de ciberseguridad para protegerlos.

La revolución del IoT ha transformado significativamente el panorama moderno, integrando la conectividad de Internet en una variedad de productos que no son computadoras tradicionales, como electrodomésticos, sistemas de iluminación y calefacción, y dispositivos de monitoreo vehicular. Estos productos incorporan componentes esenciales como una conexión a

Internet, sensores digitales para la recopilación de datos y procesadores para el análisis y ejecución de tareas.

A medida que la industria del IoT avanza, también lo hacen las preocupaciones relacionadas con la seguridad informática. El proyecto *OWASP IoT Top 10* de 2018 identifica las principales vulnerabilidades en dispositivos IoT, destacando riesgos como el uso de contraseñas débiles o codificadas de forma predeterminada, servicios de red inseguros, interfaces del ecosistema inseguras, falta de mecanismos seguros de actualización y el uso de componentes inseguros o desactualizados **[7]**. Estas vulnerabilidades aumentan la exposición de los dispositivos IoT a ataques informáticos y comprometen la seguridad de los datos.

Figura 3



Nota. Describe las capacidades de los dispositivos IoT en tres categorías: transductores (sensado y actuación), interfaces (aplicación, usuario y red) y soporte (gestión, ciberseguridad y privacidad). Tomado de *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (p. 14), por Boeckl, K.; Fagan, M.; Fisher, W.; Lefkovitz, N.; Megas, K.; Nadeau, E.; Piccarreta, B.; O'Rourke, D. G. y Scarfone, K., 2019, NIST.

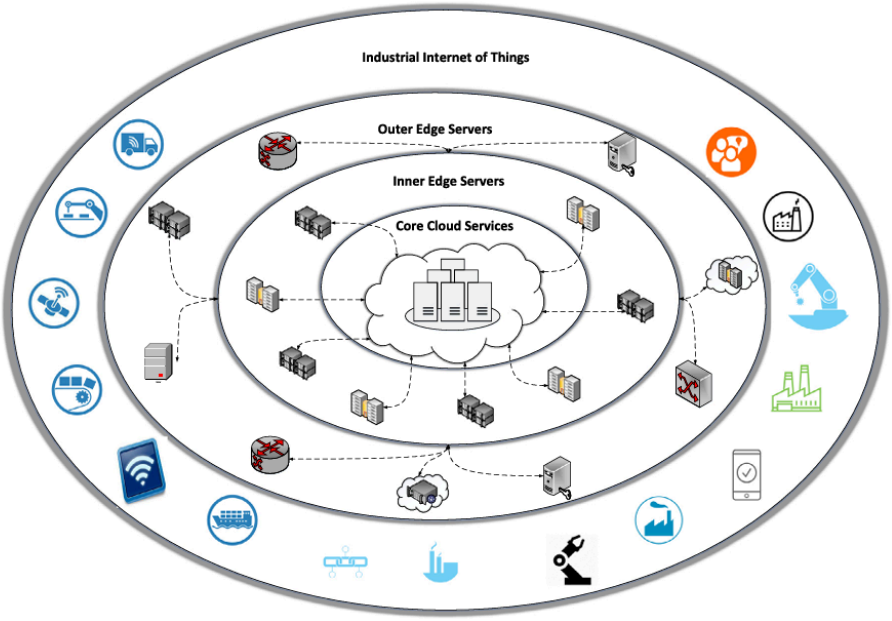
El impacto del IoT no se limita a la vida doméstica; su influencia se extiende a sectores industriales y económicos, promoviendo la eficiencia operativa, la sostenibilidad y la creación de nuevos modelos de negocio. Dentro de la presente tesina el foco se encuentra en la industria, por lo que, a continuación, debemos comprender también qué es IIoT.

2.5. IIoT

El *Internet Industrial de las Cosas* (IIoT) se refiere a la integración avanzada de tecnologías de la información y la comunicación en el entorno industrial, abarcando sectores como la manufactura, la energía, el transporte, las ciudades inteligentes y el sector médico. Esta interconexión se basa en comunicaciones máquina a máquina (M2M), donde los dispositivos y sistemas industriales interactúan y se comunican entre sí y con otros objetos conectados. Estas interacciones generan, procesan y analizan grandes volúmenes de datos de manera inteligente[3], lo que conduce a una gestión más eficiente de los procesos industriales.

[3] "Inteligente" se refiere a la capacidad de los sistemas interconectados para utilizar tecnologías avanzadas, como inteligencia artificial, aprendizaje automático y análisis de datos en tiempo real, con el objetivo de optimizar procesos, predecir fallos y tomar decisiones autónomas basadas en información procesada de forma eficiente.

Figura 4

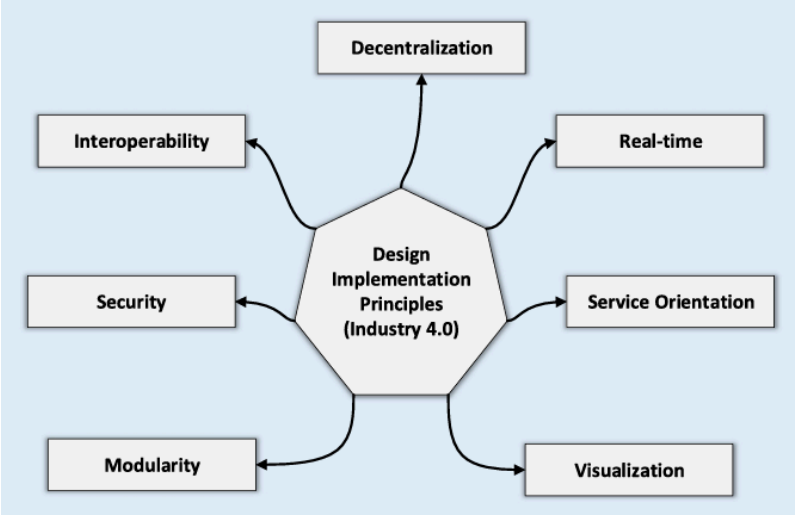


Nota. El gráfico representa la arquitectura del Internet Industrial de las Cosas (IIoT) con recursos de computación en múltiples capas: nube central, servidores internos y externos. Tomado de *The role of big data analytics in industrial Internet of Things* (p. 6), por Rehman, M. H.; Yaqoob, I.; Salah, K.; Imran, M.; Jayaraman, P. P. y Perera, C., 2019, Science Direct.

IIoT tiene como base siete principios fundamentales. El primero es asegurar la interoperabilidad entre tecnologías diversas, como *Sistemas Ciberfísicos* (CPS), dispositivos IoT y plataformas de computación distribuida, con la comunicación inalámbrica como elemento clave para facilitar esta conexión. El segundo principio es la virtualización, que debe aplicarse en múltiples niveles para optimizar la entrega de servicios en plataformas, redes, datos y sistemas operativos. El tercer principio se centra en la descentralización, permitiendo que el

procesamiento y almacenamiento de datos se distribuyan de manera eficiente en todo el sistema. El cuarto principio enfatiza la importancia de la retroalimentación en tiempo real, de modo que todos los usuarios o partes interesadas reciban información actualizada al instante. El quinto principio subraya la necesidad de una *Arquitectura Orientada a Servicios* (SOA), donde cada función del sistema esté disponible como un servicio independiente. El sexto enfoque es la modularidad, para que el sistema pueda evolucionar y adaptarse fácilmente a nuevos requerimientos. Finalmente, el séptimo y último principio (siendo el más relevante e impulsor del presente escrito) es la seguridad, que debe estar integrada en todas las capas del sistema.

Figura 5



Nota. Presenta los siete principios clave para la implementación de diseño en sistemas de la Industria 4.0: descentralización, modularidad, interoperabilidad, seguridad, orientación a servicios, tiempo real y visualización. Tomado de *The*

role of big data analytics in industrial Internet of Things (p. 6), por Rehman, M. H.; Yaqoob, I.; Salah, K.; Imran, M.; Jayaraman, P. P. y Perera, C., 2019, Science Direct.

El IIoT está impulsando una cuarta ola de revolución industrial al transformar fundamentalmente la manera en que operan las industrias, optimizando la utilización de activos, reduciendo costos operativos, mejorando la productividad de los trabajadores y aumentando la seguridad laboral. Además, esta tecnología está creando nuevas fuentes de ingresos, mejorando la sostenibilidad y elevando la experiencia del cliente. En sectores tradicionales como el petróleo, el gas y la manufactura, el IIoT está minimizando la exposición de los trabajadores a ruidos, productos químicos y otros gases peligrosos mediante el uso de sensores y datos en tiempo real para anticipar fallos en el equipo y responder rápidamente a situaciones críticas **[4]**.

Para aprovechar plenamente los beneficios del IIoT, las organizaciones deben sobresalir en tres capacidades tecnológicas clave: la computación impulsada por sensores, la analítica industrial y las aplicaciones de máquinas inteligentes. La convergencia de personas, datos y máquinas inteligentes tendrá impactos profundos en la productividad, eficiencia y operaciones de las industrias a nivel mundial.

Ejemplos claros del impacto del IIoT incluyen el uso de vehículos aéreos no tripulados para inspeccionar oleoductos y la monitorización de la seguridad alimentaria mediante sensores, demostrando cómo estas tecnologías pueden mejorar la precisión y la velocidad de respuesta en

la gestión de infraestructuras críticas. En el Reino Unido, un proveedor de servicios de agua potable y aguas residuales utiliza sensores, análisis y datos en tiempo real para anticipar fallos en el equipo y responder rápidamente a eventos adversos, como fugas o condiciones meteorológicas extremas **[23]**.

Ahora bien, a pesar los grandes beneficios que supone para el sector industrial, incidentes recientes han demostrado cómo los dispositivos IIoT pueden ser comprometidos para actividades maliciosas, destacando la necesidad de robustecer las medidas de seguridad en el diseño y la implementación de estas. Por ejemplo, en 2016, investigadores de Verizon reportaron varios ataques a una empresa de servicios de agua, conocida como *Kemuri Water Company*. Los crackers[4] lograron comprometer el sistema SCADA de la compañía, que estaba basado en un IBM AS/400[5] introducido en 1988. El evento ocurrido permitió a los atacantes manipular el sistema de tratamiento y producción de agua, resaltando la vulnerabilidad de las infraestructuras críticas con tecnología obsoleta **[8]**.

2.6. IT

La *Tecnología de la Información* (más bien conocida como IT o TI) se refiere a cualquier equipo o sistema interconectado de equipos utilizados en la adquisición automática,

[4] Son individuos que vulneran sistemas informáticos o redes con la intención de dañar, robar información o realizar actividades ilícitas, diferenciándose de los "hackers", quienes generalmente buscan explorar o mejorar sistemas sin causar daño.
[5] El IBM AS/400, lanzado en 1988, es un sistema informático de IBM diseñado para pequeñas y medianas empresas, destacando por su facilidad de uso y rendimiento.

almacenamiento, manipulación, gestión, movimiento, control, visualización, conmutación, intercambio, transmisión o recepción de datos o información por una agencia ejecutiva. Este amplio campo incluye computadoras, equipos auxiliares, software, firmware, procedimientos similares, así como servicios de soporte y recursos relacionados. La IT es fundamental para la gestión eficiente y segura de la información en diversos contextos, incluidas las agencias ejecutivas y las organizaciones industriales **[9]**.

En su núcleo, la IT abarca todo el hardware y software que permite a las organizaciones manejar y procesar información de manera automatizada. Las computadoras y dispositivos periféricos, como impresoras, escáneres y dispositivos de almacenamiento, son componentes esenciales que soportan las operaciones diarias de una organización. El software, que incluye sistemas operativos, aplicaciones y herramientas de gestión, proporciona las funcionalidades necesarias para que estos dispositivos realizan tareas específicas de manera efectiva.

La IT es vital para la eficiencia operativa y la toma de decisiones informadas en diversos sectores. En las agencias ejecutivas, la IT facilita la gestión y procesamiento de grandes volúmenes de datos, apoyando la ejecución de políticas y programas gubernamentales. En el ámbito industrial, optimiza la producción, mejora la gestión de la cadena de suministro y permite el control y monitoreo de procesos en tiempo real.

2.7. OT

La *Tecnología Operativa* (más conocida por sus siglas en inglés como OT) se refiere al uso de hardware y software para monitorear y controlar procesos físicos, dispositivos y la infraestructura. Los sistemas de OT se encuentran en una amplia gama de sectores con alta utilización de activos, realizando tareas que van desde el monitoreo de infraestructura crítica hasta el control de robots en plantas de fabricación. Estos sistemas son de gran utilidad en industrias como la manufactura, el petróleo y gas, la generación y distribución eléctrica, la aviación, la marítima, la ferroviaria y los servicios públicos, entre otros. En palabras más sencillas, podríamos decir que OT implica el hardware y software que permite "mantener en funcionamiento cosas" ("cosas" viene de de la "things" de IoT).

La seguridad de la OT es fundamental para proteger estos sistemas críticos. Gartner define la seguridad de OT como las prácticas y tecnologías utilizadas para proteger personas, activos e información; monitorear o controlar dispositivos físicos, procesos y eventos; e iniciar cambios de estado en los sistemas de OT empresariales **[10]**. Las soluciones de seguridad de OT incluyen una variedad de tecnologías de seguridad, desde *Firewalls de Próxima Generación*[6]

[6] Son dispositivos de seguridad avanzados que combinan las funciones tradicionales de un firewall con capacidades como inspección profunda de paquetes, control de aplicaciones y detección de amenazas en tiempo real.

(NGFW) hasta sistemas de *Administración de Eventos e Información de Seguridad*[7] (SIEM), y gestión de identidad y acceso, entre otras.

Tradicionalmente, la ciberseguridad de OT no era una prioridad porque estos sistemas no estaban conectados a Internet, y por lo tanto, no estaban expuestos a amenazas externas. Sin embargo, con la expansión de las iniciativas de innovación digital y la convergencia de las redes de IT y OT, las organizaciones comenzaron a agregar soluciones específicas para abordar problemas particulares. Este enfoque generó una red compleja donde las soluciones no podían compartir información ni proporcionar visibilidad completa **[11]**.

Frecuentemente, las redes de IT y OT se mantienen separadas, duplicando los esfuerzos de seguridad y evitando la transparencia. Estas redes no pueden rastrear de manera efectiva lo que sucede en toda la superficie de ataque, ya que generalmente informan a diferentes departamentos dentro de la organización. Esta falta de coordinación puede dificultar la identificación de los límites de la superficie de ataque, haciendo que las redes de IT y OT sean difíciles de administrar de manera eficiente y dejando grandes brechas en la seguridad.

Una peculiaridad que también se puede destacar es que, desde su concepción, se diseñaron a fin de llevar a cabo tareas en concreto, por ejemplo: control de temperatura, es aquí donde entran los los ICS. Estos son un componente principal de la tecnología operativa. Como

[7] Es una solución que centraliza, analiza y correlaciona datos de seguridad de múltiples fuentes para detectar amenazas, generar alertas y facilitar la gestión de incidentes.

hemos discutido, los ICS incluyen diferentes tipos de dispositivos, sistemas, controles y redes que administran una variedad de procesos industriales. Los más comunes son los SCADA y DCS. Los sistemas SCADA recopilan datos de sensores distribuidos y los envían a una computadora central que administra y controla esos datos. Los DCS se utilizan para administrar controladores locales o dispositivos de sistemas de producción en una ubicación específica.

Previamente, era crucial la supervisión por parte de las personas pero, gracias a los avances introducidos en la *Industria 4.0*[8], como los dispositivos IIOT, estos son componentes cruciales de la tecnología operativa **[6]**. Incluyen sensores, monitores, actuadores y otras tecnologías implementadas en o cerca de equipos de OT, como generadores, tuberías, ventiladores, PLC y *Unidades de Procesamiento Remoto* (RPU). Estos dispositivos IIOT desempeñan un papel fundamental en la recolección de datos y la automatización de procesos.

La convergencia de IT y OT es esencial para la innovación digital, ya que permite que los sistemas de tecnología operativa interactúen con los sistemas de tecnología de la información. Sin embargo, esta conexión expone inmediatamente la red de OT y todos los dispositivos conectados a una amplia gama de amenazas. La OT generalmente no está protegida adecuadamente, ya que fue diseñada originalmente bajo el supuesto de que no estaría expuesta a

[8] La Industria 4.0, también conocida como la cuarta revolución industrial, representa la integración de tecnologías avanzadas como el Internet de las cosas (IoT), inteligencia artificial, análisis de datos, automatización y conectividad en los procesos industriales, con el objetivo de optimizar la producción, personalizar productos y mejorar la eficiencia operativa.

amenazas externas. Además, el aumento del acceso remoto a las redes de OT por parte de proveedores externos amplía aún más la superficie de ataque y crea nuevas vulnerabilidades.

La seguridad efectiva de OT no es negociable debido a la responsabilidad de estos sistemas en el funcionamiento de procesos críticos. Las violaciones en la seguridad de OT pueden provocar interrupciones en servicios esenciales, pérdida de vidas y daños significativos a la infraestructura. Incluso un ataque exitoso contra organizaciones de OT no responsables de la infraestructura crítica puede tener graves consecuencias, como en el caso de una planta de producción de alimentos que podría enviar productos no seguros si se eliminan los controles de seguridad.

3. Desarrollo

3.1. Análisis de la Situación Actual

La presente sección se centra en examinar la creciente amenaza de ataques a sistemas SCADA, evidenciada por incidentes como *Stuxnet*[9], *Aurora*[10] y *Maroochy*[11]. Estos ataques subrayan el riesgo significativo que enfrentan los sistemas SCADA, no sólo en términos de daños económicos y de producción, sino también en términos de impacto potencial en la seguridad pública.

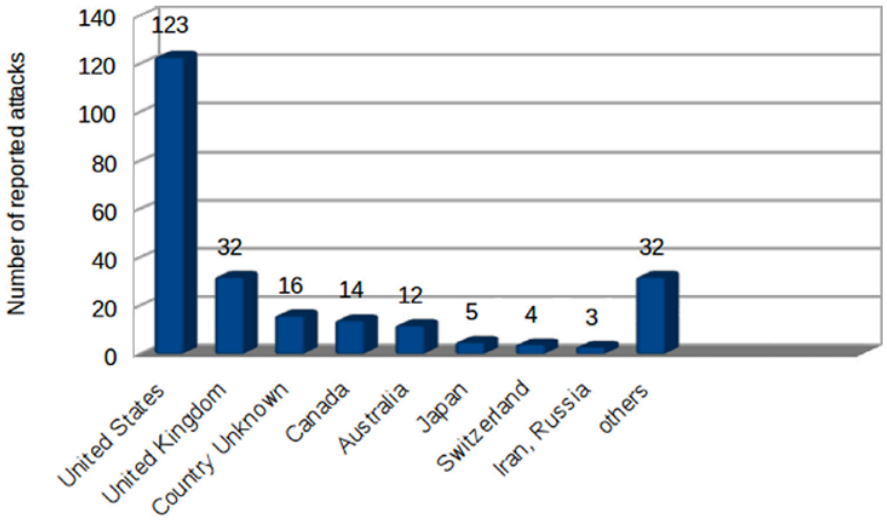
Uno de los mayores desafíos de estos sistemas es su vulnerabilidad física debido a su amplia distribución geográfica. Dado que están diseñados para operar sin interrupciones, la aplicación de parches y actualizaciones puede comprometer su funcionalidad. Además, la dependencia de comunicaciones inalámbricas aumenta la susceptibilidad a ataques de red, y la disponibilidad de patentes y publicaciones sobre sus arquitecturas facilita el acceso a información crítica por parte de potenciales atacantes **[12]**.

[9] Fue un malware dirigido específicamente a sistemas SCADA en plantas nucleares iraníes, descubierto en 2010. Su impacto incluyó la destrucción de centrifugadoras y alteraciones operativas críticas.
[10] Ataque de prueba llevado a cabo en 2007 en el laboratorio de *Idaho National Laboratory*, que demostró cómo era posible dañar físicamente generadores eléctricos mediante comandos maliciosos enviados a sistemas SCADA.
[11] Ataque ocurrido en Australia en 2000, en el que un empleado descontento utilizó un sistema SCADA para liberar aguas residuales en áreas públicas, causando daño ambiental y riesgos de salud.

Diversas bases de datos, como el *Repositorio de Incidentes de Seguridad Industrial* (RISI) y la *Base Nacional de Vulnerabilidades* (NVD), documentan ataques y vulnerabilidades en sistemas SCADA. El RISI, por ejemplo, incluye registros de 242 incidentes documentados entre 1982 y 2017, siendo una de las fuentes más completas para analizar patrones y comprender la taxonomía de los ataques. Sin embargo, se reconoce que el número real de incidentes es significativamente mayor, ya que muchos ataques no se reportan públicamente. Por otro lado, la NVD ofrece un análisis detallado de vulnerabilidades utilizando el sistema CVSS (*Common Vulnerability Scoring System*), evaluando factores como el alcance del ataque, la complejidad y los componentes vulnerables. Estas bases de datos son esenciales para identificar riesgos y desarrollar estrategias de mitigación en entornos SCADA, destacando la necesidad de medidas proactivas para abordar tanto vulnerabilidades conocidas como amenazas emergentes.

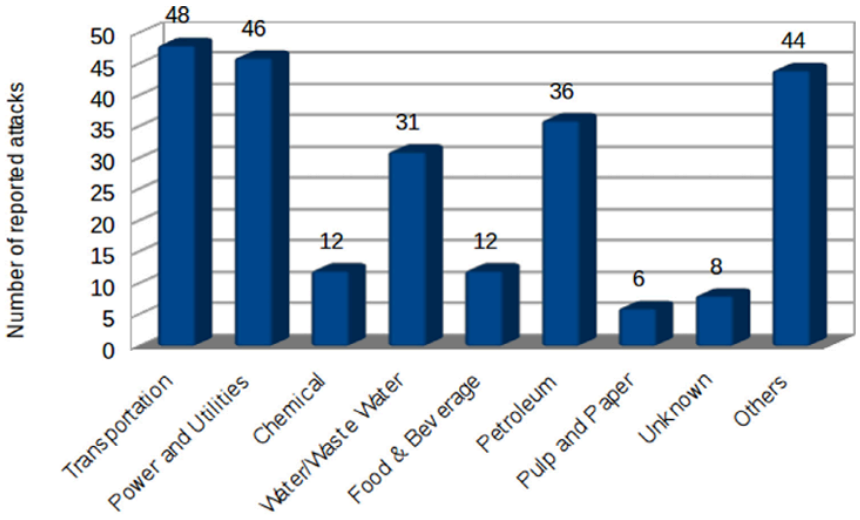
Algunos ataques emblemáticos incluyen el ataque al gasoducto siberiano en 1982, donde un troyano implantado en el sistema SCADA causó daños significativos, y el ataque de *Stuxnet* en 2010, que tuvo como objetivo las centrifugadoras nucleares de Irán, provocando daños al sistema y pérdidas financieras. Estudios como el de *Yadav y Paul (2021)* detallan que los sectores más vulnerables a estos ataques son el transporte, la energía y los servicios públicos, siendo Estados Unidos y Reino Unido los países más afectados por ciberataques a infraestructuras críticas. Además, un informe de *Dell* de 2014 indicó que la frecuencia de ataques a sistemas SCADA se duplicó en un solo año, en gran parte debido a motivaciones políticas **[24]**.

Figura 6



Nota. En el gráfico se puede observar la cantidad de ataques por país, siendo EE.UU. uno de los más afectados. Tomado de *Architecture and security of SCADA systems: A review* (p. 12), por Yadav, G. y Paul, K., (2021), Science Direct.

Figura 7



Nota. Se puede visualizar la cantidad de ataques por sector, donde los tres más afectados son el transporte, energía y agua (vitales para nuestra sociedad). Tomado de *Architecture and security of SCADA systems: A review* (p. 12), por Yadav, G. y Paul, K., (2021), Science Direct.

Para mitigar estos riesgos, es esencial que las industrias adopten políticas de seguridad adecuadas y sigan las directrices de organismos como la *IEEE*[12], la *NERC*[13] y el *NIST*[14]. La actualización y parches constantes, así como un enfoque en sistemas de detección de ataques eficientes, son pasos críticos hacia un entorno SCADA más seguro.

[12] Reconocida por establecer estándares que guían el desarrollo de tecnologías avanzadas. En el ámbito de la ciberseguridad, el IEEE promueve estándares para sistemas SCADA e IoT, orientados a garantizar su resiliencia frente a ataques cibernéticos.
[13] Organización independiente responsable de desarrollar y hacer cumplir estándares que aseguren la fiabilidad del sistema eléctrico en América del Norte. Entre sus contribuciones destaca la serie de estándares CIP (*Critical Infrastructure Protection*), diseñada para proteger infraestructuras críticas contra amenazas físicas y cibernéticas.
[14] Agencia gubernamental de los Estados Unidos dedicada a promover la innovación mediante el establecimiento de estándares tecnológicos y científicos. Su Framework para la Ciberseguridad es ampliamente reconocido por proporcionar directrices prácticas para proteger infraestructuras críticas y mejorar la gestión de riesgos cibernéticos.

3.1.1. Desafíos y Vulnerabilidades Existentes

Uno de los primeros desafíos a los que se enfrentan los sistemas SCADA es la obsolescencia tecnológica. De hecho, muchos de los SCADA actuales hacen uso de sistemas operativos que llegaron al EOL (end-of-life, o en español, "al final de su vida útil") **[13]** y, por lo tanto, ya no se envían actualizaciones de mantenimiento ni parches de seguridad. En base a esto último, los mismos quedan expuestos a vulnerabilidades que pueden ser conocidas por posibles atacantes, trayendo como consecuencia la explotación de estas.

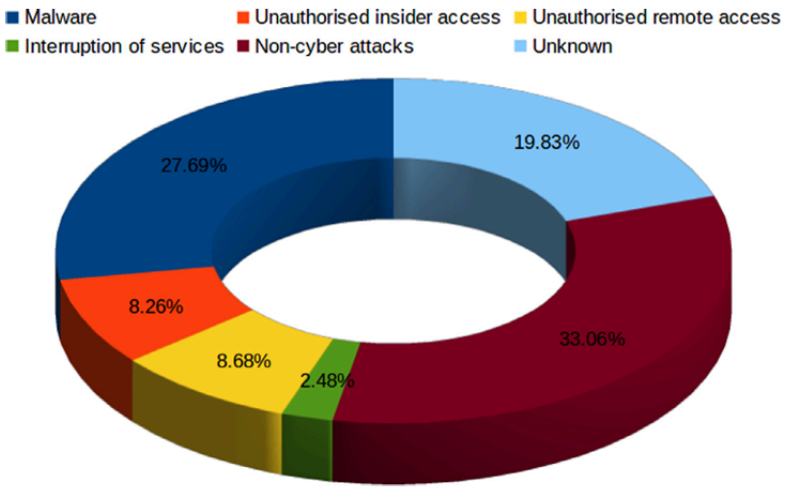
Ahora bien, para la interacción de los componentes físicos de ICS es necesario protocolos de comunicación, siendo algunos de los más populares Modbus, DNP3 y OPC, entre otros. Lo que ocurre es que la mayoría de los protocolos empleados para comunicación industrial no cuentan con medidas de seguridad. De hecho, uno de los puntos más preocupantes es el vinculado a la integridad de los datos, ya que la mayoría de estos protocolos no ofrecen protección de la misma **[13]**, causando entonces en la manipulación no detectada de las comunicaciones. Para comprender la gravedad de ello, imaginemos que un atacante intercepta las comunicaciones entre los sensores de presión y temperatura de los tanques de almacenamiento y el sistema central de control. Al modificar los datos transmitidos, el atacante podría hacer que el sistema central interprete que los niveles de presión y temperatura están dentro de los parámetros seguros, cuando en realidad están alcanzando niveles críticos y, a causa de esta manipulación, no

se tomarían las medidas pertinentes por lo que podría, por ejemplo, ocurrir una explosión o incendio.

Otro desafío significativo es la conectividad a redes externas. Anteriormente estaban aislados pero ahora estos sistemas son accesibles desde redes externas, cosa que ha introducido nuevas posibilidades de ataques.

Por otro lado, también está el acceso físico a los componentes SCADA sin controles estrictos, cosa que puede resultar en sabotaje directo o manipulación de hardware. *Mihai y Andreea (2020)* mencionan en su paper que "todos los sistemas SCADA tienen vulnerabilidades físicas (...). El acceso no autorizado a los activos SCADA representa un alto riesgo; el acceso del personal debe restringirse a quienes son necesarios. El acceso (...) por parte de personal no autorizado puede llevar a daños físicos/destrucción del hardware, robo de hardware y datos, y uso no autorizado de medios extraíbles" (p. 4). Asimismo, se destaca que "dejar puertos abiertos sin asegurar, como USB y RS, puede llevar a la conexión de dispositivos no confiables y a la instalación de software malicioso (registradores de teclas)" (p. 4).

Figura 8



Nota. En este gráfico de torta se representan los tipos de ataque. Tomado de *Architecture and security of SCADA systems: A review* (p. 13), por Yadav, G. y Paul, K., (2021), Science Direct.

La falta de capacitación y conciencia en seguridad del personal operativo es otra vulnerabilidad crítica, es más, la mayoría de los incidentes en sistemas SCADA están relacionados con errores humanos **[13]**. La formación insuficiente en cuanto a medidas de seguridad y reconocimiento de ataques de ingeniería social[15], como el phishing, representa un riesgo significativo. Los atacantes pueden explotar la curiosidad o falta de conocimiento para introducir malware u obtener credenciales de acceso. Además, las configuraciones incorrectas y la gestión de cambios inadecuada pueden dejar activos servicios innecesarios y puertos abiertos,

[15] Técnica de manipulación psicológica utilizada para obtener información confidencial o acceso no autorizado, comúnmente a través de métodos como el *phishing*, que consiste en engañar a las víctimas para que revelen credenciales o información sensible mediante correos electrónicos, mensajes o sitios web fraudulentos.

proporcionando vectores adicionales para el ataque. La ausencia de un inventario preciso y actualizado de los activos y sus configuraciones agrava este problema.

Por último, la falta de validación de los datos de entrada aumentan las posibilidades de ataques, tales como inyecciones SQL[16], desbordamientos de búfer[17] y ataques XSS[18] **[13]**.

Estos desafíos y vulnerabilidades subrayan la necesidad de un enfoque integral de seguridad que incluya tanto medidas técnicas como formación y políticas adecuadas para minimizar los riesgos y proteger los sistemas SCADA contra posibles ataques informáticos (algunos de ellos enumerados en la tabla que se encuentra debajo).

Figura 9

Some types of attacks involved in the SCADA system.

Attack types	Reflection	Initiation
Denial of Service	Enforcing maximum traffic to the network to block the actual communication	Poor authentication platform
Ransomware attacks	Malfunction and operational block of PLCs	Vulnerable hardware
Malicious node attacks	Execution of unauthorized operation	Web interface with an outdated operating system
Phishing attacks	Control over the SCADA system	Absence of network isolation and weak authentication
Worm attacks	Blocks access/operation	No network isolation
Honeypot attacks	Reframe the device function	Weak servers and vulnerable policies on security

Nota. Aquí se pueden observar algunos de los tipos de ataques vinculados a SCADA. Tomado de *SCADA securing system using deep learning to prevent cyber infiltration* (p. 3), por Diaba, S. Y; Anafo, T.; Tettech, L.; Oyibo, M. A.; Alola, A.A.; Shafie-khah, M. y Elmusrati, M., 2023, Science Direct.

[16] Ataques que explotan la falta de validación de entradas en consultas SQL, permitiendo a los atacantes manipular bases de datos para acceder, modificar o eliminar información sensible.
[17] Vulnerabilidades que ocurren cuando un programa escribe más datos en un búfer de los que puede manejar, lo que puede permitir la ejecución de código malicioso o la corrupción de datos.
[18] Exploits que inyectan scripts maliciosos en sitios web confiables, con el objetivo de robar datos, secuestrar sesiones o redirigir usuarios a sitios no deseados.

3.1.2. Consecuencias de un ataque exitoso

Las repercusiones de un ataque exitoso contra uno de estos sistemas van más allá del nivel técnico, pudiendo perjudicar otros aspectos como el económico, social y político. Uno de los ataques más complejos es aquel que tiene como objetivo la interrupción de servicios esenciales, como por ejemplo el ataque a la red eléctrica de Ucrania en 2015 la cual dejó a 225.000 personas sin suministro eléctrico durante varias horas **[13]**. La interrupción de servicios como la electricidad, el agua o las telecomunicaciones puede tener efectos en cascada, impacto no solo observable desde el lado social, sino también en la economía en sí.

Desde el punto de vista económico, un ataque como el que sufrió Ucrania en el 2015 tiene un gran impacto, ya que la interrupción de operaciones y la necesidad de reparar o reemplazar equipos dañados puede tener un costo considerable para las empresas y el gobierno. También está el hecho vinculado a la pérdida de confianza en la seguridad de estos sistemas, pudiendo resultar en una disminución de la inversión y un aumento en los costos de seguros.

A nivel social y político, estos ataques pueden socavar la confianza del público en la capacidad del gobierno y de las empresas para proteger los servicios esenciales para la sociedad. Una gran ejemplo de ello es el caso del ataque con el gusano *Stuxnet*, siendo que éste virus desacreditó al gobierno iraní al dejar en evidencia su incapacidad para proteger este tipo de instalaciones frente a ciberataques. El impacto fue tal que, el hecho de que el virus se haya

propagado a otras computadoras en el mundo y no sólo haya afectado los sistemas de control de la red nuclear, generó un sentimiento de incertidumbre y miedo a nivel global **[25]**.

De hecho, si estos ataques son percibidos como actos de guerra o terrorismo, la atribución de los mismos a un estado nación puede escalar tensiones y llevar a represalias, afectando las relaciones diplomáticas y la estabilidad global. Además de estos impactos, los ataques exitosos pueden resultar en la pérdida o robo de información sensitiva. La exfiltración de datos puede comprometer la seguridad nacional y proporcionar ventajas estratégicas a actores hostiles. En el ámbito industrial, esto puede incluir secretos comerciales y datos de propiedad intelectual.

Mayormente, cuando se piensa en seguridad informática, se suele limitar el daño a los equipos o la información, sin embargo, hay que tomar consciencia de que es posible que dichos ataques tengan el potencial de causar daño físico directo. Volviendo al caso de *Stuxnet*, el mismo logró alterar la velocidad de las centrifugadoras en la planta nuclear de Natanz, resultando en su desgaste y eventual destrucción. Este tipo de daño no solo interrumpe las operaciones, sino que también puede requerir costosas reparaciones o reemplazos. Pero, más allá de la destrucción de los equipos, el caso de Irán podría haber costado vidas.

Finalmente, está el impacto psicológico de un ataque exitoso, el cual no debe ser subestimado. La sensación de inseguridad y vulnerabilidad puede persistir mucho después de que

los servicios hayan sido restaurados. Esto puede afectar tanto a los empleados de las infraestructuras comprometidas como al público en general.

3.1.3. Análisis de la Integración de IoT y SCADA

Los sistemas SCADA son comúnmente empleados a fin de controlar la IIoT de la infraestructura crítica urbana **[14]**. Como ya hemos hablado, los mismos fueron diseñados originalmente para operar en entornos aislados y maximizando la funcionalidad, se encuentran ahora interconectados a una red más amplia de dispositivos IIoT que aporta beneficios importantes, como monitoreo en tiempo real, reducción de costos operativos y facilidad en la actualización de software y mantenimiento. Estos beneficios se deben en gran medida a la adopción de servicios en la nube, que permiten a los proveedores implementar mejoras de manera uniforme y escalable para todos los usuarios. Sin embargo, esta transición presenta desafíos significativos en términos de seguridad y rendimiento **[12]**.

Uno de los principales desafíos es la expansión de la superficie de ataque. Los dispositivos IIoT, debido a su naturaleza distribuida y su necesidad de conectividad se ven enfrentados, por ejemplo, a la posibilidad de acceso no autorizado a través de redes IP y la explotación de vulnerabilidades en protocolos de comunicación no seguros. Esta diversidad y heterogeneidad de dispositivos complican aún más la gestión de la seguridad, ya que cada dispositivo puede tener diferentes niveles de seguridad y configuraciones, lo que crea una

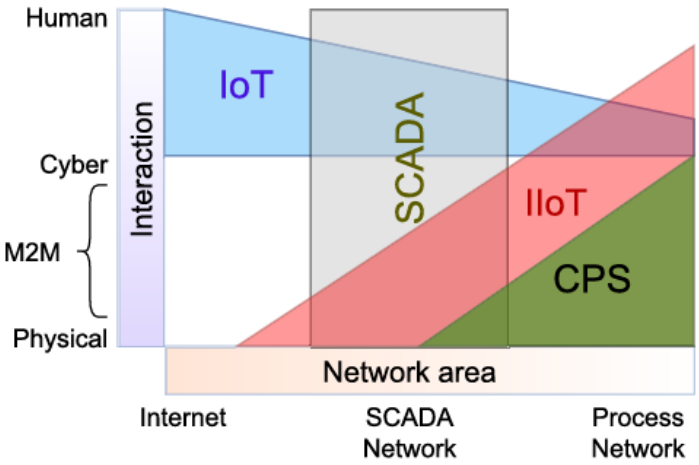
disparidad en la defensa de la red. Algunos ataques incluyen *MitM*[19] y *DoS*[20], debido a la dependencia de la comunicación en la nube y la exposición potencial a nuevas amenazas.

Por otro lado, en lo que respecta a los protocolos de comunicación, algunos como *Modbus/TCP*, *IEC 60870* y *DNP3*, que como se mencionó anteriormente son comúnmente utilizados en estos sistemas, carecen de la seguridad necesaria para soportar ataques sofisticados. Además, el uso de soluciones comerciales en lugar de propietarias aumenta el riesgo, ya que la información enviada a la nube puede ser interceptada o manipulada **[12]**.

Como ya vimos, otro desafío crítico es la gestión de actualizaciones y parches de seguridad. Los sistemas SCADA tradicionales operan bajo condiciones que requieren alta disponibilidad y estabilidad continua, lo que dificulta la implementación de parches de seguridad de manera oportuna sin interrumpir las operaciones. Esta situación se agrava en el entorno IIoT, donde los dispositivos a menudo son fabricados por diferentes proveedores, cada uno con sus propios ciclos de actualización y políticas de seguridad. Esto puede resultar en inconsistencias y brechas de seguridad que son difíciles de gestionar y mitigar.

[19] Ataque en el que un actor malicioso intercepta y manipula la comunicación entre dos partes sin que estas lo detecten, permitiendo el robo de datos, modificación de información o la suplantación de identidad.
[20] Ataque que busca interrumpir el funcionamiento normal de un sistema o red, sobrecargándolo con tráfico malicioso o explotando vulnerabilidades para que los servicios se vuelvan inaccesibles a los usuarios legítimos.

Figura 10



Nota. El gráfico muestra la distribución de tecnologías IoT, IIoT, SCADA y CPS en redes, destacando los niveles de interacción (humana, cibernética y máquina a máquina) y su ubicación en áreas de red como Internet, redes SCADA y redes de proceso. Tomado de *SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0* (p. 10), por Sverko, M.; Grbac, T. G. y Mikuc, M., 2022, IEEE.

En el artículo de *Falco, Caldera y Shrobe (2018)*, se subraya la necesidad de desarrollar modelos de riesgo específicos para evaluar las vulnerabilidades en sistemas SCADA conectados a IIoT. Utilizando métodos estadísticos y pruebas de similitud coseno, se puso en vista que los sistemas SCADA poseen atributos de riesgo únicos que los diferencian de otros sistemas de software. Contrariamente a la creencia común, los autores encontraron que los métricos de riesgo del sistema de puntuación de vulnerabilidades comunes (CVSS) no siempre son indicativos de la

explotabilidad en el contexto de SCADA. Este hallazgo subraya la necesidad de un esquema de priorización de riesgos específico y personalizable para estos sistemas críticos.

El modelo propuesto permite identificar métricas de riesgo específicas que pueden utilizarse para evaluar la probabilidad de explotación de vulnerabilidades relacionadas con SCADA. Esta evaluación es crucial, dado que la explotación de vulnerabilidades en sistemas SCADA puede tener consecuencias catastróficas, desde la interrupción de servicios esenciales hasta daños físicos en infraestructuras críticas. La creación de un esquema de priorización de riesgos basado en datos ayuda a los investigadores y profesionales de la seguridad a enfocarse en las vulnerabilidades más críticas y desarrollar soluciones específicas para mitigar estos riesgos.

Éste estudio también destaca la importancia de políticas y marcos regulatorios que fomenten la adopción de mejores prácticas de ciberseguridad. Sin embargo, la implementación de tales marcos puede ser costosa y requerir un esfuerzo considerable, lo que presenta una barrera para muchas organizaciones. En este contexto, un enfoque basado en la priorización de riesgos puede proporcionar una solución más accesible y efectiva para mejorar la seguridad de sistemas SCADA en la era del IIoT. La adopción de estos marcos debe ir acompañada de una capacitación continua del personal operativo y de la implementación de políticas claras de gestión de cambios para minimizar los riesgos asociados con las actualizaciones y configuraciones incorrectas.

Desde la perspectiva de la arquitectura de red, el desafío radica en que los dispositivos IIoT poseen capacidades limitadas de cómputo en comparación con los servidores SCADA tradicionales. Esto puede causar problemas de interoperabilidad y redundancia en los datos, ya que las distintas capas de la red deben ser capaces de procesar y gestionar un volumen creciente de datos sin perder precisión ni rendimiento. Los dispositivos IIoT se comunican en redes heterogéneas donde deben coexistir protocolos de comunicación industrial con redes TCP/IP, lo que puede alterar el flujo de datos convencional y crear una estructura de red más compleja **[15]**. En algunos casos, los dispositivos IoT de consumo podrían no ser adecuados para el entorno industrial, donde las comunicaciones *M2M*[21] requieren tiempos de respuesta inmediatos y operaciones críticas en tiempo real, algo que los sistemas SCADA tradicionalmente han gestionado en aislamiento.

Adicionalmente, la integración de IoT en SCADA afecta directamente la jerarquía funcional tradicional de la pirámide de automatización *ISA-95*[22]. La capacidad de los dispositivos IIoT para comunicarse directamente con niveles superiores (IT y nube) facilita la transmisión de datos críticos en tiempo real, lo que puede reducir la necesidad de una supervisión centralizada y hacer que el SCADA opere como una fuente de datos complementaria **[15]**. Esto debilita la

[21] Machine-to-Machine: Tecnología que permite la comunicación directa entre dispositivos o máquinas sin intervención humana, generalmente mediante redes inalámbricas o cableadas. Es ampliamente utilizada en aplicaciones de IoT (Internet of Things) y SCADA para automatizar procesos y compartir datos en tiempo real.
4o
[22] Estándar internacional que define la jerarquía funcional en sistemas industriales, organizando operaciones desde dispositivos de campo hasta la planificación empresarial.

claridad estructural de los sistemas industriales tradicionales, ya que cada dispositivo IIoT se comporta como un nodo independiente en una red distribuida, lo cual podría desestabilizar la arquitectura de control y supervisión, a menos que se implemente una planificación meticulosa de la infraestructura de red.

3.1.3.1. IoT y el Modelo Purdue

El *Modelo Purdue*, desarrollado en los años 90 como una arquitectura de referencia por el consorcio de la *Universidad de Purdue* y el comité *ISA99*[23], establece una estructura jerárquica para sistemas ICS. Este modelo segmenta las funciones operativas y empresariales en seis niveles o capas, cada una con un propósito específico y medidas de seguridad acordes a su nivel de criticidad. A través de esta estructura, el *Modelo Purdue* permite establecer controles de acceso diferenciados, segmentando la infraestructura de producción y minimizando los riesgos asociados a la interacción entre redes TI y OT.

En dicho modelo, los sistemas y dispositivos de OT suelen ubicarse en los niveles inferiores, ya que representan activos críticos para el control y monitoreo de los procesos de producción. Los sistemas de TI, por su parte, se sitúan en los niveles superiores, donde la conectividad a redes externas y la capacidad de decisión empresarial son más comunes. Una

[23] Estándar internacional para la seguridad en sistemas de control industrial, que proporciona directrices para proteger infraestructuras críticas frente a amenazas cibernéticas. Actualmente conocido como IEC 62443.

Zona de Desmilitarización[24] (DMZ) separa ambas áreas, permitiendo un control adicional que limita el intercambio de datos entre TI y OT y disminuye la exposición a amenazas provenientes de la red de TI.

Ahora bien, la adopción de tecnologías IoT y servicios en la nube ha planteado desafíos significativos para el modelo Purdue **[16]**. La conectividad directa de dispositivos OT con servicios externos y la dependencia de los dispositivos IoT de conectividad en tiempo real rompen las barreras establecidas por el modelo, ya que estos dispositivos necesitan interactuar frecuentemente con redes y servicios externos para recibir actualizaciones, realizar monitoreo remoto o recibir soporte técnico. Además, el uso de gateways IoT en la arquitectura introduce nuevos puntos de vulnerabilidad, al concentrar la comunicación de múltiples dispositivos a través de una sola interfaz, lo cual podría convertirse en un punto de fallo crítico y un vector atractivo para ataques **[16]**.

Para enfrentar estos desafíos, las políticas de seguridad de comunicaciones basadas en el *Modelo Purdue* pueden adaptarse mediante la creación de zonas de seguridad adicionales dentro de cada nivel, especialmente en aquellos que interactúan directamente con redes externas. También es recomendable implementar gateways seguros que integren autenticación avanzada y cifrado, así como aplicar controles de acceso restrictivos a dispositivos y servicios autorizados.

[24] Es una red perimetral diseñada para separar una red interna segura de redes externas no confiables, proporcionando una capa adicional de seguridad al alojar servicios accesibles públicamente, como servidores web o de correo.

Adicionalmente, el monitoreo en tiempo real de las conexiones entre TI, OT y servicios en la nube en la zona de DMZ permite detectar y responder rápidamente a posibles amenazas de seguridad.

Sin embargo, aunque dicho modelo ofrece una base sólida para la segmentación y control de redes ICS, su integración con tecnologías IoT requiere ajustes en las políticas de seguridad. Se estará realizando un análisis exhaustivo de la seguridad de las comunicaciones en estos sistemas en las próximas páginas.

3.1.4. Casos de Estudio de Incidentes Relevantes

3.1.4.1. Ataque a Oldsmar Water Treatment Plant (2021)

El ataque a la planta de tratamiento de agua de Oldsmar, que tuvo lugar en Florida, más específicamente en Febrero de 2021, expuso las vulnerabilidades de las infraestructuras críticas que involucran éste tipo de sistemas y subrayó la necesidad de mejorar las medidas de ciberseguridad en estos.

El ataque tuvo lugar en una planta de tratamiento de agua que utilizaba un sistema SCADA para supervisar y controlar las operaciones de tratamiento. En la mañana del 5 de Febrero, un operador de la planta, conocido bajo el pseudónimo "Ramone", observó que alguien

accedió brevemente a su computadora de forma remota, lo cual no consideró inusual inicialmente, ya que su supervisor solía acceder al sistema desde otros equipos. Sin embargo, más tarde, a la 1:30 pm, presenció cómo alguien tomó control del mouse y cambió los niveles de hidróxido de sodio. Este cambio podría haber tenido consecuencias desastrosas, pero Ramone actuó rápidamente para revertir los ajustes y notificó a su supervisor.

El aumento de los niveles de hidróxido de sodio en el agua potable podría haber envenenado a miles de residentes **[17]**. El rápido accionar del operador impidió una catástrofe, pero el incidente puso de manifiesto las problemáticas que ya hemos estado abordando. La investigación subsecuente realizada por *Kardon* (2021), reveló que el sistema comprometido permitía acceso remoto a través de *TeamViewer*[25], software el cual por un lado carecía de un configuración adecuada y que probablemente no estaba autorizado.

El impacto de este ataque se sintió a nivel nacional, llevando a que el senador *Marco Rubio* declarara el incidente como una cuestión de seguridad nacional. Las autoridades locales y federales, incluyendo entre algunos de ellos al *FBI* y la *Agencia de Ciberseguridad e Infraestructura* (CISA), iniciaron investigaciones para entender el alcance del ataque y prevenir futuros incidentes similares, publicando en el sitio web de la CISA el artículo *Compromise of U.S. Water Treatment Facility (2021)*. A partir de dichas investigaciones notaron que los

[25] Software de acceso remoto que permite conectar dispositivos y controlar sistemas de forma remota.

atacantes, a parte de aprovechar los softwares de acceso remoto a escritorios, también apuntan a aquellas redes de computadoras que hacen uso de sistemas operativos que están llegando a su EOL. En éste caso particular, el OS utilizado era Windows 7, al cual Microsoft dejó de brindar soporte y actualizaciones el 14 de febrero de 2020, pudiéndose optar por una *Actualización de Seguridad Extendida* (ESU) hasta enero del 2023.

El caso de la planta de Oldsmar expuso varias vulnerabilidades críticas en la seguridad de estos sistemas. La utilización de software de acceso remoto no seguro como *TeamViewer* sin las adecuadas configuraciones de seguridad facilitó el acceso de los atacantes. Aunque el operador detectó el ataque y respondió rápidamente, la falta de sistemas automáticos de detección y respuesta retrasó la mitigación del riesgo.

El incidente de Oldsmar ha llevado a un llamado generalizado a mejorar las prácticas de ciberseguridad en los sistemas SCADA. Algunas de las medidas recomendadas por la CISA en base a éste caso incluyeron:

- Mantener actualizados los sistemas operativos a utilizar para recibir actualizaciones y parches de seguridad.
- Emplear autenticación multifactor (MFA) para agregar una capa adicional de protección.

- Usar contraseñas robustas para proteger las credenciales del Protocolo de Escritorio Remoto (RDP).
- Corroborar que el antivirus, los filtros de spam y los firewalls estén actualizados, correctamente configurados y sean seguros.
- Auditar la red y los logs realizados.
- Identificar y suspender en caso de que algún usuario que exhiba actividad sospechosa.

Por otro lado, también dieron recomendaciones específicas para aquellas infraestructuras críticas vinculadas al aprovisionamiento de servicios de agua y a aquellos que hagan o quieran hacer uso de software de control remoto.

3.1.4.2. Ataque a Colonial Pipeline (2021)

El ataque de *ransomware*[26] que tuvo lugar en Mayo del 2021 se lo conoce como uno de los incidentes de ciberseguridad más disruptivos y de mayor perfil en la historia reciente de los Estados Unidos **[18]**, ¿y esto por qué? *Colonial Pipeline* es uno de los principales proveedores de combustible del país, el hecho de que dicho ataque pausara sus actividades llevó no solo a una escasez general de combustible, sino que también tuvo impactos económicos en ese mercado.

[26] Tipo de malware que bloquea el acceso a los datos o sistemas de una víctima mediante cifrado, exigiendo un pago (generalmente en criptomonedas) para restaurar el acceso.

Siguiendo la ley de oferta y demanda, si aumenta la demanda y hay poca oferta lo que se produce es un aumento de precios.

Las implicaciones de tal ataque involucran tanto al sector público como privado. Para comprender la gravedad del mismo hay que tener en cuenta que *Colonial Pipeline* operaba el mayor sistema de oleoductos de productos refinados de petróleo en el país que va desde Houston hasta Nueva York, entregando a diario 100 millones de galones a clientes de 14 estados diferentes, además de proveer sus servicios al sector militar y aéreo. Por lo que, en síntesis, podríamos decir que esta empresa cumple un rol crucial en la infraestructura energética nacional.

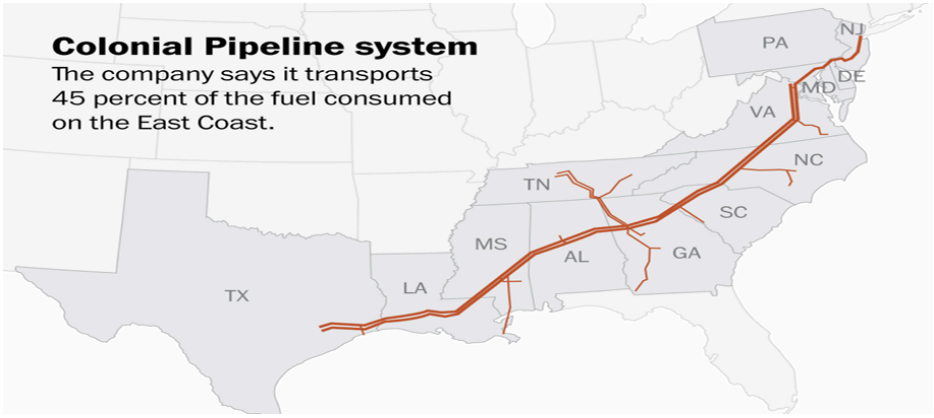
Adentrándonos un poco más, el ataque que dejó "en paro" a esta compañía fue ocasionado por un grupo de *crackers*[27] llamados "Darkside" quienes introdujeron una especie de *RaaS* (es decir, Ransomware como Servicio). Este tipo de ataque implica que un grupo de ciberdelincuentes desarrollen el ransomware y luego lo alquilan para que otro grupo de atacantes lleve a cabo esa acción.

La siguiente pregunta que surge es "¿Cómo obtuvieron acceso?". Esto fue gracias a una cuenta de una red privada virtual (VPN) que usaba un empleado. La explotación de esa vulnerabilidad trajo consigo el cierre de las operaciones del oleoducto, pánico entre los

[27] Individuos o grupos que acceden ilegalmente a sistemas informáticos con intenciones maliciosas, como robar datos, causar daños o comprometer la seguridad.

consumidores, escasez de combustible en las estaciones de servicio, aerolíneas que tuvieron que desviar vuelos e, incluso, el gobierno de EE.UU. declaró una emergencia regional.

Figura 11



Nota. En el mapa se puede apreciar las zonas afectadas por dicho ataque. Tomado de *To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack* (p. 9), por Gawazah, L., 2024, Research Gate.

El CEO, *Joseph Blount*, junto con su equipo se veían enfrentados a dos alternativas: pagar el rescate o tratar de restaurar el sistema sin las herramientas de descifrado. Por un lado, la primera opción era compleja ya que se opone a la política del país que indica que no hay que negociar con ciberdelincuentes, así como también el hecho de que una decisión como esa podría ser una forma de alentar a más ataques del estilo. Analizando la otra opción, eso puede

involucrar desde semanas hasta meses de inactividad y, como vimos, el poco tiempo de interrupción del oleoducto tuvo grandes impactos en el país.

Luego de 24 horas del ataque se pagó el rescate cosa que permitió restaurar las operaciones sin embargo, esto dejó grandes estragos desde la confianza hasta el cuestionamiento de la decisión tomada.

En un sorprendente giro de los acontecimientos después de recibir el pago del rescate de *Colonial*, el *Departamento de Justicia de EE. UU.* anunció que había rastreado y recuperado aproximadamente 2.3 millones de los 4.4 millones de dólares en *Bitcoin*[28] que la compañía pagó a *DarkSide*. Los investigadores federales dominaron técnicas para acceder a las carteras digitales utilizadas por los ciberdelincuentes. Aunque fue aclamado como una victoria simbólica contra los grupos de ransomware, el incidente subrayó las vulnerabilidades en aquella infraestructura.

Las investigaciones en el *Congreso* cuestionaron al liderazgo de *Colonial Pipeline* sobre sus prácticas de seguridad y la decisión de pagar el rescate. *Joseph Blount* defendió la decisión como necesaria para mitigar una disrupción económica mucho mayor. Según *Blount*, la empresa no tenía otra opción dada la escasez de combustible que se estaba extendiendo por varios estados de EE. UU. El cierre prolongado del oleoducto significaba que "no se trataba de mis accionistas,

[28] Moneda digital descentralizada basada en tecnología blockchain. Es ampliamente utilizada en transacciones anónimas, incluidos pagos relacionados con actividades ilícitas como el ransomware, debido a su difícil trazabilidad y la facilidad para transferir fondos a nivel global.

no se trataba de *Colonial Pipeline*. Se trataba de mantener en funcionamiento... hospitales y socorristas," dijo *Blount* al *Wall Street Journal*.

Después del ataque, *Colonial* invirtió fuertemente en controles de ciberseguridad, contrató a su primer director de seguridad de la información (CISO) e implementó capacitación en seguridad a nivel de toda la compañía. Los sistemas heredados obsoletos de la empresa y los recursos de ciberseguridad insuficientes se identificaron como áreas clave que requerían mejoras.

El ataque resultó ser entonces una dura llamada de atención sobre las vulnerabilidades que subyacen en los sistemas que impulsan la sociedad moderna. Impulsando al gobierno de EE. UU. a fortalecer las regulaciones de ciberseguridad y la supervisión de la infraestructura energética del país. Organismos reguladores como la *Administración de Seguridad en el Transporte* (TSA) emitieron rápidamente nuevos mandatos para los operadores de oleoductos. El *Congreso* también aprobó leyes como la *Ley de Notificación de Incidentes Cibernéticos* (Cyber Incident Reporting Act), que exige que las entidades de infraestructura crítica reporten incidentes cibernéticos.

3.2. Pilares y Estructura del Framework

El framework se sostiene sobre cuatro pilares fundamentales. El primer pilar, *Organización*, está diseñado para asegurar que las estructuras internas y externas de la entidad

sean capaces de soportar eficazmente las políticas de ciberseguridad. Este pilar establece roles y responsabilidades claras, fomenta la formación de equipos especializados y promueve la colaboración entre departamentos internos, como los de IT y OT, y actores externos, como proveedores tecnológicos y organismos reguladores. En el presente trabajo, como se detalló en las limitaciones, no se ahondará específicamente en dicho punto, sin embargo es una pieza fundamental la cual será incluida en parte dentro de los subtítulos desarrollados.

El segundo, *Arquitectura de Activos y Comunicación*, se enfoca en asegurar la infraestructura de conectividad de los sistemas. Este pilar abarca la protección de redes cableadas a través de estándares seguros, la implementación de medidas específicas para redes inalámbricas y la *Política de Perímetro*, que incluye el uso de firewalls y segmentación de redes para limitar el acceso no autorizado.

El tercer pilar, *Clasificación y Gestión de la Propiedad de los Datos*, el cual establece políticas para proteger la información crítica. Esto incluye medidas como la *Política de Respaldo de Datos*, que se centra en la recuperación de información en caso de incidentes; la *Política de Almacenamiento y Destrucción de Datos*, que regula el manejo seguro de los datos durante su ciclo de vida; y la *Política de Protección contra Software Malicioso*, destinada a prevenir infecciones, principalmente por malware, que puedan comprometer la integridad de los sistemas.

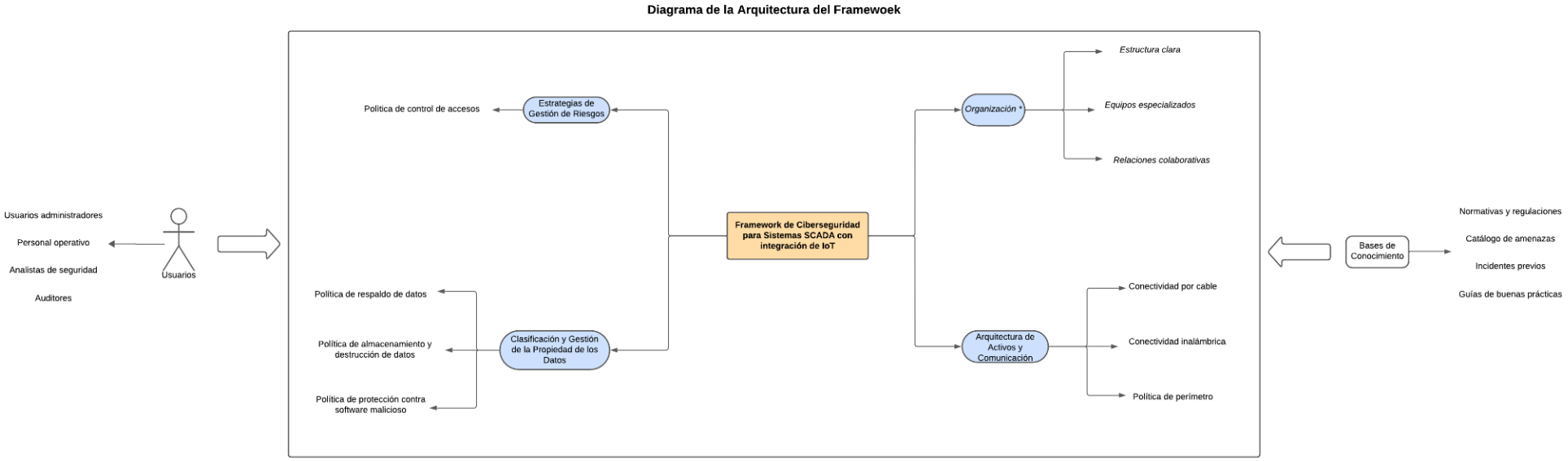
Finalmente, el cuarto, *Estrategias de Gestión de Riesgos*, que se centra en identificar, evaluar y mitigar los riesgos inherentes a estos sistemas. Dentro de este pilar, destaca la *Política de Control de Acceso*, que regula los permisos y privilegios de los usuarios para minimizar la posibilidad de accesos no autorizados a sistemas y datos sensibles.

El framework no opera de forma aislada; su eficacia depende de su interacción con elementos externos. Entre estos, los usuarios ocupan un lugar destacado. Este grupo incluye a administradores, personal operativo, analistas de seguridad y auditores, quienes desempeñan roles esenciales en la implementación, supervisión y evaluación de las medidas de seguridad. Su capacitación y concienciación son fundamentales para minimizar errores humanos y responder de manera efectiva a incidentes.

Otro componente externo clave es la base de conocimiento, un repositorio centralizado que incluye normativas y regulaciones, catálogos de amenazas conocidas, registros de incidentes previos y guías de buenas prácticas.

Cada una de estas piezas, incluyendo los pilares, serán detallados con mayor profundidad en las páginas posteriores.

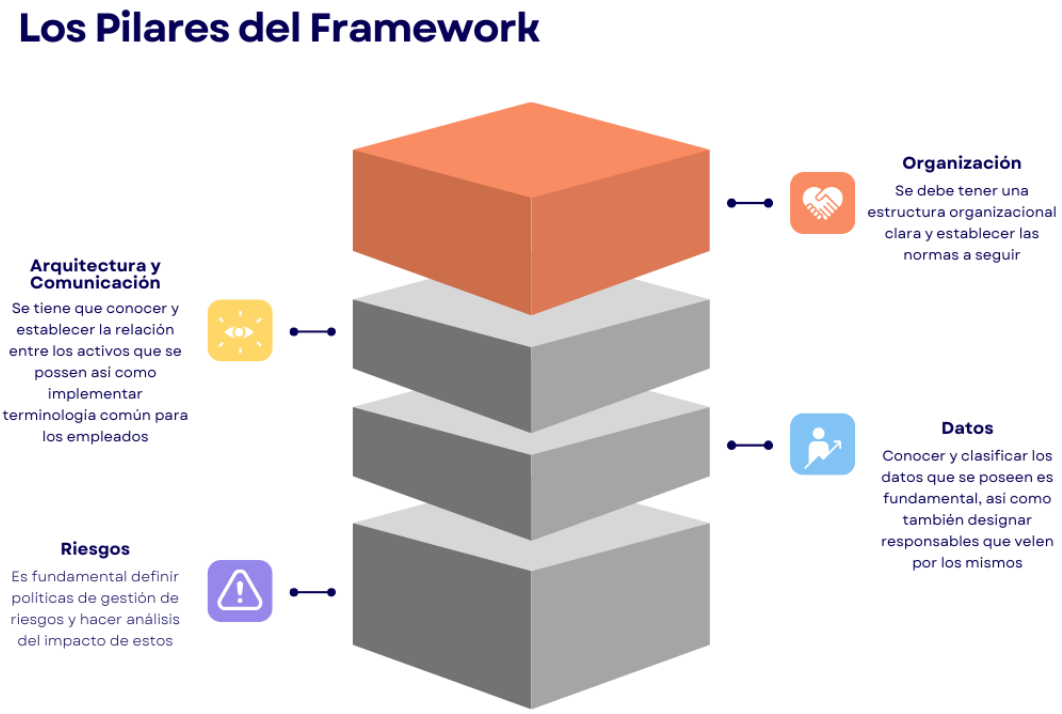
Figura 11



Nota. El presente esquema fue realizado en Lucidchart.

3.2.1. Organización

Figura 12



Nota. Gráfico que diseñado por mí utilizando una plantilla de Canvas para simplificar la visualización de los pilares que sostienen este framework.

Lo primero es tener una organización interna bien definida y relaciones colaborativas robustas. La estructura organizacional debe ser clara, con roles y responsabilidades específicos. Caso contrario, si no hay asignada una tarea y/o responsabilidad, lo más probable es que las políticas o lineamientos que se establezcan se ignoren ya que no hay nadie quien vele por el cumplimiento de los mismos.

Luego, viene la definición de qué políticas, normas o escritos (tanto obligatorios como aquellos que funcionan como guía o referencia) serán utilizados dentro de la empresa. Por ejemplo, las empresas que se dedican a la industria eléctrica podrían elegir alinearse a la *NERC 1500*[29].

Los altos ejecutivos, como el *Director de Información* (CIO) y el *Director de Seguridad de la Información* (CISO), son responsables de supervisar la estrategia de seguridad. Este nivel asegura la asignación adecuada de recursos y la alineación de las políticas de seguridad con los objetivos estratégicos de la organización. Un equipo especializado en seguridad SCADA debe estar compuesto por expertos con conocimientos profundos en sistemas OT, IT y IIoT.

Los administradores de sistemas y redes gestionan la infraestructura tecnológica subyacente, asegurando la configuración segura de dispositivos, la aplicación de parches y

[29] Conjunto de estándares desarrollados por la *North American Electric Reliability Corporation* (NERC) para proteger la infraestructura crítica del sector eléctrico en América del Norte, centrándose en la ciberseguridad y la resiliencia operativa frente a amenazas.

actualizaciones, y el monitoreo constante de las redes SCADA e IoT para detectar y responder a actividades sospechosas. Los operadores de SCADA son responsables del control diario de los procesos industriales y deben estar capacitados en prácticas de seguridad para identificar y reportar incidentes potenciales. Un equipo de respuesta a incidentes (CSIRT) gestiona y responde a incidentes de seguridad, incluyendo la detección, contención, mitigación y recuperación de sistemas afectados. También se encargan de la comunicación con las autoridades regulatorias y otras partes interesadas durante un incidente.

Por otro lado, es crucial establecer relaciones colaborativas tanto internas como externas. La cooperación entre los departamentos de TI y OT es vital. El departamento de TI se enfoca en la seguridad de la información y la gestión de datos, mientras que el departamento de OT se encarga de la operación y mantenimiento de los sistemas de control industrial. Una integración eficaz entre estos departamentos asegura que las políticas de seguridad sean coherentes y completas.

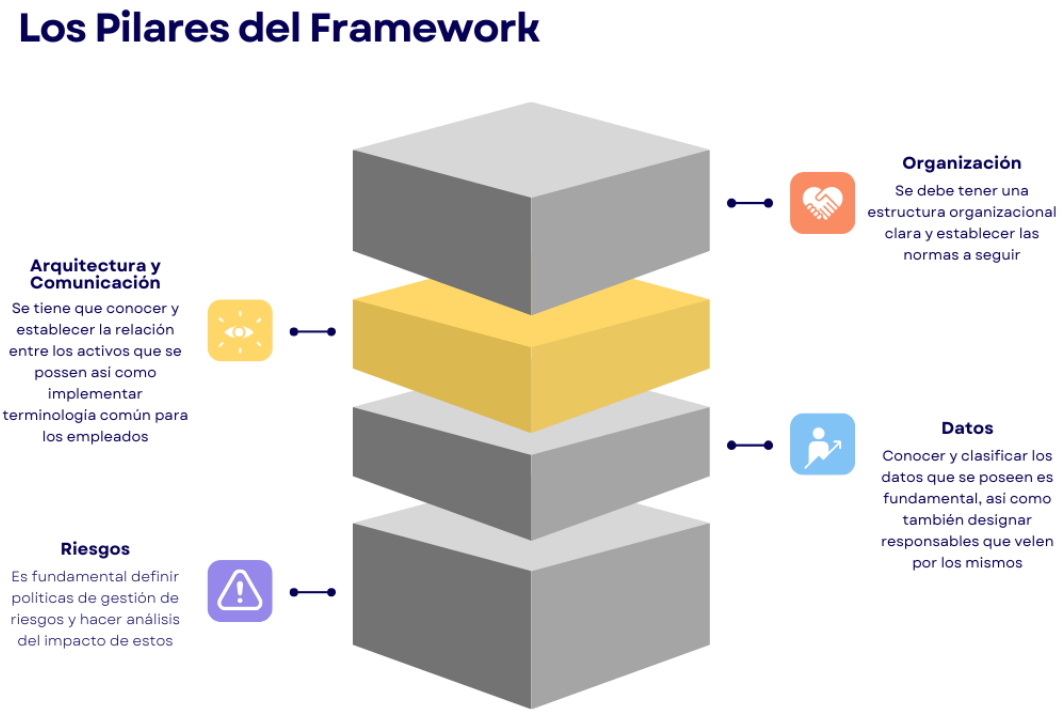
Mantener relaciones sólidas con los proveedores de tecnología y servicios es fundamental. Los sistemas SCADA e IoT dependen de hardware y software suministrados por terceros, quienes deben cumplir con los estándares de seguridad de la organización. Los acuerdos de nivel de servicio (SLA) deben incluir cláusulas de seguridad, y es esencial realizar auditorías regulares para verificar el cumplimiento. Esto permite que las prácticas de seguridad

implementadas estén alineadas con las regulaciones vigentes y las mejores prácticas de la industria.

Participar en foros (o similares) sobre seguridad permite a la organización estar al tanto de las últimas amenazas y tendencias, compartir información sobre incidentes y vulnerabilidades con otras organizaciones y grupos de interés, y contribuir a una defensa colectiva más fuerte. Una organización interna bien estructurada y relaciones colaborativas sólidas son esenciales para desarrollar ya sea políticas, procedimientos o marcos de trabajo para proteger sus infraestructuras críticas de posibles amenazas.

3.2.2. Establecer la Arquitectura de Activos y Comunicación

Figura 13



Nota. Gráfico que diseñado por mí utilizando una plantilla de Canvas para simplificar la visualización de los pilares que sostienen este framework.

La comunicación es primordial en cualquier trabajo en grupo, más aún en organizaciones con muchos empleados, gran cantidad de información y volumen de activos. Por lo que, ambas cosas se encuentran relacionadas entre sí, establecer una arquitectura de activos facilita la

comunicación de la información entre los empleados, así mismo tenemos que establecer medidas que faciliten o mejoren cada día la comunicación entre las personas, aplicando diversas técnicas, manuales y/o procedimientos a fin de poder alcanzar dicho objetivo.

Por un lado, se debe establecer un marco claro y comprensible para todos los involucrados en su gestión y operación. Es crucial definir los límites del sistema, los equipos involucrados y utilizar terminología común, así como adherirse a los estándares de ingeniería y rendimiento pertinentes. Además, en sistemas compuestos por subsistemas independientes, cada uno debe describirse en relación con los demás componentes del sistema para comprender así el rol que cumple en dicha arquitectura.

Delinear claramente los límites y los equipos incluidos abarca todos los dispositivos de control, sensores, actuadores, *interfaces hombre-máquina*[30] (IHM) y otros componentes críticos de la infraestructura en sí. Identificar y catalogar estos elementos nos permite que todos estén protegidos y gestionados de manera coherente.

Más aún si se trata de sistemas SCADA compuestos por múltiples subsistemas, allí es fundamental describir cada uno y la relación establecida. Esto incluye mapear los flujos de datos entre subsistemas, identificar puntos de integración y dependencias, y asegurar que todos los

[30] Componentes de software o hardware que permiten la interacción entre operadores humanos y sistemas automatizados, como SCADA. Facilitan el monitoreo y control de procesos industriales, pero pueden representar un vector de ataque si no se configuran y aseguran correctamente.

subsistemas estén protegidos y monitoreados adecuadamente. Una visión integral del sistema permite identificar posibles vulnerabilidades y desarrollar estrategias efectivas de mitigación.

Por ejemplo, supongamos que tenemos una empresa petrolera y que nos encargamos de distribuir combustible a todo el país, tener conocimiento de todos los equipos con los que contamos (ej. switches, routers, etc.) nos es de utilidad para mantenerlos actualizados. Podríamos armar análisis y visualizaciones para así identificar obsolescencia en equipos pasados, presentes y futuros que sean considerados activos de la organización.

Muchas veces, se compran equipos y no se les da el mantenimiento necesario, no tanto a nivel hardware, más bien a nivel software (actualizaciones). Como vimos, no tener nuestros equipos actualizados con los respectivos parches de seguridad puede ser una puerta de entrada a un posible ciberataque. En mi día a día, como *Consultora de Ciberseguridad*, me ha tocado analizar casos de tal magnitud donde los clientes no conocen qué equipos tienen, cuántas versiones y el estado de estas. Por ello, considero fundamental ser conscientes sobre la importancia del seguimiento y conocimiento de todos los equipos involucrados en su organización. Y, tener en cuenta, que más allá de que funcionen correctamente, pueden tener vulnerabilidades que sean de público conocimiento y para las cuales no se haya llevado a cabo un accionar.

Así como es crucial conocer nuestros activos, también tenemos otro punto fundamental: la terminología. La adopción de una terminología común facilita la comunicación y la comprensión entre los diferentes equipos y departamentos involucrados. Es vital definir términos técnicos, acrónimos y nomenclatura específica relevante para la operación y seguridad del sistema. Crear un glosario de términos puede ayudar a evitar malentendidos y asegurar que todos los miembros del equipo compartan una comprensión uniforme de los conceptos clave.

Volviendo a otro ejemplo, supongamos que nosotros tenemos distintos usuarios:

- Usuarios para personas que proveen servicios externos;
- Usuarios para empleados full-time internos (que, a su vez, pueden tener distintas subdivisiones en función de sus tareas);
- Y, usuarios para pasantes.

Esos tres últimos serían considerados los “usuarios nominales”. También, podríamos tener “usuarios de servicio” que sean utilizados para conectar distintos sistemas. Por otro lado se pueden catalogar usuarios de amplios privilegios (los cuales requieren un control más exhaustivo), entre otros. Pero, ¿qué se busca explicar con todo esto? Esto es un claro ejemplo de la importancia de un glosario, para poder identificar con qué tipo de usuario estoy trabajando y conocer los límites y capacidades que tiene, así como también tomar las medidas preventivas correspondientes (ej., que sea un usuario administrador). También, si tenemos la tarea de analizar

logs (o por algún motivo lo estamos corroborando) podríamos detectar anomalías al identificar usuarios cuyos accesos no son debidos.

Es importante, que la terminología sea simple y que todos la puedan comprender. En una organización de más de 800 empleados no todos se conocen. ¿Se imaginan que alguien de un servicio externo (contratado) se vea beneficiado de información que le da un empleado interno? Supongamos que utilizan una plataforma de comunicación compartida y, el empleado que se encuentra en una posición full se confunde de nombre y comenta algo que es asunto interno, eso sería grave, más allá de que no sea información altamente sensible, el hecho de que alguien externo tenga información interna con la que no debe contar es algo que no tendría que tener lugar. Si todos los empleados pueden identificar en función del tipo de ID el rol o el tipo de usuario que es, pueden tener precaución a la hora de establecer sus comunicaciones, pudiendo diferenciar entre un usuario externo (es decir, alguien de otra empresa que provee servicios o que está trabajando en un proyecto), que podría usar un ID como EXT*, y un usuario interno, que podría usar un ID como INT*.

La terminología es una de las muchas herramientas que hacen a la comunicación, sin embargo, hay más medidas que pueden emplearse. Sabemos que una organización (o empresa) suele contar con una gran cantidad de activos (piense como “activos” no solo a los equipos de hardware, sino también al software), como por ejemplo, diversas instancias: *SAP, Oracle, Active*

Directory, entre otros. Para tramitar altas, bajas y/o modificaciones de permisos en las mismas deberíamos contar con un grupo de aprobadores y delegados de las instancias, o también conocido como "propietarios". Estos se encargan de evaluar y responder por las solicitudes que llegan y velar por la protección de la triada CID en dicha instancia. En función de su tamaño, la instancia puede tener uno o más delegados (o propietarios) quienes respondan por ella, incluso, en SAP que es muy amplio, cada mandante (también se puede separar en sus objetivos: producción, testing, QA, etc.) puede tener un delegado.

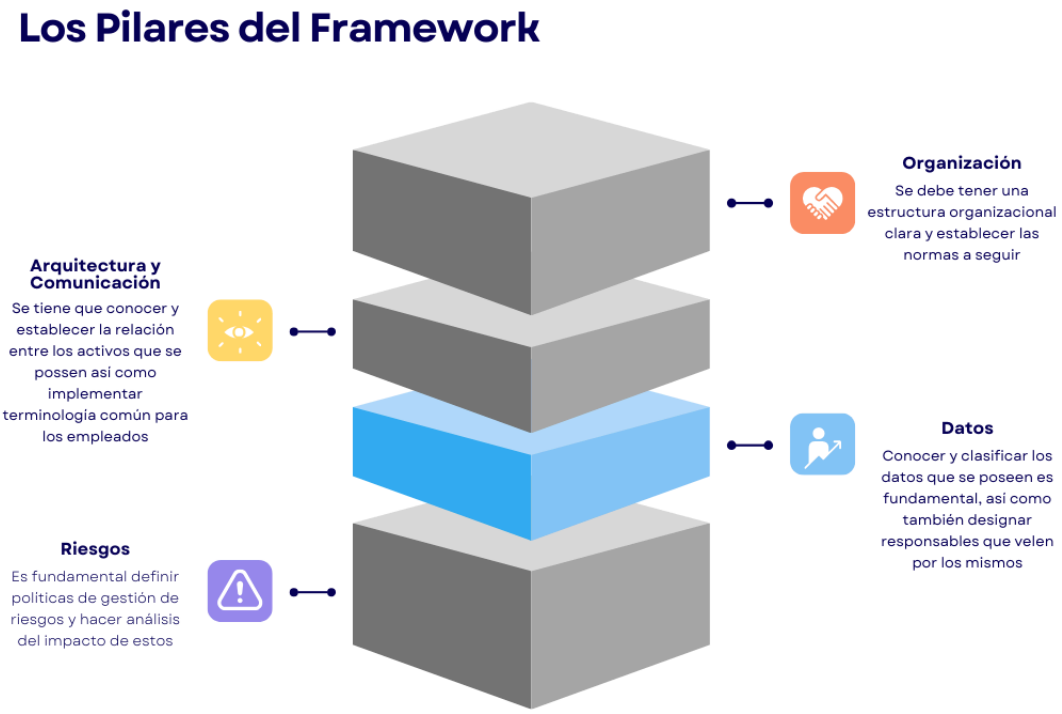
A su vez, podemos incluir estándares de ingeniería y rendimiento que proporcionan directrices y mejores prácticas a seguir para una operación segura y eficiente del sistema SCADA. Estos estándares pueden incluir normas internacionales, como las establecidas por la *IEC*[31], y normativas específicas del sector industrial relevante. La integración de estos estándares en la arquitectura de la información garantiza que se sigan prácticas reconocidas y validadas, mejorando la seguridad y la fiabilidad del sistema.

Al estructurar la información y comunicación de manera clara y detallada, se facilita la gestión segura y eficiente de estos sistemas, colaborando a que todos los componentes sean adecuadamente protegidos y que las prácticas de seguridad sean coherentes en todo el sistema, minimizando riesgos y aumentando la resiliencia ante posibles amenazas.

[31] Organización internacional que desarrolla y publica estándares globales para tecnologías eléctricas, electrónicas y relacionadas, incluidas las aplicables a la ciberseguridad y la automatización industrial, como la serie de normas *IEC 62443* para proteger sistemas de control industrial.

3.2.3. Clasificación y Gestión de la Propiedad de los Datos

Figura 14



Nota. Gráfico que diseñado por mí utilizando una plantilla de Canvas para simplificar la visualización de los pilares que sostienen este framework.

La clasificación y gestión de la propiedad de los datos es esencial para maximizar la posibilidad de tener una gestión segura y eficiente de la información. Es necesario analizar los datos contenidos, procesados, creados y utilizados por el sistema. Para facilitar este proceso, se

deben definir clases de datos que permitan identificar fácilmente los diferentes tipos de datos y sus respectivos requisitos de protección y almacenamiento. Cada categoría de datos debe tener un propietario designado, quien será la persona responsable de la gestión adecuada de estos y responderá ante cualquier manejo indebido.

La clasificación de los datos implica identificar y categorizar la información en diversas clases, cada una con sus propias necesidades de protección y almacenamiento. Los tipos de datos comunes en un sistema SCADA pueden incluir datos de configuración, históricos, en tiempo real y administrativos, entre otros. Clasificar los datos de esta manera permite aplicar políticas de seguridad específicas y adecuadas a cada tipo de información, asegurando que se mantenga su integridad, disponibilidad y confidencialidad.

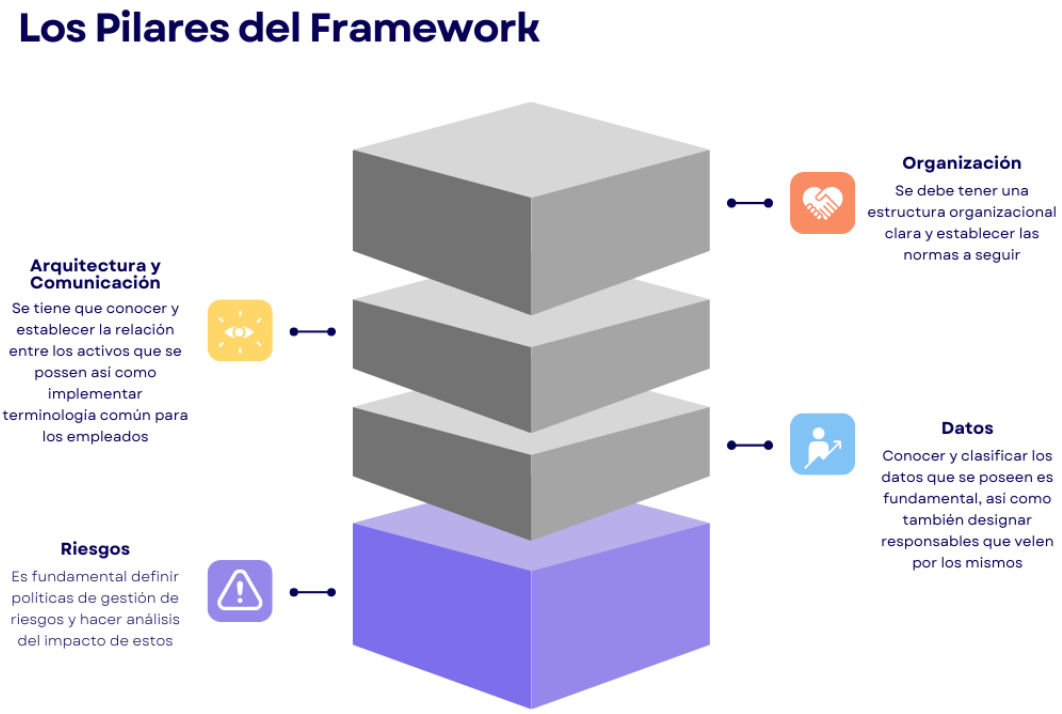
Además de la clasificación, como se mencionó más arriba, es crucial asignar la propiedad de los datos. Cada categoría de datos debe tener un propietario claramente identificado, quien será responsable de su gestión y protección. Este propietario se encargará de supervisar el cumplimiento de las políticas de seguridad, gestionar el acceso a los datos y velar a fin de que se sigan los procedimientos adecuados para el almacenamiento y protección de la información. En caso de manejo indebido de los datos, el propietario será la persona que deberá responder y tomar las medidas correctivas necesarias.

Por ejemplo, los datos de configuración, que incluyen los parámetros y ajustes del sistema SCADA, deben estar protegidos contra accesos no autorizados y alteraciones, ya que cualquier cambio no autorizado puede afectar la operatividad del sistema. Los datos históricos, que comprenden registros y archivos de eventos pasados, necesitan ser almacenados de manera segura y accesibles solo para aquellos con permisos adecuados, para mantener su integridad y utilidad en análisis futuros. Los datos en tiempo real, que son críticos para la operación diaria del sistema, requieren medidas de protección robustas para asegurar su disponibilidad continua y precisa. Los datos administrativos, que incluyen información sobre usuarios y permisos, también deben ser gestionados cuidadosamente para prevenir accesos indebidos y asegurar el cumplimiento de las políticas de seguridad.

La correcta clasificación y gestión de la propiedad de los datos no solo mejora la seguridad de la información, sino que también facilita una gestión más eficiente y ordenada. Establecer estas prácticas permite a la organización identificar rápidamente los tipos de datos y aplicar las medidas de protección adecuadas, reduciendo el riesgo de pérdida o compromiso de la información crítica. Además, tener propietarios de datos claramente definidos asegura una responsabilidad clara y una respuesta eficaz ante cualquier incidente relacionado con la gestión de datos.

3.2.4. Estrategias de Gestión de Riesgos

Figura 15



Nota. Gráfico que diseñado por mí utilizando una plantilla de Canvas para simplificar la visualización de los pilares que sostienen este framework.

Este proceso no solo es esencial para la creación de políticas de seguridad, sino que también impulsa la implementación de tecnologías y medidas de protección. El objetivo principal de cualquier programa de gestión de riesgos es alcanzar un nivel de riesgo aceptable

mediante la identificación, el análisis y la mitigación o transferencia del riesgo. Cada sistema tiene un nivel de riesgo aceptable específico, y es necesario equilibrar cuidadosamente los riesgos, los costos y el rendimiento.

El primer paso en la gestión de riesgos es la identificación de amenazas y vulnerabilidades que pueden afectar al sistema. Esto incluye tanto riesgos internos, como fallos del sistema o errores humanos, así como también riesgos externos, tales como ciberataques o desastres naturales. La identificación de riesgos implica un análisis exhaustivo de todos los posibles puntos de falla y vulnerabilidades dentro del sistema SCADA y los dispositivos IoT integrados.

Una vez identificados los riesgos, se procede a su análisis. El análisis de riesgos evalúa la probabilidad de que ocurra cada riesgo y el impacto potencial que tendría en el sistema. Esta evaluación permite priorizar los riesgos en función de su criticidad, utilizando metodologías y herramientas específicas que ayudan a determinar cuáles riesgos requieren atención inmediata y cuáles pueden ser monitorizados a largo plazo.

La siguiente fase es la mitigación o transferencia de riesgos. La mitigación implica la implementación de medidas de seguridad diseñadas para reducir la probabilidad de ocurrencia o el impacto de los riesgos identificados. Estas medidas pueden incluir controles técnicos como firewalls, sistemas de detección de intrusiones y actualizaciones de software, así como

procedimientos y políticas organizacionales, como la capacitación continua del personal y la gestión rigurosa de accesos. En ciertos casos, puede ser viable transferir el riesgo a un tercero, por ejemplo, mediante la contratación y/o externalización de funciones críticas a proveedores especializados que tengan la capacidad de gestionar mejor ciertos riesgos.

Es crucial reconocer que la gestión de riesgos no es un proceso estático, sino dinámico y continuo. Dado que los riesgos y las amenazas evolucionan constantemente, es necesario revisar y actualizar regularmente las evaluaciones de riesgos y las estrategias de mitigación. La gestión de riesgos debe integrarse en todas las fases del ciclo de vida del sistema, desde su diseño y desarrollo hasta su operación y mantenimiento, para asegurar una protección continua y adaptativa.

El equilibrio entre riesgo, costo y rendimiento es una consideración central en la gestión de riesgos. No todas las medidas de seguridad son económicamente viables o necesarias en todas las circunstancias. Por lo tanto, cada decisión debe basarse en una evaluación cuidadosa de los beneficios de la mitigación del riesgo en relación con su costo y su impacto en el rendimiento del sistema.

Implementar una gestión de riesgos eficaz permite minimizar las posibles interrupciones y daños causados por riesgos identificados. Esto proporciona una base sólida para el desarrollo de políticas de seguridad robustas y adaptativas que pueden evolucionar junto con el panorama

de amenazas en constante cambio y más aún cuando dicho sistema se encuentra conectado a Internet.

Tabla 1

Análisis y Gestión de Amenazas	
Etapas	*Tareas*
1	Identificación y Clasificación de Amenazas: Recopilar información sobre amenazas a través de registros de eventos, sistemas SIEM, y análisis de comportamiento. Categorizar amenazas en: internas (fallos de sistema, errores humanos) y externas (ciberataques, desastres naturales). Utilizar listas actualizadas de amenazas como OWASP Top 10 para guiar la clasificación
2	Evaluación de Vulnerabilidades: Realizar escaneos regulares con herramientas como *Nessus* o *Qualys*. Analizar y priorizar las vulnerabilidades usando el *Common Vulnerability Scoring System* (CVSS). Realizar pruebas de penetración para identificar puntos débiles críticos en sistemas IT, OT e IIoT
3	Clasificación y Mitigación de Amenazas: Implementar controles técnicos (firewalls, IDS/IPS) y organizacionales (políticas de acceso, capacitación del personal). Usar plataformas SOAR para automatizar respuestas a incidentes críticos. Priorizar amenazas de alto impacto y coordinar con equipos externos en caso de ataques avanzados
4	Validación y Monitoreo Continuo:

	Establecer procesos regulares de auditorías de seguridad para validar la efectividad de medidas implementadas. Monitorear amenazas emergentes con inteligencia de amenazas (*Threat Intelligence*). Automatizar alertas y respuestas en tiempo real mediante el uso de herramientas como *Splunk* o *Microsoft Sentinel*

Tabla 2

Procedimiento y Actitud Frente al Riesgo	
Etapas	*Tareas*
1	Gestión General de Riesgos: Definir un marco basado en *ISO 31000* y *NIST CSF* para identificar riesgos iniciales en IT, OT e I.IoT. Utilizar herramientas como *Splunk*, *Microsoft Sentinel* o *QRadar* para automatizar la detección de amenazas y generar informes. Contratar auditorías externas con empresas certificadas para validar la identificación de riesgos. Realizar un análisis inicial de riesgos cibernéticos relacionados con activos críticos.
2	Análisis Detallado y Mitigación: Implementar escaneos regulares con *Nessus* (IT), *Nozomi Networks* (OT) y herramientas específicas para I.IoT. Diseñar contramedidas como microsegmentación (usando soluciones como *Cisco ACI* o *Palo Alto*), políticas de acceso basadas en roles (RBAC) y despliegue de firewalls de nueva generación (NGFW). Gestionar riesgos en la cadena de suministro evaluando proveedores críticos con estándares como *ISO/IEC 27001*. Integrar controles específicos para proteger dispositivos IoT mediante autenticación y cifrado robusto.
3	Evaluación Sistemática:

	Aplicar metodologías mixtas como *STRIDE* para identificar amenazas y *CVSS* para priorizarlas según impacto y probabilidad. Desplegar simulaciones de ataques controlados (usando *Metasploit*, *Cobalt Strike*) para probar la resiliencia de los controles implementados. Incorporar frameworks como *MITRE ATT&CK* para mapear tácticas y técnicas de los adversarios. Coordinar esfuerzos con terceros especializados para cubrir brechas de seguridad.
4	Gestión Continua e Integración: Establecer un programa continuo de gestión de riesgos mediante plataformas integradas como *ServiceNow* o *RSA Archer*. Desplegar dashboards en tiempo real con *Threat Intelligence* (*ThreatConnect*, *Recorded Future*) para monitorear amenazas emergentes. Realizar ejercicios de red teaming periódicos para validar la preparación organizacional. Reforzar la resiliencia implementando copias de seguridad automatizadas y análisis post-incidente. Garantizar la alineación con la tolerancia al riesgo organizacional y cumplir con regulaciones locales e internacionales.

Una vez explicados los pilares sobre los que se asienta este framework, se procede a detallar las políticas incluídas dentro del mismo.

3.3. Política de Seguridad de Datos

Su propósito es establecer directrices claras y procedimientos detallados en búsqueda de maximizar la protección adecuada de todas las formas de datos, ya sean físicos (en papel),

digitales (almacenados en bases de datos o sistemas de archivos) o audiovisuales (imágenes o videos), entre otros, de acuerdo con su criticidad para la operación del sistema.

El enfoque de esta política se basa en la clasificación de los datos y en la adopción de controles específicos según el nivel de riesgo y la importancia del dato para la infraestructura crítica en sí. En estos tipos de sistemas, algunas categorías de datos podrían incluir: datos operativos en tiempo real, históricos, de configuración, administrativos, etc. Sin embargo, para comprender la criticidad de cada uno de estos, hagamos un análisis más profundo.

Comencemos con los datos operativos en tiempo real. Estos se consideran como información crítica para el funcionamiento y continua operación del sistema. Puede incluir, por ejemplo, datos de sensores y dispositivos IoT que monitorean y controlan procesos industriales. Estos datos requieren una alta disponibilidad y protección contra accesos no autorizados. Si pensamos en una planta de energía nuclear, los datos en tiempo real sobre la temperatura del reactor y la presión del vapor son absolutamente críticos para la operación segura de la planta. Estos datos permiten a los operadores monitorear y ajustar continuamente los parámetros del reactor para evitar condiciones peligrosas, como el sobrecalentamiento. Si personas no autorizadas acceden o alteran estos datos, podrían provocar lecturas erróneas que impidan a los operadores detectar un problema a tiempo, lo que podría llevar a fallos en el sistema de enfriamiento o incluso a un evento catastrófico.

También están los históricos que, aunque parezcan simples "rastros del pasado", esos logs y datos de producción (que si bien no afectan directamente las operaciones en curso) son fundamentales para el análisis de tendencias, auditorías y diagnósticos. Aunque pueden no requerir la misma disponibilidad que los datos en tiempo real, su confidencialidad e integridad deben protegerse ya que pueden contener información sensible que, en manos de un atacante, puedan resultar como una "herramienta" para facilitar y detectar vulnerabilidades en el sistema.

Los datos de configuración, protocolos de comunicación y ajustes operativos que determinan el comportamiento de dispositivos y redes involucradas en el sistema SCADA son cruciales. Estos datos son particularmente sensibles, debido a que su alteración podría comprometer la operación segura de la infraestructura. Yendo a un ejemplo más concreto, en un sistema de distribución de agua, la configuración del control de bombas de presión debe estar protegida a fin de evitar manipulaciones que puedan causar fallas en el suministro. Como vimos con los casos de estudio analizados (ej. *Colonial Pipeline*), las infraestructuras críticas, y más las de este tipo, tienen grandes impactos a nivel económico, social e incluso a nivel país o región.

Y, por último pero no menos importante, están aquellos datos clasificados como "administrativos". Esto implica toda aquella información relacionada con la gestión interna de la organización, como credenciales de usuarios, políticas de acceso, y reportes de mantenimiento. Estos datos, si se ven expuestos, podrían ser empleados para comprometer el sistema, por lo que

requieren controles estrictos. Por ejemplo, en el caso de una planta petroquímica, un atacante envía un correo electrónico altamente personalizado (*spear phishing*[32]) a un supervisor de IT que gestiona los accesos a los sistemas SCADA. El correo parece provenir del CEO de la empresa y solicita con urgencia que se revisen los permisos de acceso para un supuesto auditor externo que necesita revisar el sistema por una inspección de seguridad. Este incluye enlaces a un sitio web falso que imita el portal interno de la empresa. Creyendo que la solicitud es legítima, el supervisor introduce sus credenciales administrativas en el sitio. Con estas credenciales, el atacante accede a los datos administrativos, incluyendo la lista de usuarios con privilegios, políticas de acceso y permisos de control del sistema en sí. Usando estas credenciales, el atacante eleva los permisos de un usuario común a nivel de administrador, lo que le permite acceder a funciones críticas, como el control de reactores químicos y válvulas de presión. Este ataque no sólo compromete los datos administrativos, sino que otorga al atacante el poder de manipular operaciones industriales críticas, que podría desactivar o alterar sin ser detectado durante un tiempo considerable, poniendo en riesgo tanto la seguridad de la planta como la producción.

Una parte fundamental de la *Política de Seguridad de Datos* es implementar controles de acceso basados en el principio de la "necesidad de conocer". Este enfoque garantiza que solo las personas que necesitan acceder a cierta información para poder hacer su trabajo van a tener acceso a ella. En palabras más sencillas, solo van a contar con los permisos necesarios para poder

[32] Es un tipo de ataque cibernético dirigido que utiliza correos electrónicos personalizados para engañar a un individuo o grupo específico, con el fin de obtener información confidencial o instalar malware en sus sistemas.

cumplir con sus tareas y no más que esos permisos. Por ejemplo, en una planta industrial que opera con un sistema SCADA, los ingenieros de mantenimiento podrían requerir acceso a los datos de configuración del sistema, pero no a los datos financieros o administrativos.

Justamente, para estas cosas, se deben implementar diversos controles a fin de evitar que un usuario tenga más de lo que debe tener. Un ejemplo podría ser implementar un control mensual de cambios de puesto dentro de la compañía a fin de analizar si, en función de las tareas que está haciendo el usuario actualmente, requiere o no los permisos que tenía en su anterior puesto.

El control de acceso realizado debe ser gestionado a través de tecnologías como *Active Directory*[33] (más conocido como AD) o *Sistemas de Gestión de Identidades y Accesos*[34] (IAM), los cuales permiten segmentar permisos según las funciones de los empleados dentro de la organización.

[33] Servicio de directorio desarrollado por Microsoft que organiza y proporciona acceso centralizado a recursos de red, permitiendo la autenticación y autorización de usuarios, dispositivos y aplicaciones en entornos corporativos.
[34] Conjunto de tecnologías y políticas diseñadas para gestionar y proteger identidades digitales, asegurando que los usuarios adecuados tengan acceso a los recursos correctos en el momento oportuno.

Tabla 3

Gestión de la Política de Seguridad de Datos	
Etapas	*Tareas*
1	Identificación y Clasificación de Datos Sensibles: Realizar un análisis exhaustivo para identificar los distintos tipos de datos manejados en el sistema (datos operativos, datos históricos, de configuración, administrativos, etc.). Clasificar estos datos según su nivel de criticidad, integridad y disponibilidad, y establecer directrices específicas para su protección (tener en cuenta siempre las leyes y reglamentos establecidos).
2	Asignación de Propietarios de Datos y Responsabilidades: Designar responsables para cada categoría de datos, los cuales serán responsables de su custodia, acceso y uso. Definir claramente los roles y responsabilidades de los propietarios para asegurar la correcta gestión de los datos críticos y minimizar los riesgos de manejo indebido.
3	Implementación de Controles de Acceso Granulares: Definir e implementar un sistema de control de acceso basado en el principio de privilegios mínimos (*Least Privilege*) y "necesidad de conocer" (*Need-to-Know*). Utilizar sistemas avanzados de *Gestión de Identidades y Accesos* (IAM), como *Active Directory* o equivalentes, para gestionar de forma precisa los permisos de acceso, rastreando actividades de acceso en tiempo real.
4	Monitoreo y Auditoría Continua de la Seguridad de los Datos: Establecer procedimientos de monitoreo continuo para detectar accesos no autorizados o actividades sospechosas sobre datos clasificados. Implementar

	Sistemas de Gestión de Eventos de Seguridad[35] (SIEM) para la recopilación y análisis de logs de acceso y realizar auditorías periódicas (internas, operativas y externas)[36] sobre los datos críticos del sistema.
5	Cifrado y Protección de Datos en Tránsito y en Reposo: Asegurar que todos los datos críticos sean cifrados utilizando estándares de cifrado avanzados (AES-256, TLS) tanto durante su almacenamiento como durante su transmisión. Implementar mecanismos de protección contra fugas de datos (DLP) y tecnologías de control de integridad de datos para evitar manipulaciones o accesos indebidos.
6	Capacitación y Concienciación del Personal: Desarrollar programas de formación continua para asegurar que todo el personal, desde operadores hasta administradores, comprendan los procedimientos de manejo seguro de los datos. Incluir la sensibilización sobre amenazas como phishing, ingeniería social y manejo adecuado de credenciales, asegurando el cumplimiento de las políticas de seguridad.
7	Revisión y Actualización Periódica de las Políticas de Seguridad de Datos: Implementar un proceso de revisión periódico para evaluar la efectividad de las políticas de seguridad de datos en función de las nuevas amenazas, vulnerabilidades y cambios en la infraestructura. Asegurar que las políticas se mantengan alineadas con las normativas internacionales y las mejores prácticas de ciberseguridad.

[35] Son herramientas que recopilan, analizan y correlacionan datos de seguridad provenientes de diversas fuentes en tiempo real, permitiendo identificar amenazas, generar alertas y gestionar incidentes de manera eficiente.
[36] Las auditorías periódicas incluyen: internas (realizadas por la organización para evaluar controles y riesgos), operativas (centradas en la eficiencia de procesos) y externas (llevadas a cabo por terceros para verificar cumplimiento normativo).

3.3.1. Política de Respaldo de Datos

Aquí se establecen los principios y directrices técnicas necesarias para proteger la información crítica, asegurar la disponibilidad y facilitar la recuperación de datos en caso de incidentes. Esta política está diseñada para minimizar el riesgo de pérdida de datos, garantizar la integridad de los mismos y permitir la continuidad operativa en entornos de infraestructuras críticas.

Los objetivos principales son:

- Garantizar la disponibilidad de datos críticos.
- Minimizar la pérdida de datos mediante procesos de respaldo regular.
- Asegurar la integridad de los datos respaldados.
- Implementar estrategias de recuperación ante desastres para restaurar la operación normal de manera rápida y eficiente.

Por un lado, como vimos en el apartado anterior, primero tenemos que tener los datos clasificados. Y, a su vez, es esencial hacer una clasificación extra vinculada a la importancia operativa y su valor estratégico para la continuidad del negocio. Por ejemplo, los parámetros de configuración del sistema son cruciales al punto tal de que se podría afectar la operatividad del mismo, por lo que hay que hacer respaldos frecuentes. Ahora bien, los datos históricos y de

tendencias, aunque no son críticos para la operación en tiempo real, es necesario realizar respaldos periódicos para preservar la integridad de los mismos. Básicamente, la frecuencia de los respaldos estará directamente relacionada con la clasificación de los datos y los requerimientos operativos del sistema. Se proponen las siguientes estrategias de respaldo:

- Respaldos en Tiempo Real (Journaling): Este método permitirá la captura continua de cambios de datos en tiempo real. Este enfoque asegura la mínima pérdida de información en caso de una interrupción, y es recomendable para sistemas que manejan grandes volúmenes de datos sensibles.
- Respaldos Diarios y Semanales: Para datos que no requieren respaldo en tiempo real, pero que son críticos para la operación a corto y mediano plazo, se establecerán respaldos completos diarios y respaldos incrementales o diferenciales semanales. Los respaldos diferenciales pueden reducir el tiempo necesario para restaurar el sistema en caso de un fallo.
- Respaldos Mensuales/Anuales: Datos históricos, configuraciones de baja volatilidad o archivos de largo plazo se respaldan con menor frecuencia, siguiendo un cronograma mensual o anual. Este tipo de respaldo es ideal para datos de análisis histórico o informes de cumplimiento regulatorio.
- Copia de Seguridad Distribuida: Los sistemas IoT permiten la posibilidad de realizar respaldos distribuidos. En esta estrategia, los datos de los sensores y dispositivos IoT

pueden ser respaldados localmente en nodos cercanos, mientras que los datos más críticos se replican en centros de datos o en la nube. Esta estrategia mejora la disponibilidad y reduce el riesgo de pérdida de datos por fallos en la conectividad.

Una vez definida la frecuencia en función del tipo de dato, se procede con la ubicación de estas copias de seguridad. Las copias de seguridad deben almacenarse en ubicaciones seguras que estén protegidas contra posibles ataques físicos o cibernéticos. Algunas alternativas a considerar son:

- Almacenamiento Local Protegido: Es de utilidad para aquellos datos que requieren de rápido acceso, como las configuraciones del sistema SCADA o los datos operacionales en tiempo real. Estos respaldos deben almacenarse en servidores on-premise con cifrado y ubicados en centros de datos con acceso físico restringido y monitoreado. Este enfoque asegura que la organización pueda recuperar los datos de manera inmediata en caso de una interrupción operativa.
- En la Nube: Pueden emplearse en casos en los que tengamos datos que deban estar disponibles a largo plazo, como datos históricos o administrativos. Hay que elegir a proveedores que tengan altos estándares de seguridad. Otro punto a considerar es que, al estar disponibles en ubicaciones geográficas distintas, en caso de desastres naturales o

inconvenientes similares en la ubicación de la empresa, los datos van a estar disponibles. Nuevamente, el cifrado es crucial, tanto en el tránsito de los datos como cuando se alojan.

- Offline Backups: Es una estrategia eficaz para mitigar el riesgo de ransomware o malware que podría comprometer las copias conectadas a la red. Esta modalidad es ideal para datos críticos pero no urgentes, como informes periódicos o auditorías de seguridad. Al mantener estas copias desconectadas de las redes principales, se asegura una capa adicional de protección frente a posibles ataques que puedan comprometer los datos en línea.

La retención de los datos también es un punto a tener en cuenta. Cada tipo de dato tendrá un ciclo de retención específico el cual se alineará con los requisitos regulatorios y las mejores prácticas de la industria. Para ello se puede tomar las siguientes consideraciones propuestas:

- Retención de Respaldos Diarios: Por ejemplo, se pueden aplicar a datos operacionales en tiempo real, como lecturas de sensores o ajustes de control de procesos industriales. Los mismos deben ser mantenidos al menos por 30 días, cosa que nos va a permitir restaurar configuraciones recientes o recuperar información crítica en caso de fallos temporales del sistema.
- Respaldos Semanales y Mensuales: Pueden aplicarse a datos administrativos, como informes de desempeño, registros de acceso de usuarios y auditorías de seguridad. Los

mismos deben ser respaldados de forma semanal y/o mensual, siendo conservados por un período de 6 a 12 meses, dependiendo la importancia de los datos y la frecuencia de actualización de los mismos. Por ejemplo, los registros de acceso al sistema SCADA podrían necesitar una retención más prolongada para cumplir con normativas de ciberseguridad como *NIST SP 800-53*[37]. El respaldo de logs de acceso puede ser útil para la implementación de controles SOX (por ejemplo) trimestrales o semestrales a fin de que el encargado del usuario defina si esa actividad es o no correcta, hablando en este caso de usuarios administradores (no de usuarios nominales).

- Respaldos Anuales: Aquellos datos históricos, como informes de cumplimiento normativo o registro de eventos críticos, requieren un almacenamiento a largo plazo. El período de retención puede ir de 3 a 7 años, o más, según lo estipulado por las regulaciones aplicables. Por ejemplo, normas internacionales como la *ISO 27001*[38] o directivas del sector energético podrían exigir que los datos relacionados con la seguridad y la operación se conserven durante períodos extensos para auditorías o análisis futuros.
- Purgado Seguro: Al expirar el ciclo de retención de los datos es de vital importancia que los mismos sean eliminados de manera segura a fin de evitar cualquier posibilidad de recuperación no autorizada. Para ello, se deben emplear técnicas como la sobreescritura

[37] Es un estándar del NIST que define controles de seguridad y privacidad para proteger sistemas de información frente a amenazas.
[38] Es un estándar internacional para la gestión de seguridad de la información que establece requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

de datos múltiples o la destrucción física de medios de almacenamiento, siguiendo certificaciones reconocidas (como *NIST 800-88*[39]). Un ejemplo de aplicación podría ser la eliminación segura de respaldos de configuraciones de dispositivos de control al término de su ciclo de vida útil.

Hay que tener en cuenta que pueden haber excepciones y controles especiales. Es necesario definir las clases de dispositivos y datos que puedan estar exentos de los requisitos de respaldo. Estos casos deberán ser debidamente documentados y justificados basándose en su criticidad. Por nombrar un ejemplo, algunos dispositivos IoT con almacenamiento limitado pueden no requerir copias de seguridad regulares si sus datos son efímeros o de bajo impacto. Hay que saber definir qué sí y qué no es necesario backupear.

Ahora bien, ¿por qué respaldamos los datos? Las copias de seguridad no tienen sentido ni valor si no se puede restaurar debidamente cuando los datos se requieren. Por lo tanto, es esencial realizar pruebas periódicas de restauración para verificar la integridad de las copias de respaldo y la eficiencia de los procedimiento de recuperación en búsqueda de una mejora contínua. Se recomienda llevar a cabo simulacros de recuperación trimestrales o semestrales, especialmente en entornos SCADA e IoT, donde la pérdida de datos puede impactar operaciones críticas de la empresa. A su vez, esas pruebas nos van a permitir corroborar si la copia que se

[39] Es una guía del NIST que establece recomendaciones para la sanitización segura de medios de almacenamiento, asegurando la eliminación o destrucción de datos sensibles.

está llevando a cabo (que podría ser automatizada por RPA) está al día o si el robot tuvo fallas no detectadas y está levantando siempre la misma copia o, en el peor de los casos, no está siendo alguna copia de algún sistema en específico.

Tabla 4

Gestión de la Política de Respaldo de Datos	
Etapas	*Tareas*
1	Clasificación de Datos: ● Identificar y clasificar los tipos de datos (operacionales, históricos, administrativos) según su criticidad y frecuencia de cambio. ● Definir la importancia operativa y el valor estratégico de cada categoría de datos para la continuidad del negocio. ● Establecer reglas claras para la clasificación de datos críticos y no críticos.
2	Definición de Estrategias de Respaldo: ● Implementar un tipo de respaldo en función de la clasificación del dato que se desea proteger. ● Establecer ciclos de respaldo diario, semanal, mensual y anual según la importancia de los datos.
3	Ubicación y Almacenamiento Seguro: ● Almacenar respaldos locales en servidores on-premise con cifrado y ubicados en centros de datos seguros con acceso restringido. ● Replicar datos críticos a la nube mediante proveedores con altos estándares

	de seguridad, asegurando el cifrado en tránsito y reposo. ● Implementar copias de seguridad offline para datos críticos no urgentes, desconectadas de las redes principales para evitar ataques como ransomware.
4	<u>Establecimiento de Ciclos de Retención:</u> ● Definir ciclos de retención de respaldos diarios, semanales y anuales según la criticidad de los datos. ● Asegurar que los respaldos de datos históricos y regulatorios (ej. *ISO 27001*, *NIST SP 800-53*) se mantengan durante períodos de 3 a 7 años. ● Implementar procedimientos de purgado seguro al finalizar el ciclo de retención, utilizando técnicas certificadas como sobreescritura o destrucción física de medios de almacenamiento.
5	<u>Pruebas de Restauración y Mejora Continua:</u> ● Realizar pruebas trimestrales o semestrales de restauración de datos para garantizar la integridad de los respaldos y la efectividad de los procedimientos de recuperación. ● Implementar simulacros de recuperación en entornos críticos para evaluar el impacto de la pérdida de datos en la operatividad. ● Identificar posibles fallos en el proceso automatizado de respaldo (ej. fallos en robots RPA) y corregir los problemas para asegurar que las copias estén al día y sean efectivas.
6	<u>Documentación y Excepciones:</u> ● Documentar los procesos de respaldo, incluidas las clases de dispositivos y datos exentos del ciclo de respaldo, justificando la exclusión según su criticidad. ● Definir excepciones para dispositivos IoT con almacenamiento limitado y datos efímeros de bajo impacto, asegurando que las decisiones estén

	respaldadas por análisis de riesgos.

3.3.2. **Política de Almacenamiento y Destrucción de Datos**

Establece las directrices técnicas necesarias para asegurar que los datos sean almacenados de forma segura durante todo su ciclo de vida y destruidos adecuadamente al final de su utilidad. La protección de la información crítica y la garantía de que los datos no permanezcan accesibles más allá de su periodo de utilidad operativa o regulatoria es clave para la seguridad de estos sistemas.

El almacenamiento debe proteger los datos contra amenazas tanto físicas como de ciberseguridad. Por ejemplo, las configuraciones críticas de sistemas SCADA deben almacenarse en servidores locales protegidos con acceso restringido, asegurando que solo el personal autorizado tenga acceso. Otro ejemplo podría ser para el caso de los datos históricos o de cumplimiento regulatorio, como registros de auditoría, el almacenamiento en la nube ofrece ventajas, como la replicación geográfica y el cifrado en tránsito y en reposo, lo que aumenta la seguridad y disponibilidad frente a desastres.

Como ya se vió en el subtítulo anterior, tenemos diversas maneras de almacenar nuestros datos, desde local hasta en la nube y muchos más. Sin embargo, como recomendación adicional, más allá de llevar a cabo pruebas periódicas para verificar que el almacenamiento del backup

está siendo exitoso, también se puede establecer políticas de redundancia. Por medio de la replicación de los datos en varias ubicaciones geográficas, se busca protegerlos frente a desastres naturales o fallos en un solo punto de almacenamiento.

En cuanto a la destrucción de datos, es crucial garantizar que los datos se eliminen de forma definitiva cuando expire su ciclo de retención. Los datos operacionales que ya no son relevantes para la operación diaria, como registros de acceso antiguos o configuraciones obsoletas, deben eliminarse utilizando técnicas seguras y adecuadas en función del tipo y criticidad del dato que se desea proteger. Para el proceso de eliminación resulta útil apoyarse de estándares de seguridad tal como: *NIST 800-88*.

Pensemos en la eliminación segura de configuraciones obsoletas de un sistema SCADA tras una migración a una nueva plataforma. Supongamos que una planta industrial moderniza su infraestructura de control y, en el proceso, reemplaza antiguos controladores lógicos programables (PLC) con dispositivos más avanzados. Las configuraciones del sistema anterior, que contienen datos sensibles sobre protocolos de comunicación, direcciones IP y puntos de control, deben ser eliminadas mediante el uso de técnicas de sobrescritura criptográfica. Este método asegura que los datos no puedan ser recuperados ni por técnicas avanzadas de recuperación forense.

Algo importante y, la base de los procesos de las políticas de seguridad, es la clasificación de los datos que se realizó previamente. En base a ello se definirá el método de sanitización (como referencia el *NIST*) más apropiado. Por ejemplo, se puede aplicar el método de "limpieza" a aquellos dispositivos que contengan datos con sensibilidad baja. Caso contrario, se puede usar el método de "purgación" que implica sobrescritura de los datos para aquellos que tengan mayor criticidad.

El *NIST* nos propone tres métodos para poder limpiar los datos de las unidades de almacenamiento que hayamos seleccionado. Nuevamente, el método que se vaya a utilizar es en función del tipo y criticidad de datos así como también de la ubicación de la copia de seguridad.

- Limpiar (Sanitización): Proceso mediante el cual se eliminan los datos de un dispositivo de manera que no sea fácilmente accesible, aunque podría existir técnicas avanzadas para recuperarlos. Este proceso se utiliza cuando se requiere reutilizar un dispositivo o medio de almacenamiento. Por ejemplo, supongamos que un controlador SCADA se va a reasignar a otro proceso industrial. Antes de realizar esta reasignación, los datos operacionales almacenados en el dispositivo, como configuraciones y puntos de control, deben ser limpiados. Esto podría lograrse mediante una sobrescritura básica de los datos, permitiendo el uso continuo del dispositivo, pero sin eliminar completamente la posibilidad de que los datos sean recuperados por técnicas avanzadas de recuperación.

- Purgar (Borrado Seguro): Es un paso más allá de la limpieza. Implica la eliminación completa de datos de tal manera que su recuperación sea extremadamente difícil, incluso utilizando herramientas avanzadas de recuperación. Generalmente se logra mediante múltiples sobreescrituras de los datos originales con patrones aleatorios o de borrado. Imaginemos una actualización de software en los sistemas SCADA de una planta de energía. Después de dicha actualización, las configuraciones antiguas, que contenían información crítica sobre la infraestructura de control, deben ser purgadas del sistema. Esto implicaría el uso de herramientas que sobrescriben esos datos varias veces para asegurar que no puedan ser recuperados. Por ejemplo, herramientas que cumplan con estándares como el *NIST SP 800-88* pueden utilizarse para garantizar la purga efectiva de discos duros donde estaban almacenadas estas configuraciones.
- Destrucción Física o Digital: Abacar la eliminación definitiva de los datos y del medio de almacenamiento, de manera tal que no exista posibilidad de recuperación. Puede implicar la destrucción física del dispositivo de almacenamiento o el uso de métodos criptográficos. Supongamos que una empresa decide retirar un servidor obsoleto que almacenaba datos históricos críticos sobre las operaciones de una planta de agua. En lugar de simplemente formatear el disco, se opta por la destrucción física del mismo, triturando los discos duros o aplicando un método de desmagnetización (destrucción magnética) para garantizar que los datos no puedan ser recuperados por ningún medio.

Alternativamente, en medios digitales, se puede utilizar una técnica de "shredding" criptográfico, donde se eliminan las claves que permitían acceder a los datos cifrados, haciendo los mismos permanentemente inaccesibles.

Al finalizar todo proceso en el que se busque quitar información de una unidad, se deben llevar a cabo verificaciones a fin de corroborar que el objetivo fue alcanzado mediante auditorías y pruebas de muestreo. A su vez, como todo proceso auditable, se debe dejar evidencia por medio de la documentación de dicho proceso que incluya métodos empleados y su justificación, capturas con fecha y hora y la verificación de la efectividad del proceso.

Tabla 5

Gestión de la Política de Almacenamiento y Destrucción de Datos	
Etapas	*Tareas*
1	Clasificación de Datos: ● Realizar un análisis exhaustivo para clasificar los datos según su criticidad (operativos, históricos, administrativos, etc.). ● Asignar un nivel de criticidad a cada tipo de dato (alto, medio, bajo) según su valor estratégico y regulatorio.
2	Selección de Métodos de Almacenamiento: ● Definir las ubicaciones seguras para el almacenamiento (local, en la nube, offline, entre otros).

	● Determinar los requerimientos de cifrado para datos críticos en reposo y en tránsito (ej. *AES-256* para datos en servidores on-premise).
3	<u>Implementación de Redundancia:</u> ● Establecer políticas de redundancia, replicando datos críticos en varias ubicaciones geográficas (ej. copias en la nube o centros de datos secundarios). ● Realizar pruebas periódicas de replicación de datos para asegurar su disponibilidad.
4	<u>Definición de Ciclos de Retención:</u> ● Establecer los períodos de retención según la criticidad de los datos (diario, semanal, mensual o anual). ● Asegurar la retención de respaldos regulatorios (ej. auditorías) por los períodos definidos por normativas como *ISO 27001* o *NIST SP 800-53*.
5	<u>Definir Métodos de Destrucción de Datos:</u> Definir el método de destrucción según la criticidad de los datos: ● *Limpieza (Clear):* Para datos de baja sensibilidad. Se suele emplear a aquellos medios que serán reutilizados de manera interna (ej. celulares o computadoras de la empresa). ● *Purgación (Sanitización):* Se recomienda principalmente para medios que cambiarán de control o serán desechados. ● *Destrucción Física o Digital:* Aplicable a datos extremadamente sensibles, se suele indicar para aquellos casos donde la purgación no es viable. Se aplica trituración física o destrucción criptográfica (shredding). Ideal para discos duros o servidores que contienen datos operacionales o históricos de alta criticidad.

6	<u>Implementación de Procedimientos de Destrucción:</u> ● Implementar procesos de eliminación segura, como el uso de herramientas de sobrescritura criptográfica para medios reutilizables. ● Establecer procedimientos de destrucción física para discos duros o medios obsoletos que contienen datos críticos (trituración, desmagnetización). ● Aplicar procesos de eliminación de claves criptográficas en dispositivos cifrados que no requieran destrucción física.
7	<u>Monitoreo de Ciclos de Retención y Destrucción:</u> ● Monitorear el cumplimiento de los ciclos de retención de los datos, garantizando que los datos se eliminen al finalizar su período de retención. ● Automatizar alertas para el proceso de destrucción de datos al cumplirse su ciclo de vida útil.
8	<u>Pruebas de Eficiencia de Almacenamiento y Destrucción:</u> ● Realizar auditorías periódicas para asegurar que los datos críticos están correctamente almacenados y destruidos al finalizar su ciclo de vida. ● Verificar que los procedimientos de destrucción, como la sobrescritura múltiple o destrucción física, sean efectivos y cumplan con las normativas aplicables. ● Realizar pruebas de muestreo tras las destrucciones para confirmar que los datos no son recuperables.
9	<u>Documentación de Procesos y Excepciones:</u> ● Documentar todos los procesos de almacenamiento y destrucción de datos, incluyendo los métodos utilizados y las justificaciones para los casos excepcionales (ej. dispositivos IoT con almacenamiento limitado). ● Mantener registros detallados de todas las operaciones de purgado y

	destrucción de datos, incluyendo capturas con fecha y hora, y resultados de las auditorías de verificación de eliminación.
10	Capacitación y Actualización Continua: ● Desarrollar programas de capacitación para el personal responsable del almacenamiento y destrucción de datos, asegurando que conozcan los procedimientos y normativas aplicables. ● Revisar y actualizar periódicamente la política de almacenamiento y destrucción de datos en función de nuevas normativas o cambios en la infraestructura tecnológica.

3.3.3. Política de Protección contra Software Malicioso

Debido a la alta interconectividad y al uso de dispositivos IoT en estas infraestructuras, el riesgo de infecciones por malware ha aumentado significativamente. Esta política establece las directrices para prevenir, detectar y mitigar la instalación de código malicioso que pueda comprometer la integridad, confidencialidad y disponibilidad de los datos operativos.

Una de las primeras medidas a tomar es implementar el uso de soluciones antimalware. Ahora bien, más allá de que se pueden llevar a cabo análisis en tiempo real, definir y programar escaneos, así como documentar el procedimiento y resultado obtenido, es fundamental. Un ejemplo de esto es la implementación de agentes de seguridad en los PLCs para asegurar que cualquier modificación sospechosa de los parámetros sea detectada y bloqueada automáticamente antes de que afecte los procesos industriales.

La actualización continua de software y parches de seguridad es otro pilar fundamental. Las vulnerabilidades en sistemas operativos y aplicaciones son uno de los vectores de ataque más comunes para la distribución de malware. Por ejemplo, en una red de distribución eléctrica controlada por sistemas SCADA, la falta de parches en sistemas operativos obsoletos podría abrir una puerta de entrada para ataques de ransomware, como ocurrió en el caso de *Oldsmar Water Treatment Plant (2021)*. Establecer un ciclo regular de actualizaciones y revisar los parches de seguridad críticos de manera prioritaria es esencial para reducir la exposición a malware.

En este contexto, el uso de tecnologías OTA[40] (Over-the-Air) juega un rol crucial, ya que permite la distribución remota y automatizada de actualizaciones de software y firmware sin intervención física. Los sistemas SCADA y dispositivos IoT pueden recibir actualizaciones de seguridad críticas y nuevas configuraciones de forma inalámbrica, reduciendo así el tiempo de exposición a vulnerabilidades conocidas y minimizando el riesgo operativo.

Para mitigar la descarga e instalación de software no autorizado, es crucial implementar políticas de *listas blancas*[41] (whitelisting) que limiten las aplicaciones que pueden ejecutarse en los dispositivos. Solo el software autorizado, previamente evaluado y aprobado, puede instalarse

[40] Las tecnologías OTA (Over-the-Air) permiten la actualización, configuración o gestión remota de dispositivos a través de redes inalámbricas, sin intervención física.
[41] Son conjuntos predefinidos de aplicaciones, direcciones IP o usuarios permitidos para acceder a sistemas o recursos, utilizadas como medida de seguridad para restringir el acceso no autorizado.

en los sistemas críticos. Se puede optar por generar una especie de "tienda" con el software autorizado por la empresa y prohibir de manera automatizada la instalación de archivos ejecutables. En caso de que el usuario requiera instalar algún software que no esté listado por la empresa deberá comunicarlo para que el equipo de seguridad evalúe los posibles riesgos e impactos de ello. A su vez, el usuario junto con su supervisor deberán armar la correspondiente justificación a presentar y a ser analizada por los directivos del área quienes conocen a nivel funcional si es realmente necesaria dicha herramienta para llevar a cabo las tareas necesarias y pasar por una serie de aprobaciones previo a dar el permiso para la instalación. Esto va a variar en función de la organización, pero mínimo siempre tendría que tener el “okay” del responsable del usuario, a fin de justificar la necesidad (funcional), y del equipo de seguridad específico que se encarga de hacer los controles del software instalado en los equipos del personal de la empresa, quienes harán el análisis desde el punto de vista técnico de la herramienta en sí.

Los controles y escaneos de los dispositivos empresariales así como la implementación de programas desinstaladores es de gran utilidad a fin de evitar y detectar cualquier programa que no se alinee con la lista de software publicada por parte de la empresa. Es crucial que esta lista sea de fácil acceso para todos los niveles de la organización y que cada empleado firme conformidad y confirmación de lectura, declarando comprender y estar consciente del impacto de su accionar.

La segmentación de redes debe aplicarse de manera estricta para reducir la superficie de ataque. En un entorno industrial, los sistemas SCADA deben estar aislados de las redes corporativas y de internet mediante firewalls y redes segmentadas. Por ejemplo, la creación de una DMZ entre la red SCADA y la red de TI a fin de que cualquier intento de intrusión desde la red corporativa no llegue a comprometer el sistema de control operativo.

Ahora bien, en caso de que en alguno de esos escaneos se logre detectar software malicioso, la política establece un protocolo de respuesta a incidentes, el cual debe ser activado inmediatamente. Este protocolo incluye la contención del malware, la eliminación del código malicioso y la recuperación segura del sistema. Un caso de aplicación sería la detección de un troyano en una subestación eléctrica conectada a un sistema SCADA. El equipo de seguridad debería aislar el sistema afectado, iniciar el análisis forense para identificar el origen de la amenaza y luego restaurar el sistema desde una copia de seguridad limpia.

La cuarentena automatizada de archivos sospechosos es una medida clave para la contención de amenazas. Los sistemas deben ser configurados para identificar y colocar en cuarentena cualquier archivo o proceso sospechoso hasta que se pueda realizar una evaluación completa. Por ejemplo, si se detecta una posible modificación en un archivo de configuración de un PLC, este debe ser automáticamente puesto en cuarentena y evaluado antes de permitir su reintroducción en el sistema.

Es debido a ello que se vuelve a resaltar la importancia del monitoreo constante de eventos de seguridad. Esto se puede lograr a través de sistemas de detección y prevención de intrusiones (IDS/IPS) que tiene como objetivo la identificación temprana de patrones anómalos o intentos de instalación de malware. En un entorno de control industrial, la implementación de un sistema SIEM permite correlacionar eventos en tiempo real para identificar posibles amenazas antes de que comprometan la operación. Por ejemplo, un aumento en el tráfico de red no habitual podría ser una señal de que un ataque está en progreso, lo que desencadenaría una respuesta inmediata.

Anteriormente se habló de informar al usuario respecto a las políticas de instalación de software externo. En seguridad informática la mayor parte del trabajo recae en el usuario por lo que llevar a cabo periódicamente campañas de capacitación y concienciación es una medida muy útil. Pueden ir desde campañas generales a específicas. Un ejemplo práctico de esto sería la capacitación en el reconocimiento de correos electrónicos sospechosos, en los que un atacante intenta hacerse pasar por un proveedor legítimo para instalar un malware.

Tabla 6

Gestión de la Política de Protección de Software Malicioso	
Etapas	*Tareas*
1	Implementación de Soluciones Antimalware: ● Instalar y configurar soluciones antimalware en todos los dispositivos críticos, incluidos los sistemas SCADA y dispositivos IoT ● Definir y programar escaneos automáticos y en tiempo real en servidores, PLCs y estaciones de trabajo ● Documentar los procedimientos y resultados de cada escaneo para seguimiento y auditoría
2	Actualización de Software y Parches: ● Establecer un ciclo regular de actualizaciones para todos los sistemas, aplicaciones y dispositivos conectados a la red ● Priorizar la instalación de parches críticos que cierren vulnerabilidades de seguridad en sistemas operativos ● Documentar los parches aplicados y verificar su implementación mediante auditorías regulares
3	Implementación de Políticas de Whitelisting: ● Crear una lista blanca (whitelist) de aplicaciones autorizadas para ejecutarse en los sistemas críticos. ● Implementar controles que restrinjan la instalación de software no autorizado. ● Establecer un proceso para solicitar la evaluación y autorización de software nuevo, involucrando al equipo de seguridad y al supervisor del área.
4	Segmentación de Redes y Firewalls: ● Segmentar las redes industriales SCADA de las redes corporativas y del

	acceso a internet. ● Configurar firewalls y DMZs para proteger los sistemas críticos y limitar la comunicación entre las diferentes redes. ● Monitorear las conexiones entrantes y salientes para detectar intentos no autorizados de acceso.
5	<u>Monitoreo y Detección de Intrusiones:</u> ● Implementar sistemas de detección y prevención de intrusiones (IDS/IPS) en la red para identificar actividades sospechosas. ● Integrar un sistema SIEM para correlacionar eventos de seguridad en tiempo real y generar alertas automáticas. ● Monitorizar el tráfico de red anómalo que pueda indicar un ataque o instalación de malware.
6	<u>Protocolo de Respuesta a Incidentes:</u> ● Desarrollar un protocolo de respuesta a incidentes, detallando las acciones a seguir ante la detección de malware. ● Aislar y contener sistemas comprometidos para evitar la propagación del malware. ● Realizar análisis forense para identificar el origen del ataque y aplicar medidas correctivas. ● Restaurar el sistema desde copias de seguridad limpias si es necesario.
7	<u>Cuarentena y Evaluación de Archivos Sospechosos:</u> ● Configurar sistemas para que cualquier archivo o proceso sospechoso sea automáticamente puesto en cuarentena. ● Establecer procedimientos para la evaluación forense de archivos en cuarentena, asegurando que sean revisados antes de reintroducirlos en el sistema. ● Documentar el análisis y las decisiones tomadas sobre los archivos evaluados.
8	<u>Capacitación y Concienciación del Personal:</u> ● Desarrollar programas de capacitación regulares sobre el reconocimiento

	de correos de phishing y amenazas de malware para todo el personal. ● Realizar talleres específicos sobre el uso seguro de dispositivos críticos (SCADA, PLC, IoT) y cómo evitar la instalación de software no autorizado. ● Mantener una campaña de concienciación continua sobre las amenazas cibernéticas.
9	Auditorías y Verificación de Procesos: ● Realizar auditorías periódicas de los sistemas de seguridad para verificar la correcta implementación de las políticas antimalware. ● Llevar a cabo pruebas de muestreo en dispositivos críticos para asegurar que no se haya instalado software no autorizado. ● Documentar los hallazgos de las auditorías y las acciones correctivas tomadas, si es necesario.

3.4. Política de Seguridad de la Plataforma

Dicha política tiene como objetivo establecer las configuraciones predeterminadas seguras para todos los componentes dentro del sistema SCADA, asegurando que los dispositivos críticos, como servidores, clientes y equipos SCADA (RTU/PLC/IED), funcionen bajo directrices específicas que garanticen su protección frente a amenazas de seguridad.

Cada dispositivo tendrá un conjunto de reglas independientes que definirán qué configuraciones se requieren a fin de asegurar su correcto funcionamiento. Por ejemplo, los PLCs deben tener configuraciones específicas de acceso restringido, mientras que los servidores deben cumplir con requisitos más avanzados, como cifrado en reposo y en tránsito. Un PLC

utilizado en una planta industrial, debe tener configuraciones de firewall y control de acceso que solo permitan conexiones desde dispositivos autorizados. Del mismo modo, los servidores SCADA deben implementar políticas de contraseñas robustas y autenticación multifactor (MFA).

Se deben realizar controles de acceso. Yendo a un ejemplo en concreto, uno de los muchos controles que se puede hacer es el control por cambio de puesto dentro de la compañía u, otro aparte, el control por desafección directa (es decir, cuando el empleado se encuentra deshabilitado y ya no forma parte de la empresa). En ambos casos, es fundamental controlar qué usuarios tienen acceso a cuáles plataformas y bajo qué permisos. Por ejemplo, si un operador es dado de baja de la organización, es necesario que su cuenta sea desactivada de inmediato en todos los sistemas SCADA para prevenir cualquier uso indebido.

Otro control a llevar a cabo, más allá de los usuarios nominales y/o de servicio, es para los usuarios administradores. La cantidad de cuentas de este tipo debe ser limitada, se deben controlar sus permisos y el registro de actividad de los mismos debe ser supervisada y aprobada por un usuario que tenga dicha cuenta a cargo.

Además, esta política aborda conceptos clave como el control de acceso, la verificación de virus, y la detección y prevención de intrusiones. Es esencial que cada dispositivo sea configurado para realizar escaneos periódicos de virus y malware, asegurando que los sistemas no sean vulnerables a infecciones que puedan comprometer la operación del sistema. Un ejemplo

de implementación sería la integración de software antivirus en los servidores de gestión SCADA y los RTUs, los cuales deben realizar escaneos regulares para detectar posibles amenazas.

La encriptación es otro aspecto esencial de la política. Tanto los datos en reposo como en tránsito deben ser cifrados utilizando estándares robustos como AES-256 o TLS, asegurando que cualquier transmisión de datos entre servidores SCADA y dispositivos de campo esté protegida frente a interceptaciones.

Ahora bien, siempre hay excepciones. Por ende, al implementar y adaptar dicha política al entorno industrial y la compañía a la que se le desee aplicar, se debe tener en cuenta que, debido a las capacidades variables de cada plataforma puede que no siempre se pueda configurar de la manera que se propuso. En estos casos, se debe establecer un proceso formal para solicitar excepciones, y dichas excepciones deben ser aprobadas solo después de un análisis exhaustivo de los riesgos y posibles medidas de mitigación. A su vez, toda excepción debe tener un periodo de tiempo (ej. de 6 meses) a fin de solventarlo, en caso de que no sea posible, se convertirá en un registro de riesgo con la respectiva evidencia y justificación de por qué no se pudo solventar en ese tiempo.

Tabla 7

Gestión de la Política de Seguridad de Plataforma	
Etapas	*Tareas*
1	Clasificación de Dispositivos y Sistemas: ● Identificar y clasificar todos los dispositivos SCADA (RTU, PLC, IED), servidores y clientes conectados. ● Asignar niveles de criticidad según la función de cada dispositivo (alto, medio, bajo) en la infraestructura crítica.
2	Definición de Configuraciones Predeterminadas Seguras: ● Establecer configuraciones seguras para cada tipo de dispositivo. ● Implementar políticas de contraseñas robustas y autenticación multifactor (MFA) para servidores SCADA. ● Definir configuraciones específicas de firewall y acceso restringido para PLCs y otros dispositivos de campo.
3	Control de Acceso para Usuarios Nominales y de Servicio: ● Implementar controles de acceso basados en los privilegios mínimos y la "necesidad de conocer". ● Establecer procedimientos para la creación y terminación de cuentas de usuarios nominales y de servicio. ● Controlar cuentas administrativas, limitando la cantidad de usuarios con estos privilegios.
4	Monitoreo de Actividades de Cuentas de Administradores: ● Registrar y monitorear la actividad de los usuarios administradores en sistemas SCADA. ● Establecer un proceso de supervisión y aprobación de actividades críticas por parte de un administrador responsable.

5	Escaneos y Verificación de Seguridad: ● Implementar escaneos automáticos de virus y malware en servidores SCADA y dispositivos como RTU/PLC. ● Establecer la detección de intrusiones (IDS/IPS) para monitorear actividades sospechosas en las redes SCADA.
6	Encriptación de Datos en Reposo y en Tránsito: ● Asegurar que todos los datos en reposo y en tránsito estén cifrados con estándares de cifrado avanzados (AES-256, TLS). ● Verificar el correcto uso de la encriptación en las comunicaciones entre servidores SCADA y dispositivos de campo.
7	Proceso de Revisión de Usuarios y Acceso: ● Realizar revisiones periódicas de los usuarios con acceso a los sistemas SCADA, eliminando permisos innecesarios, especialmente en casos de cambios de puesto o desafección del empleado. ● Desactivar inmediatamente las cuentas de usuarios nominales al finalizar su relación con la organización.
8	Solicitudes de Excepciones y Análisis de Riesgo: ● Establecer un proceso formal para gestionar solicitudes de excepción cuando las configuraciones propuestas no sean factibles. ● Luego del periodo establecido y, en caso de no haberse solventado, toda excepción se convertirá en un registro de riesgo.1q2 ● Realizar un análisis de riesgos exhaustivo para evaluar el impacto de no cumplir con las configuraciones de seguridad.
9	Capacitación y Concienciación de Personal: ● Implementar programas de capacitación para garantizar que el personal entienda las configuraciones de seguridad de la plataforma. ● Capacitar a los operadores en la identificación de amenazas y en el uso adecuado de los sistemas SCADA bajo configuraciones seguras.

10	Auditorías y Revisión de Políticas: ● Realizar auditorías regulares para verificar el cumplimiento de las políticas de seguridad de la plataforma. ● Actualizar las configuraciones de seguridad en función de nuevos riesgos, vulnerabilidades y avances tecnológicos.

3.4.1. Control de Acceso

En redes SCADA, donde los protocolos de comunicación industrial como Modbus y DNP3 están ampliamente implementados, los riesgos asociados a la falta de seguridad intrínseca son evidentes. Por ejemplo, Modbus, que permite la comunicación entre millones de dispositivos de automatización, carece de mecanismos básicos de seguridad como la autenticación o cifrado. Esto lo deja vulnerable a ataques como Man-in-the-Middle (MITM), eavesdropping y replay. La implementación de TLS (Transport Layer Security), como se ha propuesto en versiones mejoradas de Modbus, junto con un modelo de Acceso Basado en Roles (RBAC), es clave para mejorar la seguridad de las comunicaciones y autorizar tanto a los clientes en el servidor como las tramas Modbus en tránsito.

El RBAC es un enfoque eficiente para limitar el acceso a los sistemas SCADA, asegurando que cada usuario solo tenga los permisos estrictamente necesarios para realizar sus funciones. Este modelo organiza a los usuarios en roles según sus responsabilidades. En este contexto, RBAC es especialmente útil para proteger dispositivos sensibles como PLC

(Controladores Lógicos Programables) y RTU (Unidades Terminales Remotas), que controlan procesos industriales clave. Por ejemplo, un PLC que gestiona operaciones de una planta petroquímica debe tener sus configuraciones y parámetros accesibles únicamente por administradores con permisos específicos. Los permisos de estos usuarios deben ser monitoreados continuamente y revisados periódicamente para evitar ampliaciones innecesarias de sus capacidades operativas.

En el artículo *"A Role-Based Access Control Model in Modbus SCADA Systems. A Centralized Model Approach"*, se diseñó una arquitectura centralizada que incluye cinco subsistemas principales: el cliente, el manejador de MBAPS, el manejador de MBAP, el módulo de control de acceso (AC) y la base de datos de roles. Cada uno de estos componentes interactúan para garantizar que solo los usuarios autorizados puedan acceder a las funciones críticas del sistema SCADA.

El proceso se puede dividir en dos fases. En el primero, durante el establecimiento de la sesión TLS, el servidor autentica al cliente mediante el uso del certificado digital X.509v3. Este proceso asegura que solo las entidades con certificados válidos puedan iniciar una comunicación segura. Una vez autenticado, el manejador de MBAPS envía la información de rol del cliente al módulo de control de acceso. Este módulo consulta la base de datos de roles y ejecuta las políticas de autorización para verificar si el cliente tiene los permisos necesarios. Por ejemplo, si

un operador de planta intenta acceder a los parámetros críticos de un PLC, el sistema verifica que el rol "operador" esté autorizado a modificar dichas configuraciones. Si el rol está autorizado, la conexión continúa; de lo contrario, el sistema cierra la conexión.

En la siguiente fase, una vez establecida la sesión TLS y autorizado el cliente, las tramas Modbus pueden intercambiarse de forma segura. Cada trama contiene un unit_id, que es un identificador único utilizado para autorizar la trama. El manejador de MBAP extrae el unit_id de la trama y lo envía al módulo de control de acceso para validarlo contra la base de datos de roles. Solo las tramas que estén asociadas con un unit_id autorizado pueden ser procesadas y ejecutadas. Por ejemplo, si un sistema SCADA envía una trama Modbus para cambiar el estado de una válvula en una planta de tratamiento de agua, el unit_id de la trama debe coincidir con un dispositivo autorizado en la base de datos de roles. Si la autorización es exitosa, el manejador de MBAP procesará la trama y ejecutará la acción solicitada.

RBAC es un ejemplo de los muchos tipos de control los cuales deben ser elegidos en base a un análisis exhaustivo del funcionamiento de nuestro sistema. Otros tipos de control de acceso incluyen:

- Lista de Control de Acceso (ACL): Define permisos explícitos para usuarios o grupos en un recurso en concreto. Por ejemplo, en una red SCADA, un ACL puede permitir que solo los administradores accedan a

los servidores de control, mientras que los operadores sólo pueden acceder a las interfaces de usuario. Cada dispositivo tiene una lista detallada que define quién puede leer, escribir o ejecutar ciertas acciones.

- Control de Acceso Basado en Atributos (ABAC): Otorga acceso según atributos del usuario, recursos, o entorno. Por ejemplo, un técnico que trabaje de noche (atributo de tiempo) solo puede acceder a los sistemas SCADA si está dentro de su turno autorizado. O bien, un usuario puede acceder a un PLC únicamente si está en la ubicación geográfica asignada (atributo de ubicación).
- Control de Acceso Basado en Directivas (PBAC): Aplica reglas predeterminadas para conceder acceso basado en políticas definidas. Por ejemplo, una política puede especificar que solo los administradores con MFA habilitado pueden realizar cambios en los sistemas de control de una planta de energía.

Ahora bien, más allá de los diversos métodos de control de acceso existentes (autorización), también es importante contar con métodos de autenticación. La opción más común es el uso de contraseñas, sin embargo, un paso extra es optar por MFA. Esta es una capa adicional de verificación más allá de las contraseñas tradicionales, como códigos generados por aplicaciones (ej. Microsoft Authenticator) o autenticación biométrica. La implementación de

MFA es particularmente importante en casos de acceso remoto, como cuando un técnico necesita acceder a una subestación eléctrica desde una ubicación externa. Para asegurar que este acceso esté completamente protegido, el sistema requerirá múltiples factores de autenticación para verificar la identidad del usuario.

Sin embargo, más allá de las medidas que se puedan tomar, es igual de importante realizar monitoreos en los accesos para validar que las medidas tomadas son eficientes o, caso contrario, reforzar y mejorar el proceso definido. Todos los accesos deben ser registrados y auditados, especialmente aquellos realizados por usuarios con privilegios elevados, como los administradores. Las auditorías regulares permiten detectar cambios no autorizados en los sistemas y son necesarias para cumplir con normativas como NIST SP 800-53 e ISO 27001. Por ejemplo, en una planta de producción de químicos, se deben registrar todas las actividades relacionadas con los sistemas de control de temperatura y presión. Si se detecta acceso fuera de horas laborales o desde ubicaciones no autorizadas, el sistema de monitoreo debe activar alertas automáticas para el equipo de seguridad.

Por último, pero no menos importante, volvemos a resaltar la importancia de la implementación de un control de cuentas de usuario, ya sea por cambio de puesto dentro de la compañía como por separación de la misma. Y, remarcar que lo ideal no es bloquear al usuario en las instancias a las que se encuentre asociado, sino removerle todos los permisos también.

Esto a fin de que si el usuario solicita desbloquear su ID, no termine teniendo nuevamente más roles de los que debería tener, esto sería un ejemplo para el RBAC.

Tabla 8

Gestión de la Política de Control de Acceso	
Etapas	*Tareas*
1	Clasificación y Asignación de Roles: ● Realizar un análisis exhaustivo para identificar y clasificar usuarios en roles específicos según sus responsabilidades (operador, técnico, administrador). ● Asignar permisos mínimos necesarios para cada rol.
3	Autenticación y Autorización: ● Definir el método de autenticación (ej. MFA) y autorización a utilizar en función de las características del sistema empleado. Por ejemplo, si el protocolo de comunicación es Modbus, tender a la opción RBAC.
5	Monitoreo y Auditoría de Accesos: ● Registrar todas las actividades de acceso, especialmente las realizadas por administradores. ● Realizar auditorías periódicas para detectar accesos no autorizados y asegurar cumplimiento con normativas.
6	Desactivación de Cuentas y Revocación de Permisos:

	● Desactivar y eliminar los permisos de usuarios que cambien de puesto o que abandonen la organización. ● Implementar políticas de desactivación automatizada para accesos temporales o usuarios de servicio.

3.5. Política de Seguridad de Comunicaciones

La política de seguridad de comunicaciones establece un marco regulador para la representación y el intercambio de datos a través de los enlaces de comunicación, enfocándose en la protección y estandarización de los protocolos que intervienen en las interacciones entre las MTU[42] (Master Terminal Units) y las RTU[43] (Remote Terminal Units). Los primeros sistemas SCADA usaban comunicaciones remotas mediante conexiones locales *RS232*[44] o interfaces de módem de acceso telefónico, limitados y sin la capacidad de soportar la escalabilidad requerida por aplicaciones industriales cada vez más complejas. Con el tiempo, estas limitaciones impulsaron el desarrollo de protocolos avanzados que permiten mayor flexibilidad y alcance en las comunicaciones **[12]**.

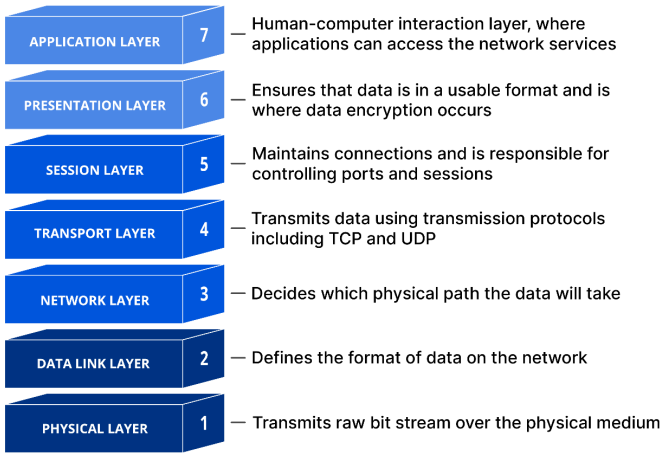
Dado que un sistema SCADA incluye numerosos componentes de diferentes proveedores, cada uno con protocolos específicos, la interoperabilidad se convierte en un

[42] Son unidades centrales que supervisan y controlan sistemas SCADA, enviando comandos y recibiendo datos de campo.
[43] Son dispositivos remotos que recopilan datos de sensores y ejecutan comandos enviados por las MTU.
[44] Es un estándar de comunicación serial utilizado para la transmisión de datos entre dispositivos, común en equipos industriales, sistemas embebidos y conexiones de hardware como computadoras y periféricos.

desafío. Los protocolos propietarios de cada fabricante suelen diferir en sus reglas y procedimientos de comunicación, afectando aspectos como la presentación y conversión de datos, la asignación de direcciones, la generación de comandos y la información de estado. Esta diversidad hace imperativa la adopción de estándares abiertos que faciliten la integración de dispositivos y minimicen la dependencia de los proveedores.

Para promover la adopción de protocolos abiertos, se introdujo el modelo de *Interconexión de Sistemas Abiertos* (OSI) en 1984. Este modelo descompone el proceso de comunicación en siete capas independientes, cada una describiendo cómo se manejan los datos en diferentes etapas de transmisión. La estructura de capas del modelo OSI es esencial para garantizar que los protocolos sean ampliamente compatibles, ofreciendo una mayor disponibilidad e interoperabilidad de los dispositivos, disminuyendo la dependencia de tecnologías propietarias y optimizando los costos y la asistencia técnica.

Figura 16



Nota. Capas del Modelo OSI. Tomado de *¿Qué es el modelo OSI?*, (s.f.), Cloudflare.

Esta política clasifica los protocolos de comunicación en dos categorías principales: cableada e inalámbrica. La comunicación cableada (o "wireline") se refiere a la transmisión de datos mediante tecnologías cableadas, como los cables *Ethernet*, que proporcionan una conexión robusta y segura, ideal para entornos industriales. Por otro lado, la comunicación inalámbrica no depende de cables físicos, sino que utiliza tecnologías de radiofrecuencia, como ondas de radio, para transmitir datos. Algo a destacar es que los protocolos inalámbricos, cada vez son más relevantes en entornos SCADA ya que facilitan la movilidad y la flexibilidad en la arquitectura de red, especialmente en áreas de difícil acceso para instalaciones cableadas.

Es fundamental comprender cómo funciona y cuáles son los componentes de la arquitectura de comunicación de un sistema como este. La interfaz de usuario, como ya hemos hablado, es el HMI (o IHM) que permite visualizar los datos y monitorear. Por otro lado, en lo que respecta al hardware, esta arquitectura se compone principalmente de las MTU, que desempeñan un rol crucial al servir como el centro de procesamiento y toma de decisiones, mientras que las RTU, PLC, o *Dispositivos Inteligentes de Extremo*[45] (IED) interactúan directamente con el entorno físico. Estas unidades están conectadas mediante una red troncal que combina medios cableados e inalámbricos, lo que permite la recolección de datos y el control de procesos en tiempo real. Por otro lado, la inclusión de tecnologías IoT en la arquitectura otorga una mayor flexibilidad y escalabilidad al incorporar dispositivos que utilizan el protocolo *6LoWPAN*[46] para conectarse a redes *IPv6*[47], lo que facilita el intercambio de información entre dispositivos IoT y los sistemas SCADA **[19]**.

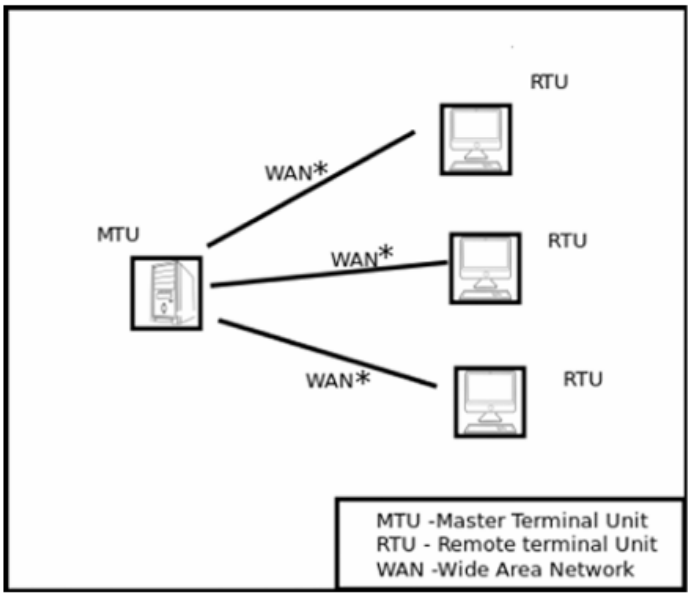
Las arquitecturas SCADA han evolucionado a través de diversas etapas. En los años 70, los sistemas SCADA monolíticos operaban en entornos completamente aislados, sin conectividad con otros sistemas. Su diseño estaba orientado a funcionar de manera independiente, utilizando minicomputadoras grandes para el procesamiento de datos. Un ejemplo

[45] Son equipos electrónicos utilizados en sistemas industriales para recopilar datos, realizar análisis locales y ejecutar acciones automatizadas, comúnmente empleados en redes eléctricas inteligentes y sistemas SCADA.
[46] Es un protocolo que permite la transmisión de datos IPv6 en redes inalámbricas de baja potencia, optimizado para dispositivos IoT en entornos con recursos limitados.
[47] Es la última versión del Protocolo de Internet, diseñada para ampliar el espacio de direcciones, mejorar la eficiencia del enrutamiento y proporcionar soporte avanzado para la conectividad de dispositivos en redes modernas e IoT.

notable de estos sistemas de primera generación es la serie *PDP-11*, desarrollada por *Digital Equipment Corporation*. En esta arquitectura, las MTU estaban conectadas a las RTU a través de redes WAN. Sin embargo, los protocolos de WAN de esa época eran diferentes de los actuales, en una etapa preliminar y de naturaleza propietaria. Estos protocolos solo permitían la conexión entre MTUs y RTUs del mismo fabricante, limitando las operaciones a escaneo, control e intercambio de datos.

La conexión entre las MTUs y las RTUs, en ausencia de redes abiertas, se realizaba a nivel de bus, mediante estándares de comunicación como *RS-232* o adaptadores propietarios que se conectaban directamente al backplane de la CPU. Esta falta de estándares abiertos dificultaba la interoperabilidad entre dispositivos de diferentes proveedores, lo que evidenciaba la necesidad urgente de implementar estándares abiertos.

Figura 17



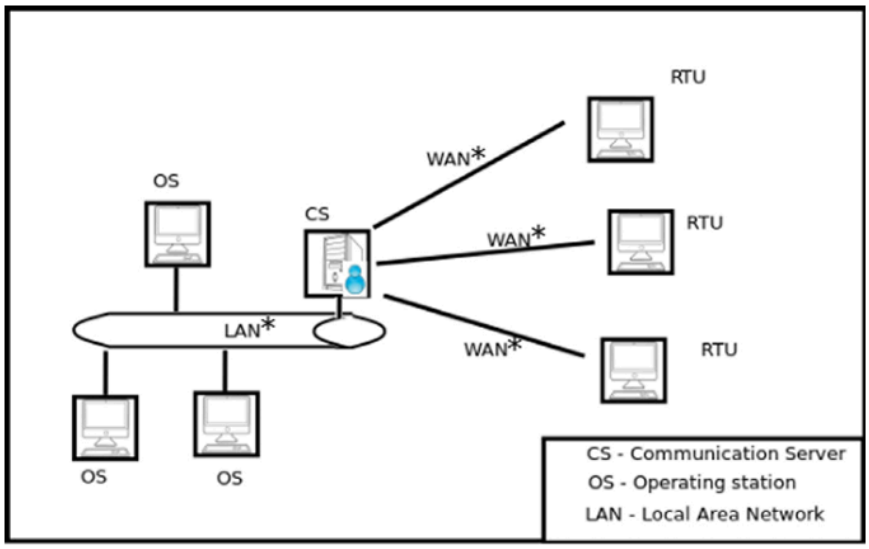
Nota. Arquitectura monolítica de SCADA. Tomado de *Architecture and security of SCADA systems: A review* (p. 4), por Yadav, G. y Paul, K., 2021, Science Direct.

En las décadas de 1980 y 1990 surgieron las arquitecturas SCADA distribuidas, donde introdujeron un enfoque de comunicación entre las MTU y las RTU mediante protocolos de comunicación y servidores, aunque aún no permitían conexión a Internet. Estas arquitecturas interconectadas se limitaban a redes de corto alcance, como redes LAN. Los protocolos de LAN y WAN utilizados en esta época eran propietarios y distintos de los protocolos actuales, lo que los hacía específicos para el entorno de cada proveedor. Esta generación distribuida permitía repartir la carga de procesamiento en múltiples sistemas conectados a través de la LAN,

asignando funciones específicas a cada uno. Por ejemplo, algunos actuaban como procesadores de comunicación, otros como interfaces de operador, servidores de base de datos, entre otros.

A pesar de esta estructura distribuida, en el lado de las MTU, las capacidades de las RTU seguían siendo limitadas. La comunicación entre las MTU y las RTU se realizaba a través de la WAN, mientras que el intercambio de información entre los dispositivos de la MTU se hacía en la LAN. Sin embargo, la longitud máxima de los cables en esta red local restringía la conexión a un entorno limitado, como una sola sala. Los sistemas SCADA distribuidos, al igual que los monolíticos, dependían de hardware, software y protocolos de red propietarios suministrados por el mismo fabricante, lo cual impedía la comunicación con dispositivos externos que usaran otros protocolos.

Figura 18



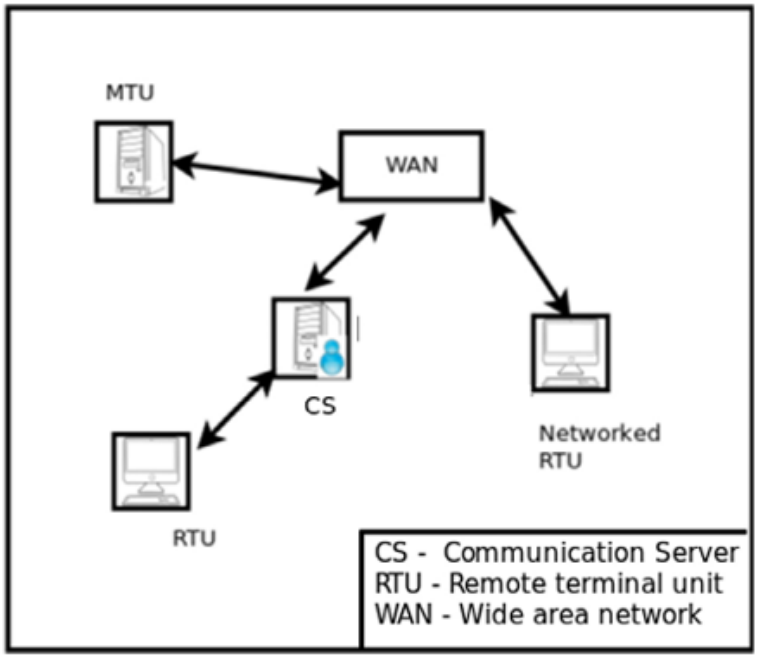
Nota. Arquitectura distribuída de SCADA. Tomado de *Architecture and security of SCADA systems: A review* (p. 8), por Yadav, G. y Paul, K., 2021, Science Direct.

Posteriormente, en los años 2000, se introdujeron las arquitecturas SCADA en red, que permitieron la interconexión a través de Internet, mejorando la capacidad de monitoreo y control remoto. Aunque los SCADA en red comparten similitudes con los SCADA distribuidos, la diferencia clave radica en el uso de protocolos abiertos y estándares de comunicación en lugar de protocolos propietarios, permitiendo así la conexión de dispositivos periféricos de terceros a la red. La incorporación del *Protocolo de Internet*[48] (IP) en la comunicación entre MTU y RTU fue un cambio decisivo, ya que introdujo una mayor capacidad de recuperación ante desastres.

[48] Es el estándar de comunicación que define cómo se envían y reciben datos a través de redes interconectadas, siendo fundamental para el funcionamiento de Internet y otras redes.

Además, el uso de estándares abiertos facilita la interoperabilidad, permitiendo que la funcionalidad de la MTU se distribuya a través de una red WAN. Esto representa un avance significativo en términos de flexibilidad y escalabilidad de los sistemas SCADA, al mismo tiempo que plantea nuevos desafíos de seguridad al estar expuestos a redes externas.

Figura 19

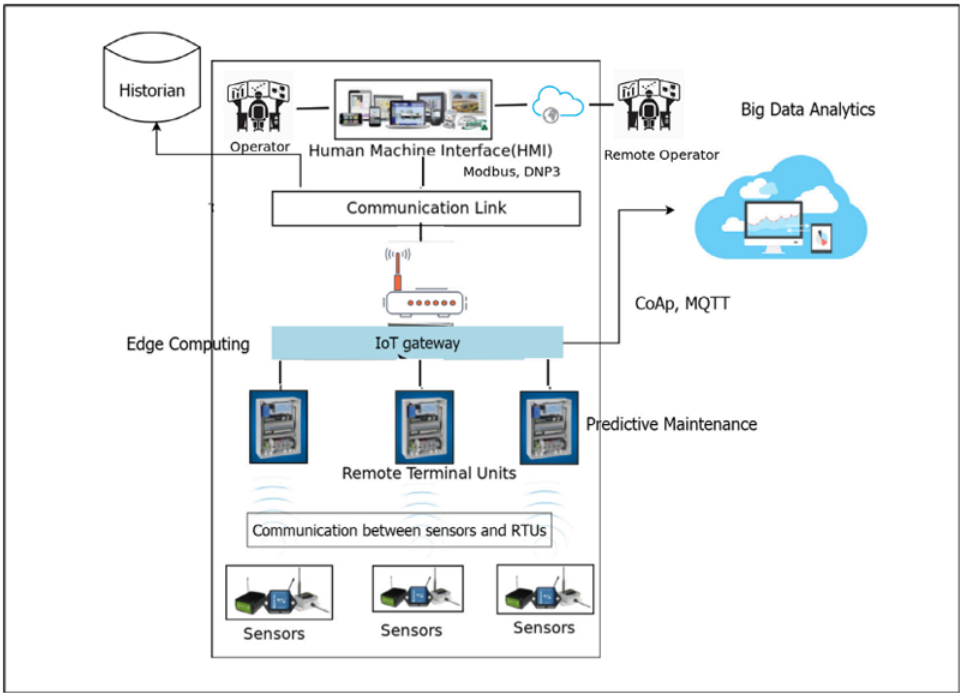


Nota. Arquitectura de sistemas SCADA en red. Tomado de *Architecture and security of SCADA systems: A review* (p. 5), por Yadav, G. y Paul, K., 2021, Science Direct.

Por otro lado, las arquitecturas SCADA basadas en la web permiten que los usuarios accedan a estos sistemas a través de navegadores web y dispositivos móviles, facilitando el control remoto. A medida que dicho sistema se fue complejizando, se fue volviendo más susceptible **[19]**.

Finalmente están los sistemas SCADA basados en IoT. Se caracterizan por la integración de la nube, la computación cognitiva y la analítica avanzada de datos, lo que permite optimizar tanto el monitoreo como el control de procesos industriales. Esta arquitectura utiliza estándares abiertos de comunicación para facilitar la interoperabilidad y escalabilidad, permitiendo una conexión eficiente de dispositivos distribuidos a través de redes *IPv6* y tecnologías de la *Industria 4.0*. La capacidad de estos sistemas para almacenar datos en la nube y extraer información valiosa mediante análisis predictivos ha reducido considerablemente los costos de infraestructura y mantenimiento **[12]**. Además, incorpora técnicas avanzadas de detección de anomalías, lo que incrementa su resiliencia ante fallas y permite programar el mantenimiento preventivo, mejorando así la eficiencia operativa y reduciendo el tiempo de inactividad en infraestructuras críticas.

Figura 20



Nota. SCADA basado en IoT. Tomado de *Architecture and security of SCADA systems: A review* (p. 6), por Yadav, G. y Paul, K., 2021, Science Direct.

Como ya se ha hablado a lo largo de la presente TFC, las redes SCADA, al igual que cualquier otro tipo de red o sistema industrial, enfrentan una serie de amenazas de seguridad que pueden comprometer su funcionamiento, integridad y disponibilidad. Debido a su importancia en infraestructuras críticas, como la energía, el agua y el transporte, la seguridad de estos sistemas es esencial para prevenir daños catastróficos.

Por un lado, los ataques *DoS*, como el uso de herramientas *Slowloris* y *GoldenEye* en el sistema operativo *Kali Linux*, o la herramienta *Low Orbit Ion Cannon* (LOIC), están diseñados para sobrecargar los recursos de la red SCADA, bloqueando el acceso legítimo a los servicios y haciendo que los sistemas de control queden inutilizados temporalmente. Otro desafío, que ya se ha tratado, se vincula a los protocolos de comunicación. En muchos sistemas SCADA, el *Protocolo de Red Distribuida 3.0* (DNP3), utilizado para la comunicación entre dispositivos, carece de mecanismos de autenticación adecuados. Esta debilidad en la seguridad del protocolo puede facilitar ataques de suplantación de identidad, en los que un atacante se hace pasar por un dispositivo autorizado para emitir comandos maliciosos dentro del sistema. A continuación, se puede observar la amplia variedad de ataques a los que se enfrenta dicho sistema y sus redes, junto con sus orígenes y posibles herramientas a emplear. Dicha tabla se basa en lo publicado en el paper *A Survey of Security in SCADA Networks: Current Issues and Future Challenges* (p. 4 y 5):

Tabla 9

Ataques	Descripción del ataque	¿Cómo ocurre?
Man-in-the-Middle (MiTM)	El atacante intercepta la comunicación entre dos partes y altera o espía los datos transmitidos	Se infiltra entre la MTU y las RTU utilizando técnicas de secuestro de sesión o IP Spoofing para manipular la conexión

Denegación de Servicio (DoS)	Saturación de recursos del sistema para hacerlo inaccesible a los usuarios legítimos	Sobrecarga de la red enviando paquetes masivos a la MTU o dispositivos IoT, agotando el ancho de banda y recursos
Fragmentación	Envío de datagramas de gran tamaño para provocar la saturación de la red y la indisponibilidad de recursos	Envío de paquetes mayores al tamaño máximo permitido, agotando la capacidad de transmisión de la red
Suplantación de Identidad (Masquerade)	El atacante se hace pasar por un usuario legítimo para acceder al sistema sin autorización	Mediante técnicas de IP Spoofing y ataques de fuerza bruta para obtener credenciales o contraseñas robadas
Eavesdropping (Escucha pasiva)	Escucha no autorizada de comunicaciones para robar información sensible	El atacante accede a las comunicaciones inalámbricas entre dispositivos IoT o SCADA utilizando herramientas de monitoreo

Los estándares tradicionales y los sistemas de detección de intrusiones, como los firewalls, no son suficientes para enfrentar los ataques emergentes en las redes SCADA. Para aumentar la inmunidad de los sistemas SCADA, se están utilizando algoritmos de aprendizaje automático, como *Naïve Bayes*, *Random Forest*, el *algoritmo C4.5* de árboles de decisión y *Máquinas de Soporte Vectorial* (SVM), para detectar intrusiones en la red **[19]**. Un enfoque popular es el IDS basado en reglas, que utiliza un análisis profundo del protocolo y un método de *Inspección de Paquetes* (DPI). Las reglas establecidas permiten detectar tanto ataques conocidos

como su fuente, aunque tienen limitaciones frente a intrusiones no identificadas en redes abiertas.

En arquitecturas SCADA aisladas, también conocidas como redes m-conectadas, se emplean modelos dinámicos de detección que utilizan loggers de paquetes y algoritmos de coincidencia de patrones para generar nuevas reglas de detección. Sin embargo, estos enfoques no garantizan la detección de ataques desconocidos y requieren investigación adicional para mejorar su precisión. Por otro lado, el *modelo OCSVM* (One-Class Support Vector Machine) desarrollado en 2014, permite detectar anomalías sin necesidad de datos etiquetados para el entrenamiento. Utiliza descripciones de *Datos de Soporte Vectorial* (SVDD) y métodos basados en kernels para identificar patrones anómalos en tiempo real.

El modelo combinado de *OCSVM* con *clustering K-means* aborda algunos de los desafíos de la detección de intrusiones, como los falsos positivos y el sobreajuste. Esta combinación permite agrupar alertas severas y ajustar el sistema para minimizar errores en futuras detecciones. Otro enfoque híbrido de detección de anomalías, introducido en 2017, utiliza la selección de características relevantes para minimizar la complejidad computacional y alcanzar una precisión del 99.5% en la detección de ataques específicos. Sin embargo, aunque estos sistemas de detección son efectivos para identificar comportamientos anómalos, no abordan

completamente la necesidad de proteger el canal de comunicación, lo que subraya la importancia de implementar esquemas avanzados de gestión de claves y cifrado en los sistemas SCADA **[19]**.

Uno de los protocolos más relevantes es el establecimiento de claves para SCADA, conocido como *SCADA Key Establishment* (SKE). El mismo categoriza la comunicación en dos tipos:

- La comunicación entre un controlador y sus dispositivos subordinados (Controller-Subordinate o C-S) utilizando criptografía simétrica.
- La comunicación entre iguales (peer-to-peer o P-P), que se basa en criptografía asimétrica.

Para las comunicaciones C-S, SKE emplea varios tipos de claves, como la *Clave de Largo Plazo* (Long-Term Key o LTK), que se distribuye manualmente entre el controlador y el subordinado, y la *Clave de Sesión* (Session Key o SK), generada con parámetros como la identidad del remitente y los *Parámetros de Tiempo* (TVP) que incluyen sellos temporales y números de secuencia. En cuanto a las comunicaciones P-P, SKE utiliza una *Clave Pública de Autoridad Criptográfica* (CAPK), una *Clave Común* (CK) y una SK, lo que garantiza la integridad y confidencialidad de las comunicaciones entre los nodos. No obstante, la gestión manual de estas claves puede aumentar la complejidad operativa.

Una evolución del esquema SKE es la *Arquitectura de Gestión de Claves de SCADA* (SCADA Key Management Architecture o SKMA), que simplifica la gestión de claves mediante la implementación de un protocolo de intercambio de claves entre un *Centro de Distribución de Claves* (Key Distribution Center o KDC) y los nodos de la red. Esta arquitectura reduce la cantidad de claves necesarias y acumula las claves únicamente en los nodos más críticos y en el KDC. Una vez completado el establecimiento de claves, se genera una clave de sesión que utiliza una función pseudoaleatoria, una *nonce-key*[49] y un sello temporal. Aunque SKMA simplifica el proceso de gestión, no ofrece una solución eficaz para las comunicaciones por difusión o broadcast, lo que plantea limitaciones en la confidencialidad e integridad de estas comunicaciones **[19]**.

Para abordar estos problemas, se desarrolló el protocolo de *Jerarquía Lógica de Claves* (Logical Key Hierarchy o LKH), que organiza los nodos en una estructura de árbol en la que cada nodo almacena las claves desde la raíz hasta su hoja. Cuando un nodo se une o abandona la red, las claves de todo el árbol se actualizan para preservar la seguridad del sistema. Este esquema es fundamental en redes SCADA, ya que los dispositivos pueden entrar o salir de la red con frecuencia, lo que requiere actualizaciones constantes de claves. Para optimizar aún más este proceso, se propuso la *Arquitectura Avanzada de Gestión de Claves* (Advanced Key Management Architecture o ASKMA), que distribuye la carga computacional entre nodos de alto

[49] Es un valor único generado dinámicamente y utilizado junto con una clave para garantizar la seguridad en procesos criptográficos, evitando la repetición de mensajes y protegiendo contra ataques de reproducción.

y bajo rendimiento, garantizando una gestión eficiente de los recursos y asegurando que las operaciones críticas puedan mantenerse sin interrupciones.

Otro enfoque importante es la criptografía híbrida, que combina criptografía simétrica y asimétrica para optimizar el rendimiento de los sistemas SCADA. La *Arquitectura Híbrida de Gestión de Claves* (Hybrid Key Management Architecture o HKMA) utiliza criptografía asimétrica en la comunicación entre las MTU y unidades subordinadas (sub-MTU) y criptografía simétrica para la comunicación entre las sub-MTU y las RTU. Esto reduce la cantidad de claves almacenadas en dispositivos con recursos limitados, lo que es crucial para mejorar el rendimiento en redes SCADA-IoT. Una evolución de este enfoque es la *Arquitectura Avanzada de Gestión de Claves Híbrida* (Advanced Hybrid Key Management Architecture o AHSKMA), que incorpora *Criptografía Basada en Curvas Elípticas* (ECC) para aumentar la seguridad en las comunicaciones entre los nodos.

En el ámbito de las amenazas cuánticas emergentes, se ha propuesto el uso del algoritmo criptográfico NTRU, un esquema basado en criptografía lattice que proporciona mayor velocidad en las operaciones de cifrado y descifrado en comparación con los esquemas tradicionales. NTRU utiliza operaciones polinomiales para proteger las comunicaciones en tiempo real y ha demostrado ser resistente a ataques cuánticos. Además, el algoritmo NTRU incluye mecanismos como la generación de claves públicas y privadas, la creación de firmas digitales y la verificación

de integridad mediante funciones hash, lo que lo convierte en una solución robusta para redes SCADA que requieren protección contra futuros avances en la criptografía cuántica.

Para mejorar la prevención de intrusiones en las redes SCADA, es esencial implementar IDS avanzados, que empleen tanto el análisis del comportamiento como técnicas proactivas de gestión de claves. Los *Sistemas de Distribución de Claves Autocurativas* (LiSH) destacan por su capacidad para detectar y mitigar rápidamente compromisos en la red. La idea central es que este sistema puede “autosanarse” sin intervención manual mediante estas "claves autocurativas", lo que significa que, si se detecta que un nodo o usuario está comprometido, las claves pueden ser renovadas automáticamente (rekeying) sin comprometer la seguridad del resto de la red. Esto es especialmente útil en entornos SCADA porque algunos de sus componentes, como las RTU, tienen limitaciones de almacenamiento y procesamiento.

La integración de tecnologías IoT en sistemas SCADA ha incrementado su capacidad para adaptarse a procesos complejos mediante el uso de protocolos como *6LoWPAN* y la adopción de *IPv6*. Esto facilita la conexión eficiente de dispositivos distribuidos y permite el intercambio de información en tiempo real, optimizando el monitoreo y control.

Las arquitecturas SCADA modernas utilizan una variedad de medios de comunicación, como cables, radiofrecuencia, redes celulares y satelitales, para la transmisión de datos entre dispositivos de campo y unidades centrales. Sin embargo, la dependencia de protocolos abiertos

utilizados en Internet hace que estos sistemas sean vulnerables a ciberamenazas externas. Esta apertura expone los sistemas a riesgos adicionales, ya que la interconexión con redes corporativas o externas introduce nuevas amenazas, permitiendo que paquetes maliciosos accedan a dispositivos sin necesidad de un acceso físico directo.

La transición hacia una infraestructura basada en IP requiere una gestión cuidadosa de los riesgos, con énfasis en la separación física y, de no ser posible, lógica entre la red SCADA y otras redes, como las corporativas **[20]**. La implementación de redes privadas virtuales (VPN) y sistemas de prevención de intrusiones (IPS) es esencial para proteger la integridad de las comunicaciones. Además, la criptografía desempeña un papel central en esta protección, utilizando algoritmos simétricos para un cifrado eficiente de los datos y algoritmos asimétricos para la autenticación y el intercambio seguro de claves.

El uso de *6LoWPAN* permite la integración de dispositivos IoT en redes SCADA mediante conexiones de bajo consumo energético, facilitando la adopción de *IPv6* en sistemas industriales. Sin embargo, estos dispositivos operan con recursos limitados, como baja capacidad de procesamiento, memoria restringida y limitaciones en el consumo de energía, lo que dificulta la implementación de algoritmos de cifrado complejos y mecanismos avanzados de seguridad **[20]**. Por esta razón, es fundamental diseñar esquemas de gestión de claves ligeros y eficientes

que a fin de mantener la seguridad de las comunicaciones sin comprometer el rendimiento del sistema ni agotar los recursos disponibles.

Tabla 10

Gestión de la Política de Seguridad de Comunicaciones General	
Etapas	*Tareas*
1	Inventario y Clasificación de Dispositivos: ● Identificar y registrar todos los dispositivos (MTU, RTU, PLC, IED, IoT). ● Asignar niveles de criticidad según la función del dispositivo y su impacto en la infraestructura.
2	Evaluación de Riesgos y Amenazas: ● Analizar las amenazas potenciales: DoS, MiTM, suplantación y escucha pasiva. ● Revisar protocolos en uso, como DNP3, y sus limitaciones de seguridad. ● Evaluar cómo la conectividad a Internet y la integración de IoT aumentan los riesgos.
3	Definición de Políticas y Configuraciones de Seguridad: ● Establecer segmentación física o lógica entre redes SCADA e Internet. ● Implementar configuraciones seguras en todos los dispositivos con autenticación robusta. ● Definir políticas para el uso de VPN e IPS en la protección de comunicaciones.
4	Implementación de Esquemas de Criptografía y Gestión de Claves: ● Aplicar criptografía simétrica para comunicaciones rápidas y asimétrica

	para autenticación. ● Desarrollar esquemas ligeros de gestión de claves para IoT con 6LoWPAN. ● Asegurar la distribución eficiente de claves mediante un centro de distribución (KDC).
5	Monitoreo Continuo y Auditoría de Seguridad: ● Implementar sistemas IDS para la detección temprana de intrusiones. ● Realizar auditorías periódicas y actualizar firmware de los dispositivos. ● Establecer procedimientos de respuesta ante incidentes y contingencias.

3.5.1. Conectividad por Cable

La conectividad por cable en sistemas SCADA depende de una variedad de protocolos de comunicación diseñados para facilitar la transmisión de datos entre componentes como las MTU y las RTU. Estos protocolos están estructurados en capas y cumplen funciones esenciales de control, transmisión de datos y respuesta, permitiendo la operación de sistemas industriales de manera confiable y escalable. Entre los protocolos cableados más utilizados se encuentran *Modbus*, *DNP3* (de estos dos últimos ya hemos ahondado un poco), *IEC 60870-5*, *Foundation Fieldbus*, *Profibus*, *IEC 61850* y *HART*.

Modbus es uno de los protocolos más antiguos y ampliamente adoptados en la capa de aplicación, desarrollado por *Gould Modicon* para sus controladores *Modicon*. Se caracteriza por su simplicidad y su naturaleza de código abierto, lo cual facilita su implementación y es ideal

para entornos con un solo “maestro” y “múltiples esclavos". Su variante *Modbus/TCP* permite comunicaciones confiables en redes de Internet e Intranet, aunque su seguridad es limitada frente a ataques como DoS y Man-in-the-Middle.

DNP3, desarrollado bajo el modelo de *Arquitectura de Rendimiento Mejorado* (EPA), fue diseñado para maximizar la interoperabilidad abierta entre RTUs, MTUs y PLCs. A diferencia de *Modbus*, *DNP3* admite comunicación entre múltiples “maestros” y “esclavos", además de comunicación entre iguales (peer-to-peer). Este protocolo introduce capas adicionales para manejo de errores y priorización, y se ha fortalecido mediante criptografía para evitar ataques de intermediario y de repetición.

Por su parte, el protocolo *IEC 60870-5,* que también sigue el modelo EPA, incluye una capa de aplicación que facilita las funciones específicas de los sistemas de telecontrol. Utilizado ampliamente en Europa para sistemas de automatización industrial, este protocolo permite autenticación en el nivel de comunicación, aunque no incorpora medidas avanzadas de seguridad en sus capas de aplicación y enlace de datos, lo cual lo hace vulnerable a ciertos tipos de ataques.

Foundation Fieldbus, desarrollado por *FieldComm Group*, utiliza una arquitectura de cuatro capas en la que se añade una capa de usuario para servir de puente entre dispositivos de campo y aplicaciones de software. Este protocolo destaca por su bajo costo en infraestructura y facilidad de integración en procesos industriales.

También, se encuentra *Profibus* es un protocolo promovido por Alemania para el control de procesos y manufactura discreta. Permite un intercambio de datos cíclico entre MTUs y RTUs, y su arquitectura admite variaciones como *Profibus DP* para periféricos distribuidos.

Ahora bien, *IEC 61850* fue creado por el *Comité Técnico 57* de la *IEC* para mejorar la interoperabilidad entre dispositivos electrónicos inteligentes, especialmente en subestaciones eléctricas. Este protocolo no solo gestiona la transmisión de datos, sino también su almacenamiento, y es compatible con múltiples modelos de datos, lo que facilita su integración en diversos entornos industriales.

Finalmente, *HART* (Highway Addressable Remote Transducer) es un protocolo bidireccional desarrollado inicialmente por *Rosemount Inc.* y es ampliamente utilizado en aplicaciones de control de procesos. Su estructura híbrida permite canales de comunicación simultáneos, uno analógico y otro digital, lo que facilita la transmisión de valores de proceso junto con otros tipos de información en la misma infraestructura de cableado.

Figura 21

Attribute	Modbus	DNP3	IEC 6870-5-101	Foundation Fieldbus	Profibus	**IEC 61850**	HART
Year	1979	1993	1995	2004	1989	2005 (Project started in 1995)	1986
Organization	Gould Modicon	Harris, Distributed Automation Products	IEC	FieldComm Group	Promoted by BMBF (Germany)	IEC Technical Committee 57	Rosemount Inc.
Architecture	Single layer i.e. Application layer	4 layer architecture	3 layer architecture based on EPA model.	4 layer architecture	3 layer architecture	3 layer architecture	5 layer architecture
Addressing	8-bit address	16-bit source and destination addresses	0, 8, 16-bit addresses are supported	8, 16, 32-bit addresses are supported	7-bit address (0–3 address are used by master and rest by slaves)	48-bit source and destination addresses	4-bit addresses (newer version support 32 bit address)
Users	Target low volume data applications	China, North America, and Australia	Europe, China	America and France	All over the world	All over the world	All over the world
Source	Open source	Open source	Commercially available	Open source	Commercially available	Open source	Open source
Security state	No encryption and authentication control	DNP3-SA support encryption and authen-tication control	No encryption but supports authentication control	No encryption and authentication control	Supports encryption and authentication control	No encrption but supports authentication control	No encryption and authentication control
Possible attacks	DoS, MiTM [42]	Response replay, MiTM attack [44]	DoS [43]	DoS, MiTM [45]	DoS	DoS, Spoofing, MiTM [46]	Spoofing attacks, Lack of authentication and XML injection attack

Nota. Comparación de protocolos de comunicación SCADA cableados. Tomado de *Architecture and security of SCADA systems: A review* (p. 5), por Yadav, G. y Paul, K., 2021, Science Direct.

Entre la amplia variedad de opciones existentes, es importante tener en cuenta que la elección del protocolo de comunicación adecuado depende de las necesidades específicas de cada sistema SCADA-IoT, como el volumen de datos, el alcance geográfico y las exigencias de seguridad.

Tabla 11

Gestión de la Política de Conectividad por Cable	
Etapas	*Tareas*
1	Análisis de Protocolos de Comunicación Existentes: ● Identificar y analizar los protocolos de comunicación cableados compatibles. ● Determinar los requisitos específicos de cada componente, incluyendo volumen de datos, distancia de transmisión y necesidades de seguridad. ● Evaluar la escalabilidad y facilidad de integración de cada protocolo en función de las necesidades del sistema.
2	Selección de Protocolos Adecuados para el Sistema: ● Seleccionar los protocolos que mejor cumplan los requisitos de control y transmisión de datos del sistema. ● Priorizar protocolos con mecanismos de autenticación y gestión de errores avanzados, como DNP3 e IEC 61850. ● Favorecer protocolos de código abierto cuando se busque reducir la dependencia de proveedores y mejorar la interoperabilidad.
3	Configuración de Protocolos Seleccionados: ● Configurar la estructura de capas de comunicación de cada protocolo en la arquitectura SCADA. ● Definir parámetros específicos de cada protocolo, como dirección de dispositivos y frecuencia de comunicación, para optimizar el rendimiento.
4	Implementación de Medidas de Seguridad: ● Aplicar mecanismos de cifrado y autenticación en protocolos compatibles, como DNP3 e IEC 60870-5. ● Fortalecer protocolos vulnerables mediante controles externos, como

	firewalls y VPNs, especialmente para protocolos sin seguridad avanzada (e.j., Modbus).
5	Integración y Pruebas de Comunicación: ● Realizar pruebas de conectividad entre MTU y RTU para validar la transmisión de datos en tiempo real. ● Monitorear la eficiencia y estabilidad del sistema, ajustando configuraciones para asegurar transmisión confiable.

3.5.2. Conectividad Inalámbrica

A medida que los sistemas SCADA han evolucionado, la adopción de diversos protocolos inalámbricos, como *IEEE 802.15.4*, *Zigbee*, *Bluetooth Low Energy* (BLE), *LoRa*, *WirelessHART* y *Wi-Fi*, ha permitido que estos sistemas se adapten a necesidades específicas de comunicación y transmisión de datos en entornos industriales.

Por un lado tenemos a la *IEEE 802.15.4*, la misma es un estándar fundamental para muchos protocolos inalámbricos utilizados en SCADA, como *Zigbee* y *WirelessHART*. Fue diseñado para redes de área personal de baja velocidad y opera en la banda de 2.4 GHz ISM[50], siendo ideal para aplicaciones de bajo costo y bajo consumo energético. *IEEE 802.15.4* soporta una velocidad de datos de hasta 250 kbps, con un alcance de aproximadamente 10 metros. Este

[50] Es una frecuencia libre de licencia utilizada globalmente para aplicaciones como Wi-Fi, Bluetooth y redes IoT, diseñada inicialmente para dispositivos industriales, científicos y médicos.

estándar está estructurado en las capas física y de control de acceso del modelo OSI, permitiendo configuraciones de red en topologías punto a punto y estrella.

También se encuentra *Zigbee*, basado en *IEEE 802.15.4* y desarrollado por la *Zigbee Alliance*.Es un protocolo ampliamente adoptado para redes inalámbricas de área personal en entornos industriales y se caracteriza por una estructura la cual incluye dispositivos con diferentes niveles de funcionalidad: dispositivos de funcionalidad completa, dispositivos de funcionalidad reducida y un coordinador. Esta arquitectura permite la configuración de redes ad hoc de baja potencia y bajo alcance, típicamente de entre 10 y 100 metros. Se caracteriza por ser una solución de bajo consumo y seguridad confiable, pues emplea cifrado simétrico de 128 bits, y su velocidad de transmisión de datos alcanza los 250 kbps, lo que lo convierte en una opción adecuada para aplicaciones de monitoreo y control a corta distancia en SCADA.

Bluetooth Low Energy (BLE) es una versión optimizada de Bluetooth clásica, desarrollada para minimizar el consumo de energía. BLE utiliza una arquitectura de maestro-esclavo, donde el nodo “maestro" se conecta a varios nodos “esclavos”, con cada nodo “esclavo” en modo de suspensión para conservar energía hasta que sea necesario intercambiar datos. BLE soporta la transmisión rápida de pequeños paquetes de datos con una velocidad de hasta 1 Mbps y tiene una eficiencia energética 2.5 veces superior a la de *Zigbee*. Aunque no permite transmisión continua de datos, BLE es útil para aquellas aplicaciones donde se requiere

un consumo de energía extremadamente bajo y una comunicación intermitente y controlada en redes SCADA.

Por su parte, *LoRa* (Long Range) es un protocolo de comunicación desarrollado para aplicaciones de larga distancia, permitiendo una cobertura de hasta 10 kilómetros con una baja tasa de transmisión de datos, generalmente a menos de 50 kbps. Es particularmente útil en aplicaciones donde no se necesita transmisión en tiempo real y la tolerancia a fallos es crítica. A su vez, utiliza la capa física junto con la arquitectura *LoRaWAN*, permitiendo así que sistemas SCADA en áreas geográficamente amplias puedan recopilar datos de sensores distribuidos de manera efectiva, incluso en condiciones de energía limitada.

WirelessHART es una extensión inalámbrica del protocolo *HART*, manteniendo la compatibilidad con dispositivos y herramientas *HART* existentes. *WirelessHART* opera en la banda de 2.4 GHz y se basa en una red de malla inalámbrica, en la cual cada dispositivo conectado actúa como un repetidor, aumentando la confiabilidad y el alcance de la red. Este protocolo es ampliamente utilizado en entornos industriales SCADA debido a su capacidad para proporcionar una comunicación robusta y segura, a fin de promover la continuidad del flujo de datos entre dispositivos críticos en entornos de producción.

Por último, *Wi-Fi (IEEE 802.11)*, que proporciona altas velocidades de transmisión de datos y es una opción común en redes SCADA modernas. Los estándares *Wi-Fi* actuales, como

el *802.11ac*, permiten tasas de hasta 1 Gbps y operan en las bandas de 2.4 GHz y 5 GHz. Con un alcance de aproximadamente 20 metros en interiores y 150 metros en exteriores. Es ideal para aplicaciones donde se requiere alta velocidad de transmisión de datos y acceso a redes abiertas. Sin embargo, debido a su naturaleza abierta y accesibilidad, presenta mayores riesgos de seguridad comparado con protocolos inalámbricos específicos para SCADA, ya que los adversarios dentro del rango de la red pueden intentar obtener acceso no autorizado.

En cuanto a los protocolos de capa de aplicación diseñados para IoT, el *Constrained Application Protocol* (CoAP) y *Message Queue Telemetry Transport* (MQTT) son dos opciones populares en entornos SCADA basados en IoT. CoAP es una alternativa ligera al protocolo HTTP, especialmente diseñada para dispositivos IoT con recursos limitados. Es un protocolo eficiente en espacio y en el uso de recursos, proporcionando una comunicación fiable mediante mensajes de confirmación y no confirmación, con soporte de descubrimiento de recursos, intercambio de mensajes y configuración automática. Por otro lado, MQTT sigue un modelo de publicación y suscripción, siendo adecuado para aplicaciones de baja latencia. Aquí, los clientes actúan como publicadores o suscriptores y se comunican a través de un broker central, lo que permite una transmisión de datos eficiente entre múltiples dispositivos en una red SCADA distribuida.

Nuevamente, la selección del protocolo adecuado depende de factores como la distancia, el consumo de energía, la velocidad de transmisión y las necesidades de seguridad específicas del sistema.

Tabla 12

Gestión de la Política de Conectividad Inalámbrica	
Etapas	*Tareas*
1	Análisis y Selección de Protocolos: ● Evaluar los requisitos de comunicación de acuerdo con las necesidades de la red SCADA. ● Identificar protocolos inalámbricos compatibles. ● Seleccionar protocolos según alcance, velocidad de transmisión, consumo de energía y seguridad.
2	Configuración de Seguridad en Protocolos: ● Definir y aplicar cifrado adecuado para proteger la comunicación. ● Establecer autenticación y control de acceso para dispositivos de red. ● Implementar mecanismos de detección de intrusiones para monitorear accesos no autorizados en la red.
3	Diseño de Topología de Red Inalámbrica: ● Determinar la arquitectura de red adecuada (e.g., malla en WirelessHART, punto a punto en BLE). ● Configurar los dispositivos según la topología seleccionada. ● Asegurar que la configuración soporte redundancia y recuperación ante fallos.

4	Pruebas de Conectividad y Desempeño: ● Realizar pruebas de alcance y estabilidad de señal en el entorno operativo. ● Evaluar la tasa de transmisión y latencia para asegurar el rendimiento en tiempo real. ● Verificar la interoperabilidad entre dispositivos de distintos fabricantes en la red.
5	Monitoreo y Mantenimiento Continuo: ● Implementar un sistema de monitoreo para detectar anomalías en la comunicación. ● Establecer auditorías periódicas de seguridad en la red. ● Revisar y actualizar la configuración de dispositivos y políticas de seguridad según los cambios tecnológicos y amenazas.

3.5.3. Política de Perímetro

Dicha política tiene como fin establecer las reglas para administrar de manera segura el intercambio de datos entre el sistema y otras redes externas. Se enfoca en controlar y proteger los puntos de entrada y salida de información, definiendo medidas específicas de seguridad en cada área del sistema para evitar accesos no autorizados y mantener la integridad de los datos.

Se identifican todos los puntos de conexión donde los datos ingresan o salen del sistema, lo que incluye el acceso desde redes corporativas u otras externas. En cada uno de estos puntos, se implementan controles de acceso como autenticación multifactor y restricciones según el rol

de cada usuario. Esto garantiza que solo el personal autorizado pueda interactuar con el sistema, reduciendo así el riesgo de accesos indebidos.

A su vez, se dividen las áreas del sistema en diferentes zonas de seguridad. Las zonas con datos o funciones más críticas, como las de operación y supervisión, se mantienen separadas de áreas menos sensibles, como las de administración. Esto permite personalizar los requisitos de seguridad en función de la importancia de cada área y aplicando métodos de protección específicos para cada zona.

Para proteger las comunicaciones entre el sistema y las redes externas, se implementan medidas como el uso de VPNs que cifran los datos en tránsito, evitando que puedan ser interceptados. Además, en las zonas de mayor criticidad se usa cifrado de extremo a extremo para que solo las personas autorizadas puedan acceder a los datos, incluso si la red sufre una intrusión.

No menos importante, es crucial establecer un sistema de monitoreo continuo en todos los puntos de conexión del perímetro para detectar accesos inusuales o sospechosos. Este monitoreo se complementa con auditorías regulares de seguridad que permiten revisar y actualizar la política para adaptarse a nuevas amenazas.

Tabla 13

Gestión de la Política de Perímetro	
Etapas	*Tareas*
1	Identificación de Puntos de Conexión: ● Mapear todos los puntos de entrada y salida de datos en el sistema. ● Evaluar cada punto de conexión en función de su nivel de criticidad.
2	Implementación de Controles de Acceso: ● Seguir apartado de *Política de Control de Acceso* (4.4.1).
3	Segmentación en Zonas de Seguridad: ● Dividir las áreas del sistema en zonas de seguridad según su criticidad (operación, supervisión, administración, etc.). ● Aplicar controles específicos de seguridad en cada zona basados en su "importancia".
4	Protección de Comunicaciones: ● Seguir apartado de *Política de Conectividad Cableada e Inalámbrica* (5.1 y 5.2, respectivamente).
5	Monitoreo Continuo y Auditoría de Seguridad: ● Implementar monitoreo continuo en los puntos de conexión del perímetro para detectar accesos sospechosos. ● Realizar auditorías de seguridad periódicas para actualizar la política y adaptarse a nuevas amenazas.

4. Conclusiones

4.1. Conclusiones Finales

En un contexto de creciente interconectividad, este trabajo concluye en que, la implementación de un marco de ciberseguridad robusto y adaptado a las particularidades de los sistemas SCADA integrados con IoT, es imprescindible para proteger las infraestructuras críticas. A través del análisis desarrollado, se identificaron dos desafíos principales: la falta de seguridad en los protocolos de comunicación y la obsolescencia tecnológica, siendo ambos factores que incrementan la vulnerabilidad de estos sistemas frente a amenazas externas.

Se determinó que los impactos de un ataque exitoso trascienden el ámbito técnico, afectando también el bienestar social, la estabilidad económica y, en algunos casos, la política de las regiones involucradas. Casos recientes, como los ataques a *Oldsmar* y *Colonial Pipeline*, evidencian que la falta de un enfoque integral de ciberseguridad puede generar consecuencias devastadoras para dichas infraestructuras consideradas imprescindibles para nuestra sociedad actual.

Por lo tanto, el desarrollo de este framework ofrece un enfoque estratégico estableciendo diversas políticas junto con sus lineamientos. Este modelo no solo busca maximizar la seguridad

y eficiencia operativa de los sistemas SCADA-IoT, sino también reforzar la resiliencia de estas infraestructuras ante posibles incidentes, promoviendo una confianza pública sostenida en los servicios esenciales.

Finalmente, se reafirma que la protección de las infraestructuras críticas requiere una visión abarcativa y colaborativa, que combine avances tecnológicos con una gobernanza eficaz para responder a los desafíos en un entorno cada vez más complejo.

4.2. Futuras Investigaciones

La investigación en sistemas SCADA sigue siendo un área esencial debido a la evolución de las amenazas y a la integración de tecnologías emergentes como la inteligencia artificial o la computación cuántica. Una de las áreas de investigación más prometedoras es la aplicación de la *Inteligencia Artificial* (IA) a fin de fortalecer la seguridad en estos sistemas. La IA trae consigo algoritmos avanzados, como el *Genetically Seeded Flora Transformer Neural Network* (GSFTNN), diseñados para detectar anomalías en tiempo real en los patrones operativos. Estos modelos basados en aprendizaje profundo pueden mejorar la precisión y reducir falsos positivos en la detección de intrusiones **[21]**.

Otra línea de investigación fundamental es el desarrollo de soluciones de criptografía post-cuántica. Con los avances en la computación cuántica, los métodos de criptografía

tradicionales, como el ECC y el *Algoritmo de Encriptación Avanzada* (AES), se ven en riesgo, ya que los algoritmos cuánticos, como el de *Shor*, pueden vulnerarlos en tiempos significativamente menores **[19]**. Esto sugiere una posible línea de investigación centrada en explorar y adoptar métodos de criptografía resistentes a la computación cuántica, con el objetivo de mantener así la integridad y confidencialidad de las comunicaciones en dichos sistemas en un futuro donde los ataques cuánticos podrían materializarse.

La mejora en los sistemas de detección de intrusiones mediante el uso de *machine learning* también representa una oportunidad clave en este campo. Los algoritmos de aprendizaje automático adaptados a la detección de intrusiones en SCADA, como el *GSFTNN*, necesitan ser probados y optimizados en distintos entornos industriales y contra una variedad de amenazas. Estas mejoras en detección y escalabilidad son esenciales para ambientes críticos donde la capacidad de respuesta y mitigación rápida es fundamental para garantizar la continuidad de las operaciones **[21]**.

La adopción de redes 5G en entornos industriales presenta nuevas oportunidades y desafíos. El potencial de las redes 5G para mejorar la velocidad y reducir la latencia en la comunicación industrial también introduce riesgos de seguridad adicionales **[21]**. Las investigaciones futuras deberán centrarse en la integración segura de redes SCADA en infraestructuras 5G, evaluando posibles vulnerabilidades y desarrollando contramedidas que

respondan a los riesgos específicos de un entorno de comunicación ultrarrápida, que podría ser explotado por atacantes.

Por otro lado, la simulación avanzada de ataques y el estudio de la resiliencia en SCADA son cruciales para anticipar y mitigar amenazas emergentes. Utilizar datasets especializados, como el *WUSTL-IIOT-2018*, permitirá recrear escenarios de ataques en entornos controlados y evaluar la efectividad de los mecanismos de defensa **[21]**. Estas simulaciones ayudarán a validar y mejorar las defensas contra ataques DDoS, de fuerza bruta u otros vectores de intrusión que afectan la estabilidad y seguridad de los mismos.

Cada uno de estos temas plantea direcciones potenciales para la investigación futura en el ámbito de la seguridad de SCADA. Los avances en estas áreas serán esenciales para desarrollar infraestructuras industriales resilientes y seguras para que estos sistemas puedan adaptarse a las demandas de la cuarta revolución industrial y sean capaces de resistir el cambiante panorama en el que se encuentran inmersos.

Referencias

[1] Zhu, B., Joseph, A. y Sastry, S. (2011). *A Taxonomy of Cyber Attacks on SCADA Systems*. IEEE. Recuperado el 02 de septiembre de 2023 de: https://ieeexplore.ieee.org/abstract/document/6142258

[2] Purón, D. (2021). *Los Sistemas IoT y SCADA obligados a convivir y entenderse*. Recuperado el 17 de febrero del 2024 de: https://www.barbara.tech/es/blog/iot-y-los-sistemas-scada-obligados-a-entenderse-y-convivir-en-la-era-digital

[3] Shahzad, A., Kim, Y. y Elgamoudi, A. (2017). *Secure IoT Platform for Industrial Control Systems*. IEEE. Recuperado el 10 de septiembre de 2023 de: https://ieeexplore.ieee.org/abstract/document/7883726

[4] Simon, T. (2017). *Chapter Seven: Critical Infrastructure and the Internet of Things*. JSTOR. Recuperado el 17 de abril de 2024 de: https://www.jstor.org/stable/resrep05239.12?searchText=Critical+Infrastructure&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3DCritical%2BInfrastructure%26so%3Drel&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3Ad841d28f148c1cd0b0370069b83520d5&seq=3

[5] Gobierno de Argentina. (s.f.). *Infraestructuras Críticas*. Recuperado el 17 de abril de 2024 de: https://www.argentina.gob.ar/sites/default/files/infoleg/res1523-1-328599.pdf

[6] Constante, H. (2022). *Programa de ciberseguridad orientado a I.IoT*. Recuperado el 8 de septiembre de 2024 de: https://repositorio.uai.edu.ar/items/f7c20b95-4107-4697-b13d-0468aa3fdaf8

[7] OWASP. (s.f.). *OWASP Internet of Things Project*. Recuperado el 24 de abril de 2024 de: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

[8] Industrial Cybersecurity Pulse. (2022). *Throwback Attack: Kemuri Water Company attack puts critical infrastructure at risk*. Recuperado el 24 de abril de 2024 de: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-kemuri-water-company-attack-puts-critical-infrastructure-at-risk/

[9] NIST. (s.f.). *information technology (IT)*. Recuperado el 5 de julio de 2024 de: https://csrc.nist.gov/glossary/term/information_technology

[10] Gartner. (s.f.). *Operational Technology Security Reviews and Ratings*. Recuperado el 5 de julio de 2024 de: https://www.gartner.com/reviews/market/operational-technology-security

[11] Coolfire Core. (2019). *What Is The Difference Between IT and OT?*. Recuperado el 8 de julio de 2024 de: https://coolfiresolutions.com/blog/difference-between-it-ot/

[12] Yadav, G. y Paul, K. (2021). *Architecture and security of SCADA systems: A review*. Recuperado el 5 de noviembre de 2024 de: https://www.sciencedirect.com/science/article/abs/pii/S1874548221000251

[13] Mihai, A. (2020). *Supervisory control and data acquisition (SCADA): the security of critical infrastructures nowadays*. Recuperado el 21 de julio de 2024 de: https://rocys.ici.ro/documents/51/2020_spring_article_7.pdf

[14] Falco, G.; Caldera, C. y Shrobe, H. (2018). *IIoT Cybersecurity Risk Modeling for SCADA Systems*. Recuperado el 22 de julio de 2024 de: https://ieeexplore.ieee.org/document/8332467?denied=

[15] Sverko, M., Grbac, T. G. y Mikuc, M. (2022). *SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0*. Recuperado el 5 de noviembre de 2024 de: https://ieeexplore.ieee.org/document/9907002

[16] Turun Yliopisto. (2023). *Software-defined zero-trust network architecture : Evolution from Purdue model -based networking*. Recuperado el 5 de noviembre de 2024 de: https://www.utupub.fi/handle/10024/175647

[17] America 's Cyber Defense Agency. (2021). *Compromise of U.S. Water Treatment Facility*. Recuperado el 22 de julio de 2024 de: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a

[18] Gawazah, L. (2024). *To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack*. Recuperado el 2 de septiembre de 2024 de: https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack

[19] Ghosh, S. y Sampalli, S. (2019). *A Survey of Security in SCADA Networks: Current Issues and Future Challenges*. Recuperado el 14 de octubre de 2024 de: https://ieeexplore.ieee.org/abstract/document/8753583

[20] Kim, H. (2012). *Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks*. Recuperado el 29 de octubre de 2024 de: https://journals.sagepub.com/doi/full/10.1155/2012/268478

[21] Diaba, S. Y; Anafo, T.; Tettech, L.; Oyibo, M. A.; Alola, A.A.; Shafie-khah, M. y Elmusrati, M. (2023). *SCADA securing system using deep learning to prevent cyber infiltration*. Recuperado el 12 de noviembre de 2024 de: https://www.sciencedirect.com/science/article/pii/S0893608023002915

[22] Trend Micro. (s.f.). *Industrial Control System*. Recuperado el 12 de noviembre de 2024 de: https://www.trendmicro.com/vinfo/dk/security/definition/industrial-control-system

[23] World Economic Forum. 2015. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services*. Recuperado el 15 de noviembre de 2024 de: https://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf

[24] Dell. 2015. *Dell Security Annual Threat Report*. Recuperado el 15 de noviembre de 2024 de: https://www.silicon.es/wp-content/uploads/2015/12/2015-dell-security-annual-threat-report-white-paper-15657.pdf

[25] Baezner, M. y Robin, P. (2017). *CSS CYBER DEFENSE PROJECT Hotspot Analysis : Stuxnet, available*. Recuperado el 15 de noviembre de 2024 de: https://www.researchgate.net/publication/323199431_Stuxnet

Bibliografía

Transilvania University Press. (2016). *Evolution of SCADA Systems*. Recuperado de: https://webbut.unitbv.ro/index.php/Series_I/article/view/3474

Rambus Press. (2017). *Securing the Industrial Internet of Things (IIoT)*. Recuperado de: https://www.rambus.com/blogs/securing-the-industrial-internet-of-things-iiot/

Balleste, R. (2021). *Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity*. Recuperado de: https://scholarlycommons.law.emory.edu/ecgar/vol8/iss1/1/

Liang, G.; Weller, S. R.; Zhao, J.; Luo, F y Dong, Z. Y. (2017). *The 2015 Ukraine Blackout: Implications for False Data Injection Attacks*. Recuperado de: https://ieeexplore.ieee.org/abstract/document/7752958

Fortinet. (s.f.). *¿Qué es la tecnología operativa (TO)?*. Recuperado de: https://www.fortinet.com/lat/solutions/industries/scada-industrial-control-systems/what-is-ot-security

Nazir, S.; Patel, S. y Patel, D. (2017). *Assessing and augmenting SCADA cyber security: A survey of techniques*. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S0167404817301293

Systems. Recuperado de: https://link.springer.com/book/10.1007/978-3-319-32125-7

Lamba,A.; Singh,S.; Singh,B.; Dutta,N.y Rela,S. (2019). *Mitigating Cyber Security Threats of Industrial Control Systems (Scada & Dcs)*. Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3492685

Nugent, E. y Ratte, M. (2016). *SCADA cybersecurity in the age of the Internet of Things*. Recuperado de: https://www.controleng.com/articles/scada-cybersecurity-in-the-age-of-the-internet-of-things/

Huda, S.; Yearwood; J.; Hassan, M. M. y Almogren, A. (2018). *Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks*. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S1568494618303491

Grubbs, R.; Stoddard, J.; Freeman, S. y Fisher; R. (2021). *Evolution and Trends of Industrial Control System Cyber Incidents since 2017*. Recuperado de: https://onlinelibrary.wiley.com/doi/abs/10.18278/jcip.2.2.4

Kaufman, E.; Adeoye, S. y Batarseh, F. (2023). *Leadership for CyberBioSecurity: The Case of Oldsmar Water*. Recuperado de: https://vtechworks.lib.vt.edu/bitstream/handle/10919/113624/Oldsmar%20Case%20Narrative.pdf?sequence=3

Griffin, R. P. y Benjamin, U. T. (2022). ICCWS 2022 17th International Conference on Cyber Warfare and Security. Recuperado de: https://books.google.es/books?hl=es&lr=&id=Shd2EAAAQBAJ&oi=fnd&pg=PA19&dq=Oldsm

ar+Water+Treatment+Plant+Attack&ots=szaJogBSm0&sig=UMidXv5sN8hi9eOpH7d3htY8Ncs#v=onepage&q=Oldsmar%20Water%20Treatment%20Plant%20Attack&f=false

Lalone, N. (2024). *Chapter 13 - On the growing importance of routine cybersecurity: The Oldsmar Water Plant "Hack"*. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/B9780128095263000117

Beerman, J. ; Berent, D.; Falter, Z. y Bhunia, S. (2023). *A Review of Colonial Pipeline Ransomware Attack*. Recuperado de: https://ieeexplore.ieee.org/abstract/document/10181159

Goodell, J. W. y Corbet, S. (2023). Commodity market exposure to energy-firm distress: Evidence from the Colonial Pipeline ransomware attack. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S1544612322005086

Congressional Research Service. (2021). *Colonial Pipeline: The DarkSide Strikes*. Recuperado de: https://www.everycrsreport.com/files/2021-05-11_IN11667_ed37409706a0e9b48e3630b28cb838b03af6faa8.pdf

Gawazah, L; Rondla, A. y Balhareth, M. S. A. (2024). *To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack*. Recuperado de: https://www.researchgate.net/profile/Lazarus-Gawazah/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack/links/66c1b6bf8d007355925dd805/To-Pay-or-Not-to-Pay-The-US-Colonial-Pipeline-Ransomware-Attack.pdf

Kilman, D. y Stamp, J. (2005). *Framework for SCADA Security Policy*. Recuperado de: https://www.researchgate.net/publication/224179264_SCADA_system_cyber_security_-_A_comparison_of_standards

Figueroa-Lorenzo, S.; Añorga, J. y Arrizabalaga, S. (2019). *A Role-Based Access Control Model in Modbus SCADA Systems*. *A Centralized Model Approach*. Recuperado de: https://www.mdpi.com/1424-8220/19/20/4455

Vistbakka, I. y Troubitsyna, E. (2021). *Modelling and Verification of Safety of Access Control in SCADA Systems*. Recuperado de: https://link.springer.com/chapter/10.1007/978-3-030-68887-5_23

Al-Muntaser, B. ; Mohamad, A. M.; Ammar Y. T. y Imran, A. R. (2023). *Cybersecurity Advances in SCADA Systems*. Recuperado de: https://www.proquest.com/openview/7c71a273bfdf4c328acb90996c0296a6/1?pq-origsite=gscholar&cbl=5444811

Basholli, F.; Mema, B.; Hyka, D.; Basholli, A. y Daberdini, A. (2023). *Analysis of security challenges in SCADA systems, a technical review on automated real-time systems*. Recuperado de: https://publish.mersin.edu.tr/index.php/aed/article/view/1378

Altaleb, H. y Rajnai, Z. (2023). *Malware Attacks on SCADA Systems: Assessing Risks and Strengthening Cybersecurity Measures*. Recuperado de: https://ieeexplore.ieee.org/abstract/document/10417951

Ruiz Salvador, L. C.; Phuoc Dai, N. H. y Zoltán, R. (2023). SCADA Systems: Security Concerns and Countermeasures. Recuperado de: https://ieeexplore.ieee.org/abstract/document/10044495

Wai, E. y Lee, C. K. M. (2024). *Depth in Defense: A Multi-layered Approach to Cybersecurity for SCADA Systems in Industry 4.0*. Recuperado de: https://www.researchgate.net/profile/Eric-Ch-Wai/publication/380523433_Depth_in_Defense_A_Multi-layered_Approach_to_Cybersecurity_for_SCADA_Systems_in_Industry_40/links/66421da308aa54017a055ad6/Depth-in-Defense-A-Multi-layered-Approach-to-Cybersecurity-for-SCADA-Systems-in-Industry-40.pdf

Strohmier, H.; Londhe, R. A.; Clark, C. A.; Pawar, R. y Kram, B. (2024). *Exploring ICS/SCADA Network Vulnerabilities*. Recuperado de: https://link.springer.com/chapter/10.1007/978-3-031-61382-1_14

Mwenda, A. y Ngodya, D. (2023). *A Review of SCADA IoT Device Vulnerabilities in the Power Grid (A Case Study of Smart Meter)*. Recuperado de: https://www.ceeol.com/search/article-detail?id=1217866

Ghosh, S.; Zaman, M.; Joshi, R. y Sampalli, S. (2024). *Multi-Phase Quantum Resistant Framework for Secure Communication in SCADA Systems*. Recuperado de: https://ieeexplore.ieee.org/abstract/document/10474193

Naz, M. T. y Elmedany, W. (2024). *Securing SCADA systems in smart grids with IoT integration: A Self-Defensive Post-Quantum Blockchain Architecture*. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S2542660524003226

Acrecenta. (s.f.). *NIST 800-88: Guía para el Borrado Seguro de Información*. Recuperado de: https://acrecenta.com/es/guias-borrado-seguro-nist-800-88

Nsys Group. (2023). *¿Qué es NIST 800-88 y qué significa realmente Sanitización de Medios?*. Recuperado de: https://nsysgroup.com/es/blog/what-is-nist-800-88-media-sanitization/

Grade, M. y Deoskar, A. (2020). *Industry 4.0 -Digital Transformation, Challenges and Benefits*. Recuperado de: https://www.researchgate.net/publication/344832176_Industry_40_-Digital_Transformation_Challenges_and_Benefits

Boeckl, K.; Fagan, M.; Fisher, W.; Lefkovitz, N.; Megas, K.; Nadeau, E.; Piccarreta, B.; O'Rourke, D. G. y Scarfone, K. (2019). *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*. Recuperado de: https://csrc.nist.gov/pubs/ir/8228/final

Rehman, M. H.; Yaqoob, I.; Salah, K.; Imran, M.; Jayaraman, P. P. y Perera, C. (2019). *The role of big data analytics in industrial Internet of Things*. Recuperado de: https://www.sciencedirect.com/science/article/abs/pii/S0167739X18313645

Sverko, M.; Grbac, T. G. y Mikuc, M. (2022). *SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0*. Recuperado de: https://ieeexplore.ieee.org/document/9907002

Cloudflare. (s.f.). *¿Qué es el modelo OSI?*. Recuperado de: https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

IBM. (s.f.). *¿Qué es la infraestructura crítica?*. Recuperado de: https://www.ibm.com/mx-es/topics/critical-infrastructure

Kardon, S. (2023). Florida Water Treatment Plant Hit With Cyber Attack. Recuperado de: https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack